The 2018 Annual Gathering of The West Virginia State Bar

The Greenbrier

White Sulphur Springs, WV

Twenty Years on the Fourth Circuit

Judge Robert King
U.S. Court of Appeals for the Fourth Circuit

Robert Bruce King
United States Circuit Judge
for the Fourth Circuit

Robert Bruce King was appointed to the United States Court of Appeals for the Fourth Circuit by President Clinton in October 1998.

Bob King was born in Greenbrier County in 1940. As a boy, he worked as a caddie at The Greenbrier. Judge King thereafter brought his passion for golf to West Virginia University, where he lettered three years for Ira Rodgers on the men's golf team. After earning an A.B. degree at WVU in 1961, Judge King entered active duty as an officer in the Air Force. Following military service, he returned to Greenbrier County, where he worked as a school teacher and met his wife Julia. At the WVU College of Law, Judge King graduated Order of the Coif, the law school's highest academic honorary.

As a lawyer, Judge King first served as a law clerk to John A. Field, Jr., then the Chief District Judge for southern West Virginia and later a judge on the Fourth Circuit. Judge King thereafter practiced law in Greenbrier County, served as an Assistant United States Attorney from 1970 to 1974, and practiced at a Charleston law firm from 1975 to 1977. In 1977, Judge King was appointed by President Carter — on the recommendation of Senator Robert C. Byrd — as United States Attorney for the Southern District of West Virginia. When Judge King left that office in 1981, the Charleston Gazette editorial page observed: "Would that the legal profession were sated with lawyers of his integrity and sense of purpose." Judge King then practiced in the Charleston law firm of King, Betts & Allen, later known as King, Allen, Guthrie & McHugh.

During thirty years of law practice, Judge King tried dozens of cases and argued scores of appeals — prosecuting and defending criminal cases, and representing plaintiffs and defendants in all types of civil proceedings. In a law review article written by Fourth Circuit Judge Blane Michael, it was related that "there was little that Judge King had not done in the practice of law by the time he became a judge."

Judge King, who was recommended for appointment to the Fourth Circuit by Senators Robert Byrd and Jay Rockefeller, has now served on the court of appeals for nineteen years. During that time, he has authored hundreds of opinions, many of which address complex constitutional and criminal law issues.

Bob and Julia King have four children and thirteen grandchildren.

TWENTY YEARS ON THE FOURTH CIRCUIT — TWENTY SELECTED CASES

Robert Bruce King
United States Circuit Judge
for the Fourth Circuit

The 2018 Annual Gathering
of the West Virginia State Bar
The Greenbrier
April 9, 2018

(1) *Kolbe v. Hogan*, 849 F.3d 114 (4th Cir. 2017) (King, J., writing for the en banc majority) (concluding that the assault weapons and large-capacity magazines subject to a Maryland ban are not protected by the Second Amendment, and that, even if they were, the ban would survive intermediate scrutiny), *cert. denied*, 138 S. Ct. 469 (2017).

> "Put simply, we have no power to extend Second Amendment protection to the weapons of war that the *Heller* decision explicitly excluded from such coverage." *Kolbe*, 849 F.3d at 121.

(2) *United States v. Basham*, 789 F.3d 358 (4th Cir. 2015), and *United States v. Fulks*, 683 F.3d 512 (4th Cir. 2012) (King, J., writing for the unanimous panels) (affirming the denial of 28 U.S.C. § 2255 motions to vacate the federal death sentences of Chadrick Fulks and Brandon Basham, the murderers of 19-year-old Marshall University student Samantha Burns and 44-year-old Alice Donovan of South Carolina), *cert. denied*, 136 S. Ct. 1449 (2016) and 134 S. Ct. 52 (2013).

> "The federal charges in South Carolina related to the abduction and murder of Alice Donovan on November 14, 2002, in the course of a multistate crime spree engineered by Fulks and . . . Basham, following their escape from a Kentucky jail. Three days prior to Donovan being carjacked, kidnapped, and killed, Samantha Burns suffered the same fate in West Virginia at the hands of Fulks and Basham." *Fulks*, 683 F.3d at 515.
>
> *See also United States v. Fulks*, 454 F.3d 410 (4th Cir. 2006) (King, J. writing for the panel majority) (detailing Basham and Fulks's horrendous crime spree and affirming Fulks's death sentence on direct appeal), *cert. denied*, 127 S. Ct. 3002 (2007).

(3) *Boyer-Liberto v. Fontainebleau Corp.*, 786 F.3d 264 (4th Cir. 2015) (King, J., writing for the en banc majority) (recognizing that an isolated, but extremely serious, incident of harassment can create a Title VII hostile work environment, and that an employee is protected from retaliation when she reports an isolated incident of harassment that is physically threatening or humiliating, even if a hostile work environment is not engendered by that incident alone).

> "[W]e seek to promote the hope and expectation — ingrained in our civil rights laws and the Supreme Court decisions interpreting them — that employees will report harassment early, so that their employers can stop it before it rises to the level of a hostile environment." *Boyer-Liberto*, 786 F.3d at 288.
>
> *See also Jordan v. Alternative Resources Corp.*, 458 F.3d 332 (4th Cir. 2006) (King, J., dissenting) (advocating principles eventually adopted in *Boyer-Liberto*), *cert. denied*, 127 S. Ct. 2036 (2007); *Jordan v. Alternative Resources Corp.*, 467 F.3d 378 (4th Cir. 2006) (King, J., dissenting from the denial of rehearing en banc on a 5-5 vote).

(4) *United States v. Abramski*, 706 F.3d 307 (4th Cir. 2013) (King, J., writing for the unanimous panel) (affirming the convictions of a straw purchaser of a Glock 19 handgun even though the actual buyer was legally entitled to purchase the firearm), *aff'd*, 134 S. Ct. 2259 (2014).

> "In sum, the assertion that Abramski was the actual buyer of the Glock 19 handgun was a false and fictitious answer to question 11.a. of the ATF Form 4473, and that false statement was material to the lawfulness of the Virginia sale of the handgun. Moreover, the identity of the actual purchaser . . . was a fact required to be maintained by the Virginia firearms dealer that sold the firearm." *Abramski*, 706 F.3d at 317.

(5) *United States v. Whitfield*, 695 F.3d 288 (4th Cir. 2012) (King, J., writing for the unanimous panel) (affirming a would-be bank robber's conviction of forced accompaniment while evading apprehension, where the fleeing defendant broke into a home and directed its elderly occupant to go into her residence's computer room), *aff'd*, 135 S. Ct. 785 (2015).

> "Although Whitfield required Mrs. Parnell to accompany him for only a short distance within her own home, and for a brief period, no more is required to prove that a forced accompaniment occurred." *Whitfield*, 695 F.3d at 311.

(6) *United States v. Dire*, 680 F.3d 446 (4th Cir. 2012) (King, J., writing for the unanimous panel) (affirming the piracy convictions of five Somalis for their violent but fruitless attack on the USS Nicholas in the Indian Ocean, after rejecting their contention that piracy as defined by the law of nations is limited by an 1820 Supreme Court decision to robbery at sea), *cert. denied*, 133 S. Ct. 982 (2013).

> "The defendants would have us believe that, since [1820], the United States' proscription of general piracy has been limited to 'robbery upon the sea.' But that interpretation of our law would render it incongruous with the modern law of nations and prevent us from exercising universal jurisdiction in piracy cases." *Dire*, 680 F.3d at 468-69.
>
> *See also United States v. Said*, 680 F.3d 374 (4th Cir. 2012) (King, J., writing for the unanimous panel) (relying on *Dire* to reinstate piracy charges against defendants who fired on, but did not seize or otherwise rob, the USS Ashland in the Gulf of Aden), *cert. denied*, 133 S. Ct. 982 (2013); *United States v. Said*, 798 F.3d 182 (4th Cir. 2015) (King, J., writing for the unanimous panel) (affirming the defendants' convictions and concluding that mandatory life sentences for piracy, as applied to them, do not contravene the Eighth Amendment), *cert. denied*, 136 S. Ct. 2448 (2016).

(7) *Elmore v. Ozmint*, 661 F.3d 783 (4th Cir. 2011) (King, J., writing for the panel majority) (awarding 28 U.S.C. § 2254 habeas corpus relief to a mentally challenged South Carolina inmate who had been behind bars for more than thirty years, mainly on death row, for the rape and murder of an elderly woman who had employed him as a handyman).

> "Having scrutinized volumes of records of Elmore's three trials and his state [postconviction relief] proceedings, we recognize that there are grave questions about whether it really was Elmore who murdered Mrs. Edwards. And we are constrained to conclude — notwithstanding the demanding strictures of § 2254(d) — that Elmore is entitled to habeas corpus relief on his Sixth Amendment claim of ineffective assistance of counsel premised on his trial lawyers' blind acceptance of the State's forensic evidence. All told, Elmore's is one of those exceptional cases of extreme malfunctions in the state criminal justice systems where § 2254 may appropriately be used to remedy injustice." *Elmore*, 661 F.3d at 786 (internal quotation marks omitted).

(8) *Tice v. Johnson*, 647 F.3d 87 (4th Cir. 2011) (King, J., writing for the unanimous panel) (affirming the district court's award of habeas corpus relief to one of the "Norfolk Four" — four men who claim they were coerced by police into falsely confessing to a gruesome rape and murder — on the ground that his lawyers rendered ineffective assistance by failing to move to suppress his confession for being unlawfully obtained after he invoked the right to remain silent).

> "There is simply nothing we can discern from the record that would excuse the defense team's failure to move to suppress Tice's confession. The error was of sufficient magnitude that we cannot help but conclude that counsel's performance in this singular instance was constitutionally deficient within the meaning of *Strickland*. Our only reluctance in so saying is that, based on our review of the record, the assistance provided Tice by [his lawyers] throughout both trials and the first appeal was otherwise laudably effective and competent. However, even an isolated error can support an ineffective-assistance claim if it is sufficiently egregious and prejudicial. Such is the case here." *Tice*, 647 F.3d at 106 (internal quotation marks omitted).

(9) *Snyder v. Phelps*, 580 F.3d 206 (4th Cir. 2009) (King, J., writing for the panel majority) (reversing a $5 million judgment against the notorious Westboro Baptist Church and three of its Phelps family members because their written "Epic" naming a Marine killed in Iraq and picketing near his funeral were protected by the First Amendment), *aff'd*, 562 U.S. 443 (2011).

> "Notwithstanding the distasteful and repugnant nature of the words being challenged in these proceedings, we are constrained to conclude that the Defendants' signs and Epic are constitutionally protected. To paraphrase our distinguished colleague Judge Hall, judges defending the Constitution 'must sometimes share [their] foxhole with scoundrels of every sort, but to abandon the post because of the poor company is to sell freedom cheaply. It is a fair summary of history to say that the safeguards of liberty have often been forged in controversies involving not very nice people.'" *Snyder*, 580 F.3d at 226 (quoting *Kopf v. Skyrm*, 993 F.2d 374, 380 (4th Cir. 1993)).

(10) *Collins v. Pond Creek Mining Co.*, 468 F.3d 213 (4th Cir. 2006) (King, J., writing for the panel majority) (with respect to a widow's Black Lung Benefits Act claim, according collateral estoppel effect to an earlier administrative ruling in favor of her then-living husband).

> "[A] coal miner's widow seeking survivor's benefits under the Black Lung Act may generally rely on the doctrine of offensive nonmutual collateral estoppel to establish that, as a result of his work in the mines, her deceased husband had developed pneumoconiosis." *Collins*, 468 F.3d at 222-23.

(11) *Ridpath v. Board of Governors Marshall University*, 447 F.3d 292 (4th Cir. 2006) (King, J., writing for the panel majority) (affirming the denial of qualified immunity to Marshall officials at the dismissal stage of proceedings brought by an employee who claimed he was made a scapegoat for the University's NCAA rules violations).

> "[T]he allegations of Ridpath's Amended Complaint . . . establish that the Administrators publicly made a false charge against Ridpath, connoting dishonesty and other serious character defects on his part, in the course of subjecting him to a significant demotion to a position outside his field of choice. Moreover, it is undisputed that the Amended Complaint reflects that Ridpath was not provided notice or an opportunity to be heard with respect to this charge." *Ridpath*, 447 F.3d at 313.

(12) *Robinson v. Polk*, 438 F.3d 350 (4th Cir. 2006) (King, J., dissenting in part) (maintaining that a North Carolina death row inmate deserved an evidentiary hearing on the claim that his jury's death penalty deliberations were improperly influenced by a juror who read aloud an "an eye for an eye" passage from a Bible secretly provided by the court bailiff), *cert. denied*, 127 S. Ct. 514 (2006).

> "This appeal presents an important Sixth Amendment issue, and I write separately because it is being wrongly decided. The Sixth Amendment entitles an accused to the sacrosanct right of a fair trial before an impartial jury, a mandate that goes to the fundamental integrity of all that is embraced in the constitutional concept of trial by jury. And when a jury's deliberations have been contaminated by an improper external influence — even if that influence relates to the Bible of England's first Stuart King — public confidence in our judicial system is undermined and the jury's verdict must not be enforced." *Robinson*, 438 F.3d at 368 (internal quotation marks omitted).
>
> *See also Robinson v. Polk*, 444 F.3d 225 (4th Cir. 2006) (King, J., dissenting from the denial of rehearing en banc on a 9-4 vote).

(13) *Ohio Valley Environmental Coalition v. Bulen*, 437 F.3d 421 (4th Cir. 2006) (King, J., dissenting from the denial of rehearing en banc on a 5-3 vote) (contesting the panel's unanimous decision upholding a general permit promulgated by the Army Corps of Engineers in favor of mountaintop coal mining projects).

> "This case is of exceptional importance to the nation and, in particular, to the states in the Appalachian region. The Appalachian mountains, the oldest mountain chain in the world, are one of the nation's richest, most diverse, and most delicate ecosystems, an ecosystem that the mountaintop coal mining authorized by the Corps' general permit may irrevocably damage or destroy." *Ohio Valley Envtl. Coal.*, 437 F.3d at 424.

(14) *Wachovia Bank, N.A. v. Schmidt*, 388 F.3d 414 (4th Cir. 2004) (King, J., dissenting) (rejecting the panel majority's conclusion that, for purposes of diversity jurisdiction, a national bank is a citizen of every state in which it maintains a branch), *rev'd*, 546 U.S. 303 (2006) (agreeing with Judge King that a national bank is instead a citizen only of the state in which its main office is located).

> "The relevant history of our national banks reveals that Congress intended for such banks to enjoy the same access to federal courts as that accorded other banks and corporations." *Wachovia Bank*, 388 F.3d at 434.
>
> *See also Wachovia Bank, N.A. v. Schmidt*, 445 F.3d 762 (4th Cir. 2006) (King, J., writing for the unanimous panel on remand from the Supreme Court) (recognizing diversity jurisdiction in this matter and affirming the district court's denial of Wachovia Bank's petition to compel arbitration).

(15) *Mellen v. Bunting*, 327 F.3d 355 (4th Cir. 2003) (King, J., writing for the unanimous panel) (concluding that the state-operated Virginia Military Institute's daily "supper prayer" violated the Establishment Clause of the First Amendment), *cert. denied*, 124 S. Ct. 1750 (2004).

> "Although VMI's cadets are not children, in VMI's educational system they are uniquely susceptible to coercion. VMI's adversative method of education emphasizes the detailed regulation of conduct and the indoctrination of a strict moral code. Entering students are exposed to the "rat line," in which upperclassmen torment and berate new students, bonding new cadets to their fellow sufferers and, when they have completed the 7-month experience, to their former tormentors. At VMI, even upperclassmen must submit to mandatory and ritualized activities, as obedience and conformity remain central tenets of the school's educational philosophy. In this atmosphere, General Bunting reinstituted the supper prayer in 1995 to build solidarity and bring the Corps together as a family. In this context, VMI's cadets are plainly coerced into participating in a religious exercise. Because of VMI's coercive atmosphere, the Establishment Clause precludes school officials from sponsoring an official prayer, even for mature adults." *Mellen*, 327 F.3d at 371-72 (internal quotation marks omitted).

(16) *Monroe v. Angelone*, 323 F.3d 286 (4th Cir. 2003) (King, J., writing for the unanimous panel) (affirming the district court's award of habeas corpus relief to a Virginia woman who was convicted of the first-degree murder of her wealthy, philandering boyfriend by a single gunshot wound to the head).

> "This murder prosecution was closely contested, and the Commonwealth's evidence of premeditation and malice, essential elements of first-degree murder in Virginia, was particularly sparse. In attempting to portray Monroe as a cold-blooded, calculating killer, the Commonwealth relied primarily on the testimony of Zelma Smith, who told the jury that Monroe sought to obtain an untraceable handgun about a year before Burde's death. Significantly, the Commonwealth suppressed several evidentiary items that would have severely damaged the credibility of this crucial witness. The suppression of this *Brady* evidence undermines our confidence in the verdict, and there is a reasonable probability that, had the prosecution properly disclosed exculpatory material, the jury would not have convicted Monroe of first-degree murder." *Monroe*, 323 F.3d at 291.

(17) *Belk v. Charlotte-Mecklenburg Board of Education*, 269 F.3d 305 (4th Cir. 2001) (Diana Gribbon Motz, J., and King, J., jointly writing separately) (criticizing the en banc majority for upholding the district court's determination that the Charlotte-Mecklenburg Board of Education ("CMS") had achieved unitary status in every respect, requiring its decades-old, federal-court-ordered and -supervised plan for school desegregation to be dissolved), *cert. denied*, 122 S. Ct. 1537 (2002) and 122 S. Ct. 1538 (2002).

> "Nothing yet demonstrates that CMS has eliminated all vestiges of the unlawful discrimination that has long permeated its school system. In holding to the contrary, the majority has only succeeded here in dashing the hopes of the citizens of Mecklenburg County, particularly those of African-American descent, who have long fought for the fair and equitable implementation of the desegregation plan approved by Judge McMillan some thirty years ago. These successive generations of parents and children have been slowly starved by a well-meaning — but irresolute — governing body, whose sins have been absolved by the court below (and now by a majority of this Court) without anything but the most cursory examination. Although CMS has clearly achieved unitary status in certain respects, there remain several areas of primary concern that have not been subjected to anything approaching a proper constitutional analysis. We deplore, and believe the Court itself may one day regret, the refusal of a present majority to recognize this." *Belk*, 269 F.3d at 371.

(18) *Bell Atlantic Maryland, Inc. v. MCI Worldcom, Inc.*, 240 F.3d 279 (4th Cir. 2001) (King, J., dissenting) (asserting, contrary to the panel majority and in reliance on a 1999 decision of Justice Scalia, that federal courts may review the decisions of state regulators that enforce interconnection agreements under the Telecommunications Act), *vacated*, *Verizon Maryland Inc. v. Public Service Commission*, 535 U.S. 635 (2002) (Scalia, J.) (similarly rejecting the panel majority's decision).

> "It can hardly be stated more convincingly than Justice Scalia already has: '[T]here is no doubt . . . that if the federal courts believe a state commission is not regulating in accordance with federal policy they may bring it to heel.' In defiance of Justice Scalia's clear admonition, the majority injects equivocation where once there was certitude. Where order once reigned, chaos now impinges." *Bell Atl. Md.*, 240 F.3d at 309 (quoting *AT&T Corp. v. Iowa Utils. Bd.*, 525 U.S. 366, 379 n.6 (1999)).
>
> *See also BellSouth Telecommunications, Inc. v. North Carolina Utilities Commission*, 240 F.3d 270 (4th Cir. 2001) (King, J., dissenting), *vacated*, 122 S. Ct. 2287 (2002).

(19) *United States v. Rhynes*, 218 F.3d 310 (4th Cir. 2000) (King, J., announcing the judgment of the en banc court) (remanding for a new trial where the district court excluded a defendant's sole supporting witness for a sequestration violation).

> "Judgment vacated and new trial awarded by published opinion. Judge KING announced the judgment of the Court, in which Judge WIDENER, Judge WILKINS, Judge LUTTIG, Judge WILLIAMS, Judge MICHAEL, Judge DIANA GRIBBON MOTZ, and Judge TRAXLER joined; wrote the opinion of the Court with respect to Part III, in which Judge WILKINS, Judge WILLIAMS, Judge MICHAEL, Judge DIANA GRIBBON MOTZ, and Judge TRAXLER joined; wrote the opinion of the Court with respect to Parts IV and V, in which Judge WIDENER, Judge WILKINS, Judge LUTTIG, Judge WILLIAMS, Judge MICHAEL, Judge DIANA GRIBBON MOTZ and Judge TRAXLER joined; and wrote an opinion with respect to Parts I and II in which Judge WIDENER (except perhaps for a footnote), Judge LUTTIG (in part), Judge MICHAEL, and Judge DIANA GRIBBON MOTZ joined. Judge WIDENER wrote an opinion concurring in part and concurring in the judgment. Judge WILKINS wrote an opinion concurring in part and concurring in the judgment, in which Judge WILLIAMS and Judge TRAXLER joined. Judge LUTTIG wrote an opinion concurring in part and concurring in the judgment. Chief Judge WILKINSON wrote a dissenting opinion, in which Judge NIEMEYER joined. Judge NIEMEYER wrote a dissenting opinion, in which Chief Judge WILKINSON joined and in which Judge TRAXLER joined with respect to Parts I and II." *Rhynes*, 218 F.3d at 312.

(20) *Spriggs v. Diamond Auto Glass*, 165 F.3d 1015 (4th Cir. 1999) (*Spriggs I*) (King, J., writing for the unanimous panel) (reinstating the African-American plaintiff's claim under 42 U.S.C. § 1981 that his former employer subjected him to severe racial harassment and retaliation amounting to "forced termination" of his at-will employment), and 242 F.3d 179 (4th Cir. 2001) (*Spriggs II*) (King, J., again writing for the unanimous panel) (vacating the district court's award of summary judgment to the employer on the § 1981 and consolidated Title VII claims of hostile work environment, constructive discharge, and retaliation, where the evidence reflected, inter alia, that the plaintiff's supervisor habitually called the plaintiff a "monkey," "dumb monkey" and "n----r").

> "Far more than a mere offensive utterance, the word 'n----r' is pure anathema to African Americans. Perhaps no single act can more quickly alter the conditions of employment and create an abusive working environment than the use of an unambiguously racial epithet such as 'n----r' by a supervisor in the presence of his subordinates. [The supervisor's] constant use of the word 'monkey' to describe African Americans was similarly odious. To suggest that a human being's physical appearance is essentially a caricature of a jungle beast goes far beyond the merely unflattering; it is degrading and humiliating in the extreme." *Spriggs II*, 242 F.3d at 185 (internal quotation marks omitted).

TWENTY YEARS ON THE FOURTH CIRCUIT — APPENDIX

M. Blane Michael, *Robert C. Byrd and the Fourth Circuit Court of Appeals: An Addendum Respecting Judge Robert Bruce King*, 109 W. Va. L. Rev. 51 (2006)

Reprinted with permission from the West Virginia Law Review

ROBERT C. BYRD AND THE FOURTH CIRCUIT COURT OF APPEALS: AN ADDENDUM RESPECTING JUDGE ROBERT BRUCE KING

*M. Blane Michael**

Robert Bruce King was born in 1940 in White Sulphur Springs, Greenbrier County, West Virginia.[1] Known for his love of West Virginia, dedication to his family, and outstanding legal ability, Judge King has been serving on the United States Court of Appeals for the Fourth Circuit since 1998. Judge King was among the first group of West Virginians that Senator Robert C. Byrd and Senator John D. Rockefeller IV recommended for federal appointments when President Clinton assumed office in 1993.[2] As Senator Byrd observed at Judge King's investiture, "Robert Bruce King is a man who is eminently qualified to wear the black robe and assume the weighty responsibilities of a federal judge."[3]

Last spring the *West Virginia Law Review* published a tribute to Senator Byrd. The issue included an article by Judge King recounting the lives and careers of the Fourth Circuit judges appointed during Senator Byrd's tenure in the Senate.[4] Judge King declined to write about himself. I write to correct the omission because Judge King offers a rich and admirable story that should be told.

Judge King grew up in Organ Cave (Greenbrier County, West Virginia), where, until eighth grade, he attended a three-room school.[5] His father passed away in April 1950, when he was only ten years old, leaving his mother, Gladys

---

* Circuit Judge, United States Court of Appeals for the Fourth Circuit. I thank four of my law clerks, Elizabeth Mazur, Margaret Welles Renner, Indraneel Sur (2005-2006), and Charles Trumbull (2006-2007) for their help in preparing this article.

1 Judge King is of Scottish ancestry and immensely proud of it. He is a member of the Bruce Family, which traces its lineage to Robert the Bruce, a fourteenth-century Scottish king.

2 The senators asked the Clinton administration to allocate a third seat on the Fourth Circuit to West Virginia and recommended that the President nominate Judge King to fill that seat. *See* Press Release, Office of U.S. Sen. Robert C. Byrd (Mar. 8, 1993) (on file with author). West Virginia did not get the extra seat, but Judge King was later nominated to the Fourth Circuit in 1998.

3 Sen. Robert C. Byrd (D - W. Va.), Investiture Ceremonies for Robert Bruce King as United States Circuit Judge for the Fourth Circuit, United States Court of Appeals for the Fourth Circuit Special Ceremonial Session at the United States Courthouse, Charleston, West Virginia 49-50 (Oct. 23, 1998) (transcript on file with author) [hereinafter King Investiture Ceremonies].

4 Robert Bruce King, *Robert C. Byrd and the Fourth Circuit Court of Appeals*, 108 W. VA. L. REV. 607 (2006).

5 Judge Robert B. King, King Investiture Ceremonies, *supra* note 3, at 62.

Holyman King, a widow at the age of thirty-one. Mrs. King "centered her universe around her family," raising Judge King and his two siblings while working in the kitchen at The Greenbrier's golf and tennis club.[6] Although she herself never graduated from high school, Mrs. King constantly encouraged her children in their studies, emphasizing that hard work and a good education were the best routes to success in life.[7] The King children took their mother's advice to heart.

Judge King's budding advocacy skills were recognized when he was only a 15-year-old sophomore at Greenbrier High School. Representing his local chapter of the Future Farmers of America (FFA), Judge King won an FFA-sponsored public speaking contest with a speech entitled, "Let's Keep Our Soil at Home."[8] His award for this honor was a $25 savings bond.[9] The role that farming played in Judge King's young life was quite secondary, however, to the role that "the ancient and honorable game of golf"[10] played, and continues to play. As a boy Judge King worked as a caddie at the famed Greenbrier resort where, according to the judge, he "learned life literally from the bottom up."[11]

Judge King brought his passion for golf to West Virginia University (WVU), where he played for three years on the varsity men's golf team. He earned a letter all three years and was captain of the team in 1961.[12] During his years on the golf team Judge King forged a close relationship with his coach, Ira Errett Rodgers, whom Judge King, with great passion and admiration, still considers "West Virginia's finest athlete."[13] Judge King fondly remembers leading his team to victory against the University of Pittsburgh in 1961, the year he served as team captain. "I vividly recall Coach Rodgers sitting with us after the match, on the porch at the old clubhouse [at the Morgantown Country Club] on top of [the] hill — literally crying with joy."[14] (That season turned out to be Coach Rodgers's last one. "He was, sadly, suffering from the cancer that took his life in early 1963."[15])

---

6 Press Release, West Virginia University, Alumni Endow WVU Scholarship to Honor Their Mother's Commitment to Her Children (July 31, 2003), *available at* http://hermes.as.wvu.edu/New_Folder/newsroom/newsreleases/2003/July/kingen.html.

7 *Id.*

8 *Bobby King Wins FFA Public Speaking Contest for Greenbrier Valley Group*, BECKLEY POST-HERALD, Apr. 17, 1955. The speech did not advocate isolationism, as its clever title might suggest. Rather, it warned of the perils of soil erosion.

9 *Id.*

10 Warren Upton, King Investiture Ceremonies, *supra* note 3, at 21.

11 Judge Robert B. King, King Investiture Ceremonies, *supra* note 3, at 62.

12 Letter from William C. Field to author (July 19, 2006) (on file with author) [hereinafter Field Letter].

13 Judge Robert B. King, Remarks at the Mountain Mush & Milk Banquet 4-7 (Oct. 21, 2005) (on file with author).

14 *Id.* at 7.

15 *Id.*

After earning a Bachelor of Arts degree from WVU in 1961, Judge King entered active duty as an officer in the United States Air Force, serving in the Office of Special Investigations. During his Air Force years he played golf in numerous armed services tournaments, "where he competed against many future PGA Tour professionals, including Orville Moody, who won the 1969 U.S. Open."[16] After his discharge from the service in 1964 Judge King returned to rural Greenbrier County, where he worked as a school teacher. There he met another teacher, Julia Kay Doak, whom he married on April 16, 1965. The following year Judge King and Julia returned to Morgantown, where he attended the WVU College of Law. While in law school he was a member of the *West Virginia Law Review* and served as president of the Student Bar Association. He graduated Order of the Coif in 1968 and was awarded the Patrick Duffy Koontz Scholarship in recognition of his academic excellence, character, and leadership potential.[17]

As he was preparing to graduate, Judge King was "exceptionally lucky" in landing what turned out to be one of the most important jobs of his life: a clerkship with then U.S. District Judge John A. Field, Jr. in Charleston, West Virginia. More than thirty-five years later, Judge King attributed his success as a lawyer to Judge Field's willingness to "give [him] a chance."[18] As Judge King said, "Judge [Field], simply put, guided me through my life."[19] Also important to Judge King was Judge Field's attachment to the "ancient and honorable game of golf."[20] As Judge King recalls, "On several occasions, both during and after my clerkship with Judge Field, he reminded me that golf was the sole and only reason he had ever hired me to be one of his law clerks."[21] Judge Field's son, William C. Field, recalls how that hiring came about: one day in the spring of 1968, Judge Field

> was about to tee off on the Old White Course at the Greenbrier Hotel when Bob's stepfather [Buster Gregory], the Starter on

---

[16] Field Letter, *supra* note 12. Judge King retains his formidable skill as a golfer, scoring consistently in the seventies. His success, according to his friend and golfing companion Thomas R. Goodwin, "is based on his ability to hit the ball in the middle of the club face with a controlled and repeatable swing." Memorandum from Thomas R. Goodwin to author (Aug. 10, 2006) (on file with author). Other friends "describe [Judge King's] swing as being so smooth and sweet that it looks like honey pouring from a jar." Field Letter, *supra* note 12.

[17] WVU Alumni - Robert B. King, http://alumni.wvu.edu/about/board/bio/robert_king.

[18] Judge Robert B. King, Portrait Unveiling in Honor of Honorable John A. Field, Jr., United States Circuit Judge, United States Court of Appeals for the Fourth Circuit Sitting En Banc at Richmond, Virginia at 8 (Sept. 24, 2003) (transcript on file with author).

[19] *Id.*

[20] *Id.* at 9.

[21] *Id.* at 10.

> the Old White Course, told Judge Field that he had a pretty bright stepson who was about to graduate from law school. Judge Field told him to have his stepson call . . . about a job opening as [the judge's] law clerk. Bob called and an interview took place later that summer. Judge Field recounted many times how it took only a few minutes for him to decide Bob was going to be his law clerk. As Judge Field used to tell it, you could instantly see the intellect and quickness of Bob's mind just by looking at the spark in his eyes. Bob was hired on the spot.[22]

After his clerkship Judge King went on to practice law in Lewisburg, West Virginia, with the firm of Haynes & Ford.[23] Within a year he returned to Charleston to serve as Assistant United States Attorney (AUSA) in the Southern District of West Virginia.[24] He served in that position from 1970 until 1974,[25] distinguishing himself as a tough prosecutor. One of his most significant prosecutions as an AUSA involved a scheme to bribe a juror in the 1968 criminal trial of former West Virginia Governor William Wallace Barron and several associates, who were accused of corruption in state contracting.[26] During that 1968 trial the wife of the sequestered jury foreman approached Governor Barron's wife and sought cash in exchange for acquittals. Mrs. Barron relayed the bribery solicitation to the Governor, who set in motion a chain of events leading to the delivery of a $25,000 cash bribe to the jury foreman's wife.[27] The jury acquitted Governor Barron but convicted four of his co-defendants.[28] Judge King became an AUSA in time to take an instrumental role in the jury bribery investigation, which began in late 1970. Judge King and his fellow prosecutors, U.S. Attorney W. Warren Upton and Department of Justice lawyer Charles F.C. Ruff, cracked the case in February 1971 when the jury foreman confessed to accepting the bribe.[29] In due course Governor Barron pled guilty, was sentenced to a prison term of twelve years, and became a government witness (examined by Judge King) in the trials of two others indicted in the jury bribery scheme.[30] The Barron case was not the only one in which Judge King confronted the politically powerful. As an AUSA he also prosecuted and convicted five Logan

---

22 Field Letter, *supra* note 12.

23 Response of Robert Bruce King to Questionnaire for Judicial Nominees of the Committee of the Senate Judiciary Committee at 14 (July 3, 1998) [hereinafter King Questionnaire].

24 *Id.*

25 *Id.* at 14-15.

26 *Id.* at 26.

27 *Id.*

28 *Id.* at 26-27.

29 *Id.*

30 *Id.*

County, West Virginia, public officials on civil rights charges relating to vote fraud and election theft.[31]

In 1974 Judge King returned to private practice at the Charleston law firm of Spilman, Thomas, Battle & Klostermeyer, where he was a partner from 1975 until mid-1977.[32] It surprised no one when Senator Byrd in 1977 recommended that the 37-year-old former AUSA be appointed United States Attorney for the Southern District of West Virginia. President Carter adopted Senator Byrd's recommendation, and the Senate confirmed Judge King for that post.[33] As United States Attorney, Judge King burnished his reputation as a prosecutor who fearlessly took on "explosive, potentially political cases,"[34] "ceaselessly waged war" against white collar crime and public corruption,[35] and was "invariably . . . more interested in justice than in headlines."[36] For instance, from 1978 through early 1980 Judge King led an extensive criminal investigation of the American liquor industry and the Alcohol Beverage Control Commission of West Virginia.[37] This investigation resulted in the prosecution and conviction of more than forty individuals and corporations on various charges, including commercial bribery, mail fraud, extortion, and Racketeer Influenced and Corrupt Organizations Act (RICO) violations.[38] Most of these convictions were based on guilty pleas, but Judge King himself was the lead prosecutor at the trials of two of the defendants. Both cases resulted in convictions, which were later affirmed by the Fourth Circuit.[39] Not surprisingly, Judge King's tenacity as a prosecutor at times exposed him to death threats,[40] but he persevered. When Judge King left the office, the *Charleston Gazette* editorial page observed: "Would that the legal profession were sated with lawyers of his integrity and sense of purpose."[41]

That praise was later echoed by Judge K. K. Hall, who lauded Judge King's skill and intelligence as a prosecutor. Judge Hall, who presided over dozens of cases in which Judge King was an advocate, said that "[i]t was just

---

31 *Id.* at 28-29.

32 *Id.* at 15.

33 Paul Akers, *Court King: Experience Key Asset for New Prosecutor*, CHARLESTON DAILY MAIL, July 15, 1977.

34 *King Looks Back on Four Years as U.S. Attorney*, CHARLESTON DAILY MAIL, Jan. 12, 1981, at 1B.

35 *Needed: A Good Lawyer*, CHARLESTON GAZETTE, Mar. 11, 1981, at 6A.

36 Editorial, CHARLESTON DAILY MAIL, Mar. 2, 1981, at 4A.

37 King Questionnaire, *supra* note 23, at 34-35.

38 *Id.*

39 United States v. Barber, 668 F.2d 778 (4th Cir. 1982); United States v. Margolis, 612 F.2d 1311 (4th Cir. 1979).

40 *King Looks Back on Four Years as U.S. Attorney*, *supra* note 34, at 1B.

41 *Needed: A Good Lawyer*, *supra* note 35, at 6A.

magnificent the way [Judge King] tried a case."[42] According to Judge Hall, Judge King was extraordinarily thorough and adept as a trial lawyer. This respect was reciprocal, for Judge King admired Judge Hall's "unmatched dignity," "unimpeachable integrity," sense of humor, and long service to West Virginia.[43] (It was a testament to their mutual respect and close friendship that Judge Hall, despite struggling with a painful fatal illness at the time, served as de facto master of ceremonies at Judge King's investiture as a Fourth Circuit judge and administered the oath of office.[44] At the close of this ceremony, Judge King "[could not] thank Judge Hall enough" for his guidance and support.[45])

In 1981 Judge King returned to private practice, with a continuing commitment to quality lawyering and the highest ethical standards. He was instrumental in founding the law firm of King Betts & Allen (now called Allen Guthrie McHugh & Thomas), where he served as managing partner from 1981 to 1993 and from 1997 until his judicial appointment.[46] At his firm Judge King continued to represent high-profile clients. For example, he served as defense counsel for Governor Rockefeller in several federal civil rights suits brought against the Governor and officials of the West Virginia Department of Highways by former department employees, who claimed they were fired for political reasons.[47] Early in the litigation the district court denied the Governor and certain other defendants qualified immunity. Judge King argued the appeal of this denial in the Fourth Circuit, which held by a divided vote that it did not have jurisdiction at that stage of the case.[48] Despite this setback, Judge King succeeded in his representation of the Governor. During the trial of the lead case in April and May 1986, the district court directed a verdict in Governor Rockefeller's favor, and the other cases against him were dismissed.[49]

Throughout his years in private practice Judge King devoted considerable time to the advancement of the legal profession. From early 1976 to the summer of 1977, while he was at the Spilman firm, Judge King served as counsel for the West Virginia State Bar's Committee on Legal Ethics, which handles lawyer discipline in the state.[50] In that capacity he investigated complaints alleging violations of the rules of professional responsibility, and he represented the committee in disciplinary proceedings before the Supreme Court of Appeals

---

42 Judge K. K. Hall, King Investiture Ceremonies, *supra* note 3, at 36.

43 Judge Robert B. King, Memorial Ceremony in Honor of The Honorable K. K. Hall, United States Court of Appeals for the Fourth Circuit 9 (Oct. 27, 1999) (transcript on file with author).

44 *Id.* at 10.

45 King Investiture Ceremonies, *supra* note 3, at 61, 65.

46 King Questionnaire, *supra* note 23, at 3.

47 *Id.* at 40-41.

48 Bever v. Gilbertson, 724 F.2d 1083, 1084-88 (4th Cir. 1984).

49 *See* King Questionnaire, *supra* note 23, at 40-41.

50 *Id.* at 15.

of West Virginia.[51] Judge King later served the West Virginia State Bar as a member of its governing board from 1981 to 1984 and as a member of its Committee on Legal Ethics from 1984 to 1987.[52] Judge King was also a member of the Judicial Investigation Commission of West Virginia from 1990 to 1994.[53] This commission investigates complaints against West Virginia judges and gives advice and opinions to judges on matters of professional ethics.[54] In addition, throughout his time in private practice Judge King took on pro bono cases, representing clients who could not afford a lawyer. In 1990 Judge King represented (free of charge) Paul "Butch" Goode, the Wyoming County Prosecuting Attorney.[55] Goode had been a friend of Judge King at WVU, where Goode played on the basketball team and roomed with Jerry West.[56] Goode had financial problems stemming from bad health, a fire, and a divorce, and he was under indictment for failure to file federal income tax returns.[57] Judge King represented Goode at trial, where the government won a conviction.[58] Two years later, while still serving his sentence on home confinement, Goode overwhelmingly won reelection to the office of prosecutor.[59] Local reports were that Judge King's client campaigned from his front porch, waving to potential voters as they passed by.[60]

Judge King also found some time for political activities. In 1982 he served as counsel to Senator Byrd's reelection campaign, providing advice on a number of matters, including what the campaign considered improper advertising tactics by the National Conservative Political Action Committee.[61] In the

---

[51] *Id.* at 52.

[52] *Id.* at 53.

[53] *Id.*

[54] *Id.*

[55] Robert Bruce King, Remarks by the New Judges of the Circuit, 69th Judicial Conference of the United States Judges of the Fourth Circuit 13 (June 25, 1999) (on file with author).

[56] *Id.* at 14.

[57] *Id.* at 13.

[58] *Id.* at 14.

[59] *Id.*

[60] *Id.* Later, when Senators Byrd and Rockefeller recommended Judge King for the Fourth Circuit, Butch Goode sent the judge a letter pledging unqualified support. *Id.* at 15. The letter read:

> King,
>
> I hope you get that job in Richmond. I'll come out for ya, if that'll help, or I'll come out against ya, if that's best.... You don't need my advice, but I'll give it anyway. Read the damn Constitution and always call them as you see 'em.

Id. As the latter portion of this article reveals, Judge King has followed Goode's advice.

[61] Mark Ward, *Leaders Pushing Byrd Re-election Defend Letter to Broadcasters*, CHARLESTON DAILY MAIL, Mar. 10, 1982.

latter stages of the campaign Judge King also served as the repository for the senator's income tax returns and financial statements, making these documents available for public inspection. In addition, in 1983 and 1984 Judge King was counsel to Friends of Jay Rockefeller, the committee responsible for Senator Rockefeller's election campaign.[62] During the same period the judge was also counsel to the West Virginia Democratic Party.[63]

Senator Byrd and Judge King have much in common, beginning with their devotion to family. Senator Byrd recognized this bond at Judge King's investiture when he extended a special wish, based on an old Irish blessing, to the judge, his wife Julia, and their family. It was a wish for "work for your hands, a straight path for your feet, a coin for your purse, sunshine on your windowpane at evening, a song in your treetop at morning, soft rains for your garden, happiness in your hearts, love at your firesides, and God's blessings always."[64] Responding in part to these moving words, Judge King recognized Senator Byrd as the "paramount recipient" of his gratitude.[65]

Senator Byrd and Judge King also share a genuine dedication to the State of West Virginia. In 2001 the state legislature declared Senator Byrd "West Virginian of the Twentieth Century" in recognition of his exceptional service to the state.[66] This service was highlighted recently, in June 2006, when Senator Byrd became the longest-serving Senator in United States history.[67] With this same sense of commitment, Judge King serves West Virginia and its institutions in many ways in addition to his work as a judge. He has strong loyalties and ties to WVU, his alma mater and the state's flagship institution of higher education. Judge King currently sits on the WVU Alumni Association Board of Directors and serves as Vice Chair of the College of Law Alumni Association.[68] He regularly speaks at banquets and ceremonies on campus, cheers (as a letterman in his own right) for the Mountaineers, and has hired a number of WVU law school graduates to serve as his clerks. In 2003 Judge King received the Justitia Officium Award, the College of Law's highest honor.[69]

In a gesture that embodied both love of family and love of WVU, Judge King and his sister, Dean Mary Ellen Mazey, endowed a scholarship at the University in 2003 in honor of their mother's dedication to her children.[70] (Their

---

62 King Questionnaire, *supra* note 23, at 58.

63 *Id.*

64 Sen. Robert C. Byrd, King Investiture Ceremonies, *supra* note 3, at 59-60.

65 Judge Robert B. King, King Investiture Ceremonies, *supra* note 3, at 66.

66 Jim Wallace, *Honor More Than Just Another Nod: Colleagues Say Byrd Acted Differently This Time*, CHARLESTON DAILY MAIL, June 1, 2001, at 13A.

67 Paul J. Nyden, *The Pillar of the Senate, Ten Presidents Later, Byrd Longest-Serving Senator*, CHARLESTON GAZETTE, June 12, 2006, at 1A.

68 WVU Alumni - Robert B. King, *supra* note 17.

69 *Id.*

70 Press Release, West Virginia University, *supra* note 6.

brother, William E. King, passed away in 1995.) Her children's success is testimony to her steadfast commitment to their education. At the time of the endowment's creation, Dean Mazey had earned Bachelor of Arts and Master of Arts degrees from WVU and a Ph.D from the University of Cincinnati; she also served as Dean of the College of Liberal Arts at Wright State University.[71] She is now Dean of the Eberly College of Arts and Sciences at WVU. William had earned his law degree from WVU and had practiced law with distinction in Greenbrier County.[72] The Gladys Holyman King Scholarship is awarded annually to a sophomore enrolled in the Eberly College of Arts and Sciences from Greenbrier County who demonstrates academic promise and needs financial assistance.[73] The endowed scholarship stands as permanent recognition of Mrs. King's dedication to the education of rural youth.

President Clinton nominated Judge King to the Fourth Circuit on June 24, 1998, to the seat vacated when Judge K. K. Hall took senior status.[74] The Senate Judiciary Committee held a hearing on September 9, 1998, to consider the nomination. (Among other nominees considered that day was Judge William B. Traxler, Jr., of South Carolina, our colleague on the Fourth Circuit.)[75] West Virginia's senators, Byrd and Rockefeller, appeared at the hearing to express unqualified support for Judge King's confirmation.[76] Emphasizing Judge King's thirty years of legal experience, Senator Byrd noted that "this long service . . . equips Robert King with the requisite education and experience to serve as a Federal judge, but beyond this valuable experience, he also possesses the kind of deep-seated integrity, strong work ethic, and love of public service that . . . combines to make an outstanding member of the judiciary."[77] Senator Byrd, well-known for his exhaustive knowledge of ancient history,[78] also compared Judge King to Alexander the Great.[79] As Senator Byrd recounted, when a prosecutor came to Alexander to present an indictment, the Macedonian king "would put one hand over one ear and keep that ear closed. He kept that ear closed for the defendant. . . . He wanted to listen to both sides and give both sides equally an opportunity to have his attention. I believe that Bob King will

---

71 *Id.*

72 *Id.*

73 *Id.*

74 144 CONG. REC. S7038 (daily ed. June 24, 1998).

75 *Nominations of Robert B. King, William B. Traxler, Jr. to be United States Circuit Judges; H. Dean Buttram, Jr., Inge Prytz Johnson, Thomas J. Whelan to be United States District Judges*, 105th Cong. 1 (1998) [hereinafter King Nomination Hearing].

76 *Id.* at 7, 10.

77 *Id.* at 9 (statement of Sen. Robert C. Byrd).

78 *See* M. Blane Michael, *The Power of History to Stir a Man's Blood: Senator Robert C. Byrd in the Line Item Veto Debate*, 108 W. VA. L. REV. 593, 595 (2006) (describing influence of Senator Byrd's "extensive study of the classics of Western civilization" on his view of governmental powers).

79 King Nomination Hearing, *supra* note 75, at 9 (statement of Sen. Robert C. Byrd).

be the same [kind of judge]."[80] For his part, Senator Rockefeller celebrated Judge King's dedication to public service. "In West Virginia, it is interesting that people often talk about the work ethic of our people," Senator Rockefeller noted.[81] "Bob King simply works hard. He is incredibly fair. He is humble, with really very little to be humble about," Senator Rockefeller added.[82] Acting upon the favorable recommendation of the Judiciary Committee, the full Senate confirmed Judge King to the Fourth Circuit on October 8, 1998.[83]

Senator Byrd and Senator Rockefeller summarized nominee King's stellar record with complete accuracy. Few lawyers have ever come to the federal bench with broader experience than Robert Bruce King. During his thirty years of practice he tried over 120 cases and argued scores of appeals.[84] He spent about a third of his career as a federal prosecutor, prosecuting defendants in a wide variety of criminal cases, including those involving public corruption, election fraud, organized crime, drug trafficking, and fraud.[85] In private practice Judge King also handled a considerable number of criminal cases. He represented defendants charged with assorted offenses, including white collar crimes, RICO, tax fraud, mail fraud, criminal antitrust violations, and homicide.[86] He represented his share of indigent defendants, with those representations earning him a state-paid fee of $50 per felony case at the start of his career.[87] The range of cases and matters handled by Judge King on the civil side is no less impressive. He represented both plaintiffs and defendants in innumerable civil proceedings, including those involving wrongful death, personal injury, products liability, professional malpractice, civil rights, securities, and employment benefits law.[88] He also prepared title reports as a young lawyer.[89] In short, there was little that Judge King had not done in the practice of law by the time he became a judge.

Judge King's broad-scale experience makes the Fourth Circuit a much richer place. Of the judges sitting on the Fourth Circuit today, he is the only one to have served as United States Attorney. His special expertise in criminal law and procedure shows through. Judge King adhered to stringent professional

---

80 *Id.*

81 *Id.* at 11 (statement of Sen. John D. Rockefeller IV).

82 *Id.*

83 Federal Judicial Center, Biographical Directory of Federal Judges, Robert Bruce King, http://www.fjc.gov/servlet/tGetInfo?jid=2790.

84 King Questionnaire, *supra* note 23, at 23. Judge King's trial skills and experience led to his election to the American College of Trial Lawyers. *Id.* at 6, 17.

85 *Id.* at 14-16.

86 *Id.* at 15-18.

87 *Id.* at 14.

88 *Id.* at 16.

89 *Id.* at 14.

standards when serving as a federal prosecutor, and he demands that government lawyers hold to those same standards today. As he has emphasized, "[p]rosecutors have 'a unique role in the criminal justice system, which regards them not just as advocates but as ministers of justice.'"[90] A prosecutor's task is not merely to advocate for the government in seeking a conviction; as Judge King has explained, the prosecutor is "also obligated to seek to prevent the appearance and reality of unfairness."[91] Moreover, Judge King has underscored the necessity for absolute neutrality on the part of a judge presiding in a criminal trial. This neutrality requires the trial judge to take great care in posing questions to witnesses, especially the defendant. Judge King has stressed that "[e]ven when the evidence provides the court with a negative impression of the defendant, the judge must refrain from interjecting that perception into the trial. He is always obliged to retain the general atmosphere of impartiality required of a fair tribunal, and must not – under any circumstance – become an advocate for the prosecution."[92] Although Judge King is not reticent about criticizing prosecutorial or judicial conduct that violates these principles, his practical experience has sharpened his ability to distinguish between legal errors that require a conviction to be set aside and those that do not.[93] In addition, Judge King is a fierce protector of the inviolability of the jury deliberation process, as his dissents in *Robinson v. Polk*[94] reflect. There, disagreeing with the panel majority, Judge King argued that a federal habeas petitioner's constitutional rights were violated when the jury obtained a Bible from the bailiff and consulted numerous Biblical passages during its deliberations.[95] This extrajudicial resort to a sacred text, Judge King believed, presented a great risk that the jury was improperly swayed.[96]

Judge King has also made substantial contributions to Fourth Circuit law in civil rights cases. He has demonstrated great respect for the congres-

---

[90] United States v. Rolle, 204 F.3d 133, 138 n.7 (4th Cir. 2000) (quoting ABA/BNA LAWYERS MANUAL ON PROFESSIONAL CONDUCT, 61:601 (1999)).

[91] United States v. Godwin, 272 F.3d 659, 672 n.16 (4th Cir. 2001).

[92] *Id.* at 678 (punctuation omitted).

[93] *See Godwin*, 272 F.3d at 679-80 (determining that trial court's improper questioning of defendant did not necessitate reversal because error did not affect substantial rights); *Rolle*, 204 F.3d at 140-41 (determining that even though the trial court erred in not allowing the defendant to attend voir dire, the defendant's failure to object to the error, and his inability to show that the error affected his substantial rights, meant that the error was not grounds for reversal); *see also* United States v. Turner, 198 F.3d 425, 429-31 (4th Cir. 1999) (holding that the district court erred in prohibiting defense counsel from examining a government witness about her fear that she would be prosecuted for crimes more serious than those to which she had pled guilty if she did not cooperate with the government, but reasoning that the error did not affect the outcome of the proceedings and was therefore not a basis for reversal).

[94] 444 F.3d at 230-33 (King, J., dissenting from denial of rehearing en banc); 438 F.3d at 368-76 (King, J., dissenting).

[95] *Id.*

[96] *Id.*

sional purpose behind the civil rights statutes, which were enacted to advance America's promise of equality to all. The two opinions Judge King wrote for the unanimous panel in *Spriggs v. Diamond Auto Glass*, in which an African-American, at-will employee alleged that he was fired because of his race, are illustrative.[97] In the first opinion the panel classified this allegation as a claim of purposeful racial discrimination in the termination of a contract.[98] The court held that at-will employment (as defined by state law) was a contract, permitting the plaintiff to state a claim under 42 U.S.C. § 1981.[99] Section 1981 prohibits racial discrimination in contract formation and enforcement and "specifically includes 'termination of contracts' as an aspect of making and enforcing contracts that is protected."[100] On this basis the panel reversed the district court's dismissal and remanded the case for further proceedings.[101] The case was appealed a second time, after the district court granted summary judgment to the defendants.[102] Speaking once again through Judge King, the court explained that genuine issues remained for trial, in part because there was enough evidence that the plaintiff's supervisor, by regularly using highly offensive racial epithets, had created a racially hostile work environment that was severe or pervasive.[103] Other circuits have relied on the opinions in *Spriggs* for guidance in employment discrimination cases.[104]

Judge King's fidelity to the broad remedial intent behind the civil rights statutes also informed his dissent in *Jordan v. Alternative Resources Corp.*[105] In that case an African-American plaintiff contended that he was fired in reprisal for reporting to his employer that a co-worker had used extremely ugly racial epithets. The panel concluded, among other things, that the plaintiff did not state a claim for retaliation under Title VII.[106] Judge King disagreed, arguing

---

97 242 F.3d 179 (4th Cir. 2001) (*Spriggs II*); 165 F.3d 1015 (4th Cir. 1999) (*Spriggs I*).

98 *Spriggs I*, 165 F.3d at 1020.

99 *Id.*

100 *Id.*

101 *Id.*

102 *Spriggs II*, 242 F.3d 179.

103 *Id.* at 184-86.

104 *See, e.g.*, Cerros v. Steel Techs., Inc., 398 F.3d 944, 953 (7th Cir. 2005) (quoting *Spriggs II*, 242 F.3d at 188, to support the proposition that mere existence of an anti-harassment policy does not insulate the employer from liability for racial harassment); Williams v. Admin. Review Bd., 376 F.3d 471, 478 (5th Cir. 2004) (citing *Spriggs II*, 242 F.3d at 186 n.9, as an example of a racial harassment case applying the affirmative defense standard originally crafted for sexual harassment claims); Lauture v. IBM, 216 F.3d 258, 260, 262-63 (2d Cir. 2000) (citing *Spriggs I*, 165 F.3d at 1018-19, and joining it in holding that "an at-will employee may sue under § 1981 for racially discriminatory termination.").

105 No. 05-1485, 447 F.3d 324 (4th Cir. 2006), *withdrawn and reh'g granted*, No. 05-1486, 2006 U.S. App. LEXIS 20737 (4th Cir. Aug. 14, 2006).

106 Title VII of the Civil Rights Act of 1964 prohibits discrimination based on a worker's "race, color, religion, sex, or national origin," 42 U.S.C. § 2999e-2(a), and its anti-retaliation section

that the majority's rule puts employees in a bind: either complain about racially offensive behavior and face retaliation, or do not complain about such behavior and forfeit any subsequent claims for judicial relief. Judge King noted that in drafting Title VII, "Congress exercised its considered judgment that [private suits] are an essential tool for ensuring compliance with Title VII's provisions,"[107] and he argued that the majority's ruling effectively undercut that legislative judgment.

Judge King has also written for the court in numerous constitutional cases. For example, in *Mellen v. Bunting*[108] several cadets at the state-operated Virginia Military Institute (VMI) contended that VMI officials violated the Establishment Clause in holding a daily supper prayer, during which students were required to stand and remain silent.[109] The district court granted the cadets prospective equitable relief but held that the cadets could not obtain money damages from the Superintendent of VMI because he was entitled to qualified immunity.[110] Judge King, writing for a unanimous panel, vacated the grant of prospective relief because the cadets, having graduated from VMI, could no longer claim ongoing injury.[111] The money damages claim survived, however, which required the court to examine the availability of qualified immunity.[112] The court concluded that the supper prayer violated the Establishment Clause.[113] It reasoned that the "adversative" instructional method used at VMI made the cadets "uniquely susceptible to [school] coercion" to participate in the religious exercise.[114] It also concluded that the prayer had the "primary effect of promoting religion"[115] and that through the prayer, VMI "took a position on what constitutes appropriate religious worship," rendering the prayer impermissible under Supreme Court precedent. [116] The court affirmed the qualified immunity ruling, however, because the Superintendent could not reasonably have known that his action was a violation of a clearly established constitutional right.[117]

---

prohibits "discriminat[ion] against" a worker who has, among other things, "made a charge, testified, assisted, or participated in" a Title VII investigation, § 2000e-3(a).

[107] Jordan v. Alternative Resources Corp., No. 05-1486, 2006 U.S. App. LEXIS 20737, *67 (4th Cir. Aug. 14, 2006).

[108] 327 F.3d 355, *en banc reh'g denied*, 341 F.3d 312 (4th Cir. 2003), *cert. denied*, 541 U.S. 1019 (2004).

[109] *Mellen*, 327 F.3d at 362.

[110] *Id.* at 363.

[111] *Id.* at 364-65.

[112] *Id.* at 365.

[113] *Id.* at 377.

[114] *Id.* at 371.

[115] *Id.* at 374.

[116] *Id.* at 375.

[117] *Id.* at 376.

The defendants were unsuccessful in their efforts to obtain en banc and Supreme Court review of the court's opinion authored by Judge King.[118]

Judge King has, of course, been in disagreement with his colleagues on occasion, leading him to write dissenting opinions or dissents from the denial of rehearing en banc. It is in those opinions that Judge King's individual voice has often sounded most clearly. In *Ohio Valley Environmental Coalition v. Bulen*,[119] Judge King wrote a powerful dissent from the Fourth Circuit's denial of rehearing en banc. The case concerned eleven mining projects in West Virginia approved by the Army Corps of Engineers (Corps).[120] These projects entailed extensive valley fills and surface impoundments that were estimated to impact roughly 140,000 linear feet of West Virginia's streams.[121] The Corps had authorized these projects by issuing a nationwide permit that, plaintiffs alleged, circumvented the Clean Water Act (CWA) by allowing all sorts of environmentally damaging activities without first subjecting them to the CWA's notice requirements and other safeguards.[122] In the district court proceeding, Judge Joseph R. Goodwin concluded that the Corps' authorization procedure violated the CWA; the district judge accordingly ordered suspension of the eleven projects and enjoined the Corps from issuing similar authorizations in the Southern District of West Virginia.[123] The Fourth Circuit reversed this holding and denied the petition for rehearing en banc.[124] In his dissent from the denial of rehearing en banc, Judge King agreed with Judge Goodwin and expressed in forceful terms his opinion that Congress's mandate for the protection of a unique mountain ecosystem was not being followed:

> [T]his case is of exceptional importance to the nation and, in particular, to the states in the Appalachian region. The Appalachian mountains, the oldest mountain chain in the world, are one of the nation's richest, most diverse, and most delicate ecosystems, an ecosystem that the mountaintop coal mining authorized by the Corps' general permit may irrevocably damage or destroy. In enacting the CWA, Congress mandated the protection of our environment through strict procedural requirements.

---

[118] The Fourth Circuit divided evenly on, and therefore denied, a petition for en banc rehearing, with three circuit judges writing separate dissents from the denial. 341 F.3d 312 (4th Cir. 2003). The Supreme Court thereafter declined to review the case on certiorari. 541 U.S. 1019 (2004). Justice Scalia, joined by Chief Justice Rehnquist, wrote in dissent from the Court's refusal to review the case, leading Justice Stevens to write a reply, joined by Justices Ginsburg and Breyer, explaining why further review was not warranted. *Id.*

[119] 437 F.3d 421 (4th Cir. 2006) (King, J., dissenting from denial of rehearing en banc).

[120] *Id.*

[121] Ohio Valley Envt'l Coal. v. Bulen, 410 F.Supp.2d 450, 457 (S.D. W. Va. 2004).

[122] *Id.* at 456.

[123] *Id.* at 471.

[124] Ohio Valley Envt'l Coal. v. Bulen, 429 F.3d 493, 499-500 (4th Cir. 2005).

> The panel's decision, in authorizing the Corps to skirt the CWA-mandated permitting process, undermines the enactment's primary purpose and poses unnecessary risks to one of this nation's great places.[125]

* * *

At Judge King's investiture Senator Byrd said he had "every confidence" that the judge's "wisdom and intellect will help to light the course in constitutional waters that we all must follow."[126] Judge King has lived up to Senator Byrd's forecast not only in constitutional cases but also in every other aspect of the job. The exercise of sound judgment and the extension of courtesy to lawyers and colleagues have been the hallmarks of Judge King's service as a judge. The Fourth Circuit is known as a collegial court,[127] and Judge King does more than his share to keep that tradition alive. His contributions extend to all aspects of the court's business. For example, he serves on the Judicial Council, the small body of judges responsible for administering the federal courts in the Fourth Circuit.[128] Judge King is also a member of the U.S. Judicial Conference's Committee on Information Technology, and he chairs the subcommittee on planning and budget. Judge Robert Bruce King is blessed with irrepressible enthusiasm and energy, and he does all of his work with good cheer. I look forward to being his colleague for many years to come.

---

125 437 F.3d at 424 (King, J., dissenting from denial of rehearing en banc) (citation omitted).

126 King Investiture Ceremonies, *supra* note 3, at 59.

127 *See* J. Harvie Wilkinson III, *Building a Legal Culture of Affection*, 99 NW. U. L. REV. 1235, 1241 (2005) ("I can say that the Fourth Circuit works very hard at being a collegial, and even an affectionate court.").

128 *See* 28 U.S.C. § 332 (2006) (establishing role for judicial councils).

West Virginia Forward: Our State's Path to Prosperity

E. Gordon Gee
President, West Virginia University

E. Gordon Gee

Dr. E. Gordon Gee is one of America's most prominent higher education leaders, having served as president of some of the most prestigious public and private universities for more than three decades.

When he returned to lead West Virginia University in 2014 as the institution's 24th president, it was a homecoming of sorts. He was first named WVU president in 1981 at age 36 – at the time, among the youngest persons to ever serve as a university president.

He led WVU until 1985 when he went on to presidencies at the University of Colorado (1985-90), Brown University (1998-2000) and Vanderbilt University (2001-07). He served as president of The Ohio State University from 1990-97 and again from 2007-13.

On his return to the Morgantown campus, he said, "This is not a job to me; it is a calling." His leadership style bears that out as he works tirelessly to advance the University's land-grant mission and open doors to the American dream.

In his latest address to the University community, he noted that for 150 years, the institution has been a polar star guiding West Virginians toward a brighter tomorrow. He said, "That is why, in this milestone year, we recommit our University to living the values that drive our work. Serving our students and our state is not just our duty — it is our passion."

Gee has built a special relationship with the students as well as the state's citizens, making it a point to visit students where they live, learn and socialize -- and visiting all 55 West Virginia counties during his inaugural year – and at least half in subsequent years.

Born in Vernal, Utah, Gee graduated from the University of Utah with an honors degree in history and earned his J.D. and Ed.D. degrees from Columbia University. He clerked under Chief Justice David T. Lewis of the U.S. 10th Circuit Court of Appeals before being named a judicial fellow and staff assistant to the U.S. Supreme Court. In this role, he worked for Chief Justice Warren Burger on administrative and legal problems of the Court and federal judiciary. Gee returned to Utah as an associate professor and associate dean in the J. Reuben Clark Law School at Brigham Young University, and was granted full professorship in 1978.

One year later, he became dean of the WVU College of Law, and, in 1981, was named WVU's 19th president.

Gee has served on several education-governance organizations and committees, including the Big 12 Conference Council of Presidents, the Business Higher Education Forum and the American Association of Universities. He was chair of the American Council on Education's Commission on Higher Education Attainment and served as co-chair of the Association of Public and Land-Grant Universities' Energy Advisory Committee. In 2009, King Abdulaziz University in Saudi Arabia invited him to join its international advisory board. In 2009, *Time* magazine named him one of the top 10 university presidents in the United States.

Gee is serving as chair of the Big 12 Board of Directors Executive Committee for the 2017-18 year. Active in many national professional and service organizations, he is on the executive committee of the National 4-H Council Board of Trustees and serves on the board of directors of the American Council on Education, the nation's largest higher education organization, as well as on the board of trustees of the Royal University for Women in Bahrain, with which WVU has a long-standing academic partnership. A recipient of the Distinguished Eagle Scout Award, he is an executive board member of Boy Scouts of America. He has also served on the boards for the Rock and Roll Hall of Fame and Museum and Limited Brands.

In 2011, Gee began serving as secretary on the Board of Directors of Ohio's economic development program, JobsOhio. In 2011-12, Governor John Kasich asked him to chair the Ohio Higher Education Capital Funding Collaborative and the Ohio Higher Education Funding Commission. In December 2012, he began serving on the Columbus Education Commission.

Gee has received many honorary degrees, awards, fellowships and recognitions. He is a fellow of the prestigious American Association for the Advancement of Science, the world's largest science organization. In 1994, Gee received the Distinguished Alumnus Award from the University of Utah, as well as from Teachers College of Columbia University. In 2013, he received the ACE Council of Fellows/Fidelity Investments Mentor Award and the Outstanding Academic Leader of the Year Award on behalf of Historically Black Colleges and Universities. He is the co-author of 11 books, including *Law, Policy and Higher Education*, published in 2012. He has also authored many papers and articles on law and education.

In the summer of 2016, Gee announced his engagement to Laurie Erickson, leader of the Erickson Foundation. Gee's daughter, Rebekah, is Secretary of the Louisiana Department of Health. In addition to that role, she is a practicing gynecologist and Gratis Faculty at the Louisiana State University School of Medicine and Louisiana State University Health Sciences Center in New Orleans. Dr. Rebekah Gee is married to David Patrón and they have five children.

Abraham Lincoln's Almanac Murder Trial

Jack Bowman
Professor Emeritus,
West Virginia University College of Law

Forest Jackson "Jack" Bowman

Forest Jackson "Jack" Bowman is the Jackson & Kelly Professor of Law Emeritus at West Virginia University. He is a native West Virginian, and an undergraduate and law graduate of West Virginia University, where he served as President of the Student Body in 1959-60. (It was during his term as Student Body President that the effort to bring the mast of the U.S.S. West Virginia to the campus was begun.)

He retired in 2002 after serving as a Professor of Law at WVU for twenty-three years during which time he was named “Professor of the Year” by seven graduating classes at the College of Law. He also was named University-wide “Professor of the Year” in 1998, and in 1988 was named "Professor of the Year" for all of higher education in West Virginia by the Faculty Merit Foundation of West Virginia.

In a departure from typical academic isolation, he is a former President of The West Virginia Bar Association and is a Past Chair of The Salvation Army’s Evangeline Booth College in Atlanta, Georgia. For 35 years he has served as a member of the Advisory Board of The Salvation Army of Morgantown and is once again serving as Chair of that Board.

A veteran of the United States Army, Professor Bowman served over four years in the Judge Advocate Generals Corps, Regular Army. He was honorably discharged in 1967 with the rank of Captain and was awarded the Army Commendation Medal. From March 2007 through February 2011 he served as Civilian Aide to the Secretary of the Army for the state of West Virginia by appointment from former Secretary of the Army Francis Harvey.

Jack is an avid student of history and was the founder and first president of the Mason-Dixon Civil War Round Table in Morgantown.

Today he will tell us the “behind the scenes story” of Abraham Lincoln’s defense of Duff Armstrong, a defense made famous by Lincoln’s effective use of three almanacs.

Abraham Lincoln's "Almanac" Trial

Forest J. "Jack" Bowman
Jackson Kelly Professor of Law Emeritus
28 Vintner Place
Morgantown, WV 26505
(304) 288-7396

Abraham Lincoln's "Almanac" Trial

Notes

A. The letter from Hannah Armstrong

1. Lincoln & Jack Armstrong

a. The Clary's Grove Boys

b. The wrestling match & its outcome

c. Lincoln's relationship with the Armstrong family

2. Duff Armstrong and Lincoln

B. Duff Armstrong is indicted for murder

1. Dilworth & Campbell hired to defend Duff Armstrong

a. What happened at Walker's Grove

i.. "Press" Metzger & his little "jokes" on Duff Armstrong & James Norris

ii. Armstrong's & Norris' "weapons"

iii. Metzger's lingering death after the ride home

Notes

b. The change of venue

c. Norris is convicted of manslaughter

C. The Armstrong's hire Lincoln to defend Duff

1. Lincoln begins preparing for trial

a. The case against Armstrong

b. The case for Armstrong

c. The trial is postponed

2. The final trial preparation

a. Lincoln's arrival in Beardstown

b. Witnesses summoned by Lincoln

c. Lincoln's medical expert

d. The mysterious disappearance of the major witness against Armstrong

e. Jury selection

D. The trial begins

1. The Prosecution's case

Notes

a. Dr. Stevenson

b. Charles Allen - the witness whose testimony had condemned James Norris

2. Lincoln takes charge

a. Lincoln's white suit.

b. The opening statement

d. The eye witnesses

i. Duff Armstrong's character

ii. Nelson Watkins & the "slungshot"

e. Dr. Parker& the cause of death

3. Lincoln calls Charles Allen, the state's chief witness, to the stand

a. How bright was the moon?

b. How far was Allen from the fight?

C. Where, exactly, was the moon?

E. The almanac comes into play

1. Lincoln uses an almanac to prove the moon's position

Notes

2. Two other almanacs are brought into the trial for comparison regarding the moon's position

F. Closing arguments

1. The state argues its case

2. Lincoln takes charge again

a. The "backwoodsy" ploy

b. The cold and analytical review of the evidence

c. The emotional play on Duff Armstrong's mother

G. The verdict

H. The legend of the "faked" almanac

I. Epilogue

We Are Who We Are, But is That All We'll Ever Be? (Implicit Bias and Its Impact on the Practitioner)

Dana Tippin Cutler
Partner, James W. Tippen & Associates

Dana Tippin Cutler

Dana Tippin Cutler is a partner in her family's law firm, James W. Tippin & Associates. She graduated from UMKC School of Law in 1989 and from Spelman College with a B.A. in 1986. Dana is a member of the American Bar Association; Jackson County Bar Association; and the Kansas City Metropolitan Bar Association. She is Immediate Past-President of The Missouri Bar (Sept 2016-Sept 2017) and is immediate-past President of The Missouri Bar Foundation. She was recently elected to the Council for the National Conference of Bar Presidents. She was appointed by the ABA President to serve on the Committee for Professionalism. She was appointed and has served on the ABA Standing Committee for Judicial Independence and The Missouri Bar Trustees. She has served as the Chair of the Diversity Committee (f/k/a Committee on Minority Issues) for The Missouri Bar and was instrumental in starting The Missouri Bar's Leadership Academy. She has served as legal counsel for the Kansas City Metropolitan Bar Foundation and as chair and vice-chair for the KCMBA's Circuit Court & Civil Practice Committee and vice-chair of the Insurance Law Committee. Dana is a three-time recipient of The Missouri Bar's President Award for service. Dana serves on and is currently the treasurer of and a past-president of the Board of Curators for Lincoln University in Jefferson City, Missouri, a gubernatorial appointment. Her community service includes serving on the Boards of Swope Parkway Health Center and Swope Community Enterprises. Her practice is concentrated primarily in education law (charter and hybrid schools in Missouri) and defense litigation. She is an active member of Concord Fortress of Hope and is the proud mother of three adult sons Keith, Jr., Dean and Austin Cutler and is the partner, in practice and in marriage, of Keith Cutler, Sr.

IMPLICIT BIAS or IMPLCIT COGNITION/ASSOCIATION

refers to the attitudes or stereotypes that affect our understanding, actions, and decisions in an unconscious manner

LAQUANDA WASHINGTON

CODE SWITCHING

the use of one dialect, register, accent, or language variety over another, depending on social or cultural context, to project a specific identity

OR

the modifying of one's behavior, appearance, etc., to adapt to different sociocultural norms

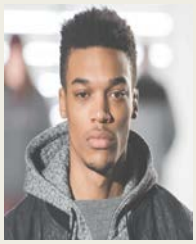
For many female Muslim students, code-switching from their home environment to that of school requires forgoing the hijab.

MICRO-AGGRESSIONS

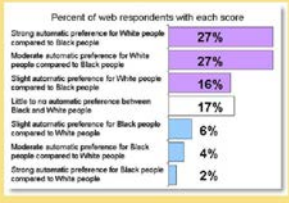
are the everyday verbal, nonverbal, and environmental slights, snubs, or insults, whether intentional or unintentional, which communicate hostile, derogatory, or negative messages to target persons based solely upon their marginalized group membership

Other Examples of Micro-Aggressions

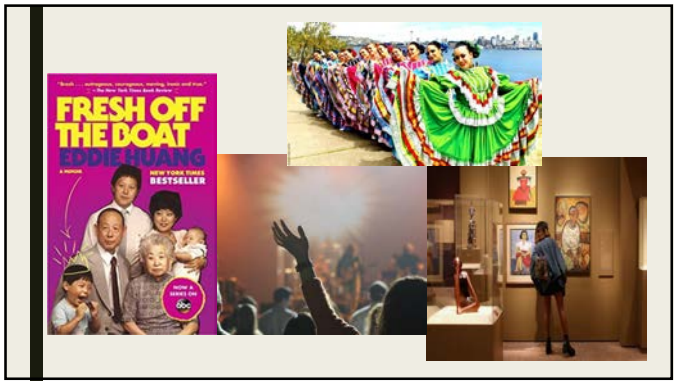
- I don't see color.
- You're so articulate.
- I have a "fill in the ethnicity" friend or friends.
- I went to the store the other day, and they gypped me out of my free gift!
- Wow, you like country music? Opera? Chamber music? Symphonic music? Chorale? Ballet?
- I presume you're bi-lingual.
- You're not like ***other*** Hispanics, Blacks, Asians.



Harvard Implicit Association Test



http://implicit.harvard.edu


FRESH OFF THE BOAT
EDDIE HUANG
NEW YORK TIMES BESTSELLER


dri
Diversity for Success
Seminar and
Corporate Expo
June
14-15,
2018
HNBA
HISPANIC NATIONAL
BAR ASSOCIATION
NBA
Diversity in the Legal
Profession Committee
NAPABA
National Asian Pacific American Bar Association


SEEK unity
INCLUSION
THE COMMUNITY HOUSE
Arts • Enrichment • Unity
RACE: unity in diversity
faith seeking understanding forum | april 20–21
Save the Date!
One Community, One Voice
October 10th, 2015
10 a.m. to 2 p.m.
Crowne Plaza • Madison, WI

The Impact and Import of State Marijuana Reforms

Douglas A. Berman
Professor, The Ohio State University Moritz College of Law

Douglas A. Berman

Robert J. Watkins/Procter & Gamble Professor of Law

Contact Information:

(614) 688-8690

berman.43@osu.edu

Education:

- A.B., Princeton University, Philosophy
- J.D., Harvard Law School

Areas of Expertise:

- Clinical Education
- Criminal Law
- Death Penalty
- Sentencing

Professor Douglas A. Berman attended Princeton University and Harvard Law School. In law school, he was an editor and developments office chair of the *Harvard Law Review* and also served as a teaching assistant for a Harvard University philosophy course. After graduation from law school in 1993, Professor Berman served as a law clerk for Judge Jon O. Newman and then for Judge Guido Calabresi, both on the United States Court of Appeals for the Second Circuit. After clerking, Professor Berman was a litigation associate at the law firm of Paul, Weiss, Rifkind, Wharton, and Garrison in New York City.

Professor Berman's principal teaching and research focus is in the area of criminal law and criminal sentencing, though he also has teaching and practice experience in the fields of legislation and intellectual property. He has taught *Criminal Law*, *Criminal Punishment and Sentencing*, *Criminal Procedure – Investigation*, *The Death Penalty*, *Legislation*, *Introduction to Intellectual Property*, *Second Amendment Seminar*, and the *Legislation Clinic*.

Professor Berman is the co-author of a casebook, *Sentencing Law and Policy: Cases, Statutes and Guidelines*, which is published by Aspen Publishers and is now in its second edition. In addition to authoring numerous publications on topics ranging from capital punishment to the federal sentencing guidelines, Professor Berman has served as an editor of the *Federal Sentencing Reporter* for more than a decade, and also now serves as co-managing editor of the *Ohio State Journal of Criminal Law*.

During the 1999-2000 school year, Professor Berman received The Ohio State University Alumni Award for Distinguished Teaching, which is given to only 10 people each year from an eligible pool of nearly 3,000 faculty members. Professor Berman was one of the youngest faculty members to ever receive this award, and he was subsequently asked to chair the university committee that selected recipients in the 2002-03 school year.

Professor Berman is the sole creator and author of the widely-read and widely-cited blog, Sentencing Law and Policy. The blog now receives nearly 100,000 page views per month (and had over 20,000 hits the day of the Supreme Court's major sentencing decision in *United States v. Booker*). Professor Berman's work on the Sentencing Law and Policy blog, which he describes as a form of "scholarship in action," has been profiled or discussed at length in articles appearing in the *Wall Street Journal*, *Legal Affairs* magazine, *Lawyers Weekly USA*, *Legal Times*, *Columbus Monthly*, and in numerous other print and online publications.

In addition, Sentencing Law and Policy has the distinction of being the first blog cited by the U.S. Supreme Court (for a document appearing exclusively on the site), and substantive analysis in particular blog posts has been cited in numerous appellate and district court rulings, in many briefs submitted to federal and state courts around the country, and in dozens of law review articles.

Professor Berman frequently is consulted by national and state policymakers, sentencing commissioners, and public policy groups concerning sentencing law and policy reforms. He has testified before the U.S. House of Representatives and before numerous sentencing commissions. He also is frequently contacted by media concerning sentencing developments by national and local media concerning sentencing developments.

In recent years, Professor Berman has appeared on national television and radio news programs and has been extensively quoted in newspaper articles appearing in nearly every major national paper and many local papers, including *The New York Times*, *The Washington Post*, *The Wall Street Journal*, *Legal Times*, and in pieces from the Associated Press, Reuters, and Knight-Ridder news services.

Professor Berman sometimes serves as a consultant to lawyers working on important or interesting sentencing cases. In most instances, Professor Berman's consulting has been on an *ad hoc* and *pro bono* basis, and it usually involves a quick review of draft briefs and other court filings and then providing general advice on litigation strategies. On some occasions, however, Professor Berman has been formally retained to play a more sustained role in certain cases, including being retained by law firms to provide consulting service on various cutting-edge federal sentencing issues.

Cybersecurity Tips at Warp Speed for Lawyers

Sharon Nelson
President, Sensei Enterprises, Inc.

John Simek
Vice President, Sensei Enterprises, Inc.

Sharon D. Nelson, Esq.

Sharon D. Nelson, Esq., is the President of Sensei Enterprises, Inc., a digital forensics, cybersecurity and information technology firm in Fairfax, Virginia.

Ms. Nelson is the author of the noted electronic evidence blog, *Ride the Lightning* and is a co-host of the Legal Talk Network podcast series called "*The Digital Edge: Lawyers and Technology*" as well as "*Digital Detectives*."

She is a frequent author (sixteen books published by the ABA and hundreds of articles) and speaker on legal technology, cybersecurity and electronic evidence topics. She was the President of the Virginia State Bar June 2013 – June 2014 and a past President of the Fairfax Law Foundation.

She may be reached at snelson@senseient.com

John W. Simek

Mr. Simek is the Vice President of Sensei Enterprises, Inc., an information technology, digital forensics and information security firm located in Fairfax, VA. Mr. Simek has a national reputation as a digital forensics technologist and has testified as an expert witness throughout the United States. He holds a degree in engineering from the United States Merchant Marine Academy and an MBA in finance from Saint Joseph's University.

Mr. Simek holds the prestigious CISSP (Certified Information Systems Security Professional) certification. He is also holds multiple technical certifications for diverse technologies to include Microsoft, Novell, mobile devices and computer networking environments. Mr. Simek is also a member of the High Tech Crime Network as well as the American Bar Association and the Fairfax Bar Association.

He currently provides information technology support to hundreds of area law firms, legal entities and corporations. He is a co-host of the Legal Talk Network podcast *Digital Detectives* and a co-author of sixteen books to include *Locked Down: Practical Information Security for Lawyers, 2nd Edition* (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association, 2015) and *The 2008-2018 Solo and Small Firm Legal Technology Guide: Critical Decisions Made Simple* (American Bar Association, 2008-2018) as well as other titles. He is a frequent author and speaker on information security, legal technology and electronic evidence throughout the country. He blogs at youritconsultant.senseient.com and may be reached at jsimek@senseient.com.

West Virginia State Bar

Cybersecurity Tips at Warp Speed for Lawyers

April 9, 2018

Presenters:

Sharon D. Nelson
President, Sensei Enterprises Inc.
snelson@senseient.com

John W. Simek
Vice President, Sensei Enterprises Inc.
jsimek@senseient.com

703-359-0700
www.senseient.com

SAFEGUARDING CONFIDENTIAL INFORMATION
Attorneys' Ethical and Legal Obligations

David G. Ries
Clark Hill PLC
Pittsburgh, PA

dries@clarkhill.com

October 2017

Contents

Introduction[1]

Confidential data in computers and information systems, including those used by attorneys and law firms, faces greater security threats today than ever before. And they continue to grow! They take a variety of forms, ranging from e-mail phishing scams and social engineering attacks to sophisticated technical exploits resulting in long term intrusions into law firm networks. They also include lost or stolen laptops, tablets, smartphones, and USB drives, as well as inside threats - malicious, untrained, inattentive, and even bored personnel.

These threats are a particular concern to attorneys because of their duty of confidentiality. Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.

Effective information security[2] requires an ongoing, comprehensive process that addresses people, policies and procedures, and technology, including training. It also requires an understanding that security is everyone's responsibility and constant security awareness by all users of technology.

The Threats

For years, technology attorneys and information security professionals warned lawyers that it was not a question of whether law firms would become victims of successful hacking attacks - it was a matter of when. They pointed to numerous law firm incidents of dishonest insiders and lost or stolen laptops and portable media, but there were not disclosed incidents of successful hacking attacks. It has now reached the "when" – over the last decade, there have been increasing reports in the popular, legal, and security media of successful hacking attacks on

[1] Parts of this paper are adapted from prior materials prepared by the author, including David G. Ries, "Safeguarding Confidential Data: Your Ethical and Legal Obligations," *Law Practice* (July/August 2010) and David G. Ries, "Cybersecurity for Attorneys: Understanding the Ethical Obligations," *Law Practice TODAY* (March 2012). This paper is an overview. For more detailed information, see Sharon D. Nelson, David G. Ries and John W. Simek, *Locked Down: Practical Information Security for Attorneys, Second Edition* (American Bar Association 2016) and the other materials listed in the Additional Information section.

[2] The term *du jour* is now "cybersecurity" – focusing on cyberspace and connectivity. But cybersecurity is actually a subset of information security because individual computers, servers and mobile devices need to be protected from threats like loss, theft and unauthorized physical access – distinct from connected cyberspace.

attorneys and law firms. They have occurred and are occurring - and attorneys and law firms need to comprehensively address security.

Breaches are becoming so prevalent that there is a new mantra in cybersecurity today – it's "when not if" a law firm or other entity will suffer a breach. Robert Mueller, then the FBI Director, put it this way in an address at a major information security conference in 2012:[3]

> I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

This observation is true for attorneys and law firms as well as companies. New York Ethics Opinion 1019 (discussed in Sections 2 B and 2 D and below) warned attorneys in May 2014 about these risks:

> Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.

ABA Formal Opinion 477 (May 2017) (also discussed in Sections 2 B and 2 D below), describes the current threat environment:

> At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of "when," and not "if." Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

The following Sections 1 A through 1 E explore current threats to attorneys and law firms.

Outside Attacks

Law firms are considered by attackers to be "one stop shops" for attacks because they have high value information of multiple clients that is well organized, often with weaker security than clients. Hackers target money, personally identifiable information that can be converted to money, client business strategy, intellectual property and technology, and information about deals and litigation. Threat actors include cybercriminals, hackers, governments, hactivists (with political agendas), and insiders.

---

[3] FBI Director, RSA Cybersecurity Conference (March 1, 2012)
https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

As a recent article explained it:[4]

> Ask hackers why they attack law firms, and their reply - to riff on bank robber Willie Sutton's famous quip - would no doubt be: "Because that's where the secrets are."

A December 2009 FBI alert warned that law firms and public relations firms were being targeted with spearphishing e-mails[5] containing malicious payloads.[6] In January 2010, the FBI issued another alert, this time warning law firms about counterfeit check schemes that used e-mails to lure them into relationships with fraudulent overseas "clients."[7]

The news reports of law firm breaches started with a February, 2010, *Wired Magazine* article that reported on advanced persistent threats (APTs), a particularly nasty form of sophisticated and extended hacking attack. It discussed an example of a 2008 APT attack on a law firm that was representing a client in Chinese litigation:[8]

> The attackers were in the firm's network for a year before the firm learned from law enforcement that it had been hacked. By then, the intruders harvested thousands of e-mails and attachments from mail servers. They also had access to every other server, desktop workstation and laptop on the firm's network.

This attack was investigated by Mandiant, a leading information security firm that specializes in investigation of data breaches.[9] Mandiant discovered that the network had been breached for more than a year before the law firm was tipped off to the breach by law enforcement. They could not determine the initial attack vector because the law firm did not have system logs available. The intruders at the law firm were able to obtain more than 30 sets of user credentials, compromise approximately three dozen workstations, and gain full access to all servers and computers on the network for an extended time.

"The intruders at the law firm were able to… gain full access to all servers and computers on the network for an extended time."

[4] Matthew J. Schwartz, "Cyberattacks: Why Law Firms Are Under Fire," *infoRisk Today* (April 7, 2016).

[5] "Spear phishing" is fraudulent e-mail that falsely appears to be from a trusted source and targets a specific organization or individual, seeking unauthorized access to confidential data, often log on credentials.

[6] FBI Release, "Spear Phishing E-mails Target U.S. Law Firms and Public Relations Firms" (November 17, 2009).

[7] FBI Release, "New Twist on Counterfeit Check Schemes Targeting U.S. Law Firms" (January 21, 2010).

[8] Kim Zetter, "Report Details Hacks Targeting Google, Others," *Wired Magazine* (February 3, 2010).

[9] See Mandiant's *M-Trends 2010 The Advanced Persistent Threat*, www.fireeye.com/current-threats/annual-threat-report.html.

A *National Law Journal* article in March, 2010, reported that Mandiant assisted over 50 law firms after security breaches.[10] A Mandiant forensics specialist stated in an interview that Mandiant spent approximately 10% of its time in 2010 investigating data breaches at law firms.[11]

The same month, an article in the *San Francisco Chronicle*, "Law Firms Are Lucrative Targets of Cyberscams," discussed recent attacks on attorneys, ranging from phishing scams to deep intrusions into law firm networks to steal lawsuit-related information.[12] It reported:

> Security experts said criminals gain access into law firms' networks using highly tailored schemes to trick attorneys into downloading customized malware into their computers. It is not uncommon for them to remain undetected for long periods of time and come and go as they please, they said.

In November, 2011, the FBI held a meeting for the 200 largest law firms in New York to advise them about the increasing number of attacks. *Bloomberg News* reported: [13]

> Over snacks in a large meeting room, the FBI issued a warning to the lawyers: Hackers see attorneys as a back door to the valuable data of their corporate clients.
>
> "We told them they need a diagram of their network; they need to know how computer logs are kept," Galligan [the head of the FBI cyber division in New York City] said of the meeting. "Some were really well prepared; others didn't know what we were talking about."

Successful attacks on law firms have continued. *Bloomberg News* published "China-Based Hackers Target Law Firms to Get Secret Deal Data" in January, 2012.[14] It described a group of major hacking incidents in which attackers successfully targeted seven Canadian law firms and two Canadian government agencies to get information about a transaction involving the sale of potash mines in Western Canada.

The SANS Institute, a highly-regarded information security research, education, and certification organization, has published an interview with the managing partner and IT partner of a New York law firm that had been

---

[10] Karen Sloan, "Firms Slow to Awaken to Cybersecurity Threat," *The National Law Journal* (March 8, 2010). www.nationallawjournal.com/id=1202445679728?slreturn=20140103163537.

[11] Kelly Jackson, "Law Firms under Siege," *Dark Reading* (April 6, 2011).

[12] Alejandro Martínez-Cabrera, "Law Firms Are Lucrative Targets of Cyberscams," *San Francisco Chronicle* (March 20, 2010), www.sfgate.com/business/article/Law-firms-are-lucrative-targets-of-cyberscams-3269938.php.

[13] Michael A. Riley and Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data" *Bloomberg News* (January 31, 2012).

[14] Id.

hacked.[15] The attorneys said that the FBI told the law firm that "our files had been found on a server in another country. The server was used as a way station for sending data to a large Asian country." It was "all our files."

Effective information security is now a requirement for attorneys. In June, 2012, the *Wall Street Journal* published "Client Secrets at Risk as Hackers Target Law Firms."[16] It started with:

> Think knowing how to draft a contract, file a motion on time and keep your mouth shut fulfills your lawyerly obligations of competence and confidentiality?
>
> Not these days. Cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients' secrets are having to reboot their skills for the digital age.

Security threats to law firms continue to grow. In February, 2013, an FBI agent gave a keynote presentation on law firm security threats at LegalTech New York. In an article reporting on it, the special agent in charge of the FBI's cyber operations in New York City is quoted as stating:[17]

> "We have hundreds of law firms that we see increasingly being targeted by hackers. …We all understand that the cyberthreat is our next great challenge. Cyber intrusions are all over the place, they're dangerous, and they're much more sophisticated" than they were just a few years ago.

The *ABA Journal News* reported in April 2013 on a law firm security incident in which a North Carolina law firm became the victim of a phishing scam. Someone at the firm clicked on a link in phishing e-mail, enabling hackers to track a user's keystrokes and learn the firm's banking passwords. The hackers used the passwords to transfer $336,600 to an account in Moscow.[18]

In August, 2013, ILTA (the International Legal Technology Association) presented "The FBI and Experts Present Security Updates and Strategies for Firms of All Sizes" at its Annual Education Conference. An FBI speaker called the cyberattacks "a paradigm shift" and noted that attackers are "already in the system." Another speaker observed that several practice areas appear to be most vulnerable to attack, including oil and gas, technology, and technology patents.[19]

---

[15] SANS Institute, "Conversations about Cybersecurity," www.sans.org/security-resources/cybersecurity-conversations.

[16] Jennifer Smith, "Client Secrets at Risk as Hackers Target Law Firms," *Wall Street Journal Law Blog* (June 25, 2012), https://blogs.wsj.com/law/2012/06/25/dont-click-on-that-link-client-secrets-at-risk-as-hackers-target-law-firms.

[17] Evan Koblenz, "LegalTech Day Three: FBI Security Expert Urges Law Firm Caution," *Law Technology News* (February 1, 2013), www.lawtechnologynews.com/id=1202586539710?slreturn=20140103164728.

[18] Debra Cassens Weiss, *ABA Journal News*, "Law firm fell victim to phishing scam, precipitating $336K overseas wire transfer, bank suit alleges (April 4, 2013), www.abajournal.com/news/article/law_firm_fell_victim_to_phishing_scam_precipitating_336k_overseas_wire_tran.

[19] Monica Bay, "Bring in the FBI: Your Paranoia is Justified," *Law Technology News* (August 26, 2013).

Shane McGee, the general counsel and vice president of legal affairs at Mandiant Corp., explained the sophistication of attacks on law firms in a September, 2013 *ABA Journal* article:[20]

> Law firms need to understand that they're being targeted by the best, most advanced attackers out there … These attackers will use every resource at their disposal to compromise law firms because they can, if successful, steal the intellectual property and corporate secrets of not just a single company but of the hundreds or thousands of companies that the targeted law firm represents. Law firms are, in that sense, 'one-stop shops' for attackers.

At a security conference in October, 2014, Mandiant reported on a law firm data breach that it investigated. The attackers used the law firm's e-mail system as a platform to infiltrate biotechnology and pharmaceutical clients. The attackers first sent phishing e-mails to the law firm and used information stolen through them to take control of the e-mail system. They then sent e-mails with malicious attachments from the law firm e-mail system to individuals at clients who had received law firm e-mails with attachments in the past. When some of the client personnel opened the attachments, malware designed to steal information was installed on the clients' systems.[21]

The attackers used the law firm's e-mail system as a platform to infiltrate biotechnology and pharmaceutical clients.

In May of 2014, five Chinese military officers were indicted in federal court in Pittsburgh, charged with hacking attacks on energy companies, suppliers to them, a steel company and a labor union.[22] While the indictment does not include any charges for hacking a law firm, it does include targeting confidential attorney-client communications. While the hacking in the indictment was taking place, a law firm representing one of the energy companies was also successfully hacked. The firm represented the solar energy company in an antidumping matter against China.[23]

Although reports of law firm data breaches have been limited, breaches have been widespread. A March, 2015 article reports that "Cybersecurity firm Mandiant says at least 80 of the 100 biggest firms in the country, by revenue, have been hacked since 2011."[24]

---

[20] Joe Dysart, "New hacker technology threatens lawyers' mobile devices," *ABA Journal Law News Now* (September 1, 2103). www.abajournal.com/magazine/article/new_hacker_technology_threatens_lawyers_mobile_devices.

[21] BSides DC 2014, "Opening Acts: How Attackers Get Their Big Breaks" www.youtube.com/watch?v=j1JC59QjPQs.

[22] U.S. Department of Justice Press Release (May 19, 2014), www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[23] Michael Riley and Dune Lawrence, "Hackers Linked to China's Army Seen from EU to D.C." *Bloomberg Business* (July 26, 2012).

[24] Susan Hansen, "Cyber Attacks Upend Attorney-Client Privilege," *Bloomberg Businessweek* (March 19, 2015) www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security.

Law firm breaches continue to be in the headlines. On March 4, 2016, the FBI issued a Private Industry Alert directed to the legal profession about hacking for insider trading. Its summary states:

> A financially motivated cyber crime insider trading scheme targets international law firm information used to facilitate business ventures. The scheme involves a hacker compromising the law firm's computer networks and monitoring them for material, non-public information (MNPI). This information, gained prior to a public announcement, is then used by a criminal with international stock market expertise to strategically place bids and generate a monetary profit.

A few weeks later, *Crain's Chicago Business* reported that the scheme targeted nearly 50 elite law firms, including 48 major U.S. firms and two members of the UK's Magic Circle.[25] The same day, the *Wall Street Journal* reported that the hackers had broken into law firms:[26]

> Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading, according to people familiar with the matter.
>
> The firms include Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, which represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations.
>
> Other law firms also were breached, the people said, and hackers, in postings on the Internet, are threatening to attack more.

Also in March of 2016, the IRS issued an alert about a targeted spearphishing scheme in which cybercriminals were sending e-mails that appeared to be from target companies' CEOs to payroll and human resources staff asking for copies of W-2 tax forms. They then used the W-2s from those who responded to file fraudulent tax returns to obtain refunds.[27] The numerous victims who sent W-2s included a major law firm.[28]

In April of 2016, another law firm data breach made the headlines – Mossack Fonesca in Panama.[29] It has been called the largest volume data breach of all time (in millions of documents

---

[25] Claire Bushey, "Russian cybercriminal targets elite Chicago law firm," *Crain's Chicago Business* (March 29, 2016). www.chicagobusiness.com/article/20160329/NEWS04/160329840/russian-cyber-criminal-targets-elite-chicago-law-firms.

[26] Nicole Hong and Robin Didel, "Hackers Breach Law Firms, Including Cravath and Weil Gotshal," *Wall Street Journal* (March 29, 2016).

[27] Internal Revenue Service Alert IR-2016-34 (March 1, 2016) www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s.

[28] Steve Ragan, "Latest tax-related data breach could affect employees and their children," CSO Online (April 8, 2016) www.csoonline.com/article/3053658/security/latest-tax-related-data-breach-could-affect-employees-and-their-children.html.

[29] Jacob Gershman, "Law Firm at the Center of "Panama Papers" Leak," Wall Street Journal Blog (April 4, 2016)
http://blogs.wsj.com/law/2016/04/04/law-firm-at-the-center-of-panama-papers-leak.

and terabytes of data) and resulted in disclosure of the "Panama Papers." The papers disclosed details of "offshore financial activities of dozens of global leaders, businessmen and celebrities."

Also in April of 2016, a former IT engineer for Locke Lord LLP, a large Dallas-based law firm, was sentenced to 115 months in federal prison for an intrusion into the law firm's network.[30] The charges alleged that, after leaving the firm, he accessed the network and "issued instructions and commands that caused significant damage to the network, including deleting or disabling hundreds of user accounts, desktop and laptop accounts, and user e-mail accounts."

A growing threat to law firms and others, over the last few years, has been ransomware, which is malware that encrypts data in victims' computers and networks and requires the victim to pay ransom, usually by Bitcoin, to obtain the decryption key from the cybercriminal.[31] On April 21, 2016, the ABA sent a Cyber Alert about ransomware to members, including a link to an FBI alert on the subject.[32] The ABA has started to send this kind of Cyber Alert to its members at the request of the FBI's Cyber Division.

In April 2016, a class action was filed against a Chicago law firm, alleging that the firm exposed client information and failed to protect client data. The case was filed under seal in U.S. District Court in Chicago and was unsealed in December. The suit alleged critical vulnerabilities in the firm's internet based time-logging system, its virtual private network, and firm e-mail server. The suit does not allege an actual breach of the data, only that it was exposed.[33]

Following the 2016 disclosures of law firm data breaches, in-house counsel have been increasing their scrutiny of the security provided by outside law firms:[34]

> The vulnerability of law firms to cyberattacks, already one of the big legal stories of 2016, is back in the news now that a judge has unsealed a class action lawsuit alleging the firm Johnson & Bell doesn't adequately protect client information from hackers. In-house counsel say the lawsuit is a good reminder of the importance of questioning outside firms about their cybersecurity efforts.

---

[30] U.S. Justice Department Press Release (April 15, 2016), www.justice.gov/usao-ndtx/pr/former-law-firm-it-engineer-convicted-computer-intrusion-case-sentenced-115-months.

[31] E.g., Susan Hansen, "Cyber Attacks Upend Attorney-Client Privilege," *Bloomberg Businessweek* (March 19, 2015) www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security and Ed Silverstein, "Law Firm Among the Latest Victims of Ransomware Attack," *Legaltech News* (March 11, 2015).

[32] www.americanbar.org/content/dam/aba/administrative/cyberalert/ransomware.pdf.

[33] Cara Salvatore, "Chicago Firm Didn't Secure Client Data, Suit Says," *Law 360* (December 9, 2016), www.law360.com/articles/871103/chicago-firm-didn-t-secure-client-data-suit-says and Andrew Strickler, "Law Firm Hacking to Breed New Kind of Malpractice Suit," *Law 360* (December 12, 2016), www.law360.com/legalindustry/articles/871575.

[34] Jennifer Williams-Alvarez, "GCs Are Questioning Their Outside Counsel About Cybersecurity," *Legaltech News* (December 19, 2016), www.legaltechnews.com/id=1202775046830/GCs-Are-Questioning-Their-Outside-Counsel-About-Cybersecurity?slreturn=20170001184804.

In a July 2016 article, *Forbes* noted the following, after the law firm data breaches that were disclosed earlier in the year:[35]

> Law firms have been duly warned in recent years that their systems have been attacked (hacked) and breached and that the attacks will likely escalate and intensify. Recent developments present very real evidence that these warnings, from many sources, including the F.B.I., have been accurate and even understated. These developments should be a loud and clear wake-up call to law firm management to intensify efforts to secure the treasure trove of highly confidential, sensitive, proprietary and often *privileged* client and employee information. After all, client confidentiality is the life's blood of any attorney's practice.

"These developments should be a loud and clear wake-up call to law firm management…"

In-house attorneys are increasingly imposing security requirements on law firms, inquiring about law firm security, and using questionnaires and audits.

In December of 2016, a law firm received a phishing e-mail that appeared to be from the settlement administrator with wire payment instructions for funds due to plaintiffs in a wage and hour case. The law firm told the bank to make the $500,000 payment and the money disappeared. It appears that the scammers also intercepted and responded to e-mails from the settlement administrator inquiring about the overdue payment.[36]

On December 27, 2016, the U.S. Department of Justice announced the arrest of one individual and indictment of 3 others in connection with the inside trading scheme about which it warned law firms earlier in 2016. The press release included:[37]

> The Defendants are charged with devising and carrying out a scheme to enrich themselves by obtaining and trading on material, nonpublic information ("Inside Information"), exfiltrated from the networks and servers of multiple prominent U.S.-based international law firms with offices in New York, New York (the "Victim Law Firms"), which provided advisory services to companies engaged in corporate mergers and acquisitions ("M&A transactions"). The defendants targeted at least seven law firms as well as other entities in an effort to unlawfully obtain valuable confidential and proprietary information.
>
> ***
>
> As alleged, from April 2014 through late 2015, the Defendants successfully obtained Inside Information from at least two of the Victim Law Firms (the

[35] Jack Vaughan, "Is Cyber Risk an Existential Threat to The Legal Sector? *Forbes* (July 13, 2016). www.forbes.com/sites/riskmap/2016/07/13/is-cyber-risk-an-existential-threat-to-the-legal-sector/#5dab531e1f0e.

[36] Bonnie Eslinger, "Law Firm Duped by Email Scammers in Wage and Hour Case," *Law360* (August 23, 2017) www.law360.com/articles/957163/law-firm-duped-by-email-scammers-in-wage-and-hour-case.

[37] U.S. Department of Justice Press Release, December 26, 2016, www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against.

> "Infiltrated Law Firms") by causing the networks and servers of these firms to be hacked. Once the Defendants obtained access to the law firms' networks, the Defendants targeted email accounts of law firm partners who worked on high-profile M&A transactions. …They allegedly hacked into two prominent law firms, stole the emails of their M&A partners, and made over $4 million in illegal profits.

A number of law firms have continued to be victims of the W-2 tax form spearphishing scheme. For example, a large law firm notified the Maryland Attorney General in February 2017, under the Maryland data breach notice law, that the 2016 W-2s of current and former employees had been compromised in response to one of these e-mails.[38]

In March 2017, a Providence, RI law firm filed a lawsuit against its insurance carrier, seeking coverage for losses from a ransomware attack on the firm in 2016. The firm sought coverage for $700,000 it lost from being locked out of its computers for months.[39]

The FBI published a Public Service Announcement in May 2017, which warned that Business E-mail Compromise (BEC) is now a $5 billion scam – reporting on worldwide losses between October 2013 and December 2016. It lists five scenarios that these schemes commonly use:[40]

> Scenario 1: Business Working with a Foreign Supplier
>
> Scenario 2: Business Executive Receiving or Initiating a Request for a Wire Transfer
>
> Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail
>
> Scenario 4: Business Executive and Attorney Impersonation
>
> Scenario 5: Data Theft

Attorneys and law firms have been victims of these kinds of BEC schemes. For example, in November 2016, an email account was hacked and a criminal used it to send fraudulent wire transfer instructions on law firm letterhead for the proceeds of a real estate transaction. The realtor transferred $180,000 to the fraudulent account.[41]

A cyberattack rapidly spread across the globe in late June 2017, infecting targets in Europe, Asia, South America and the U.S., including at least 64 large

---

[38] See, www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-280157%20(1).pdf.

[39] R. Strom, "Will Ransomware Attack Make Law Firms WannaCry?" *The American Lawyer* (May 15, 2107), http://www.americanlawyer.com/id=1202786228047/Will-Ransomware-Attack-Make-Law-Firms-WannaCry.

[40] FBI Public Service Announcement I-050417-PSA (May 4, 2017), www.ic3.gov/media/2017/170504.aspx.

[41] KrebsonSecurity, "Blind Trust in Email Could Cost You Your Home" (April 27, 2017), https://krebsonsecurity.com/2017/04/blind-trust-in-email-could-cost-you-your-home.

companies. The attack used a combination of techniques to break into networks and then spread across them.[42] One of the early reported victims was DLA Piper, a major multinational law firm that had its computers and phone systems shut down across the firm – including offices in the U.S., UK, Europe and the Middle East.[43]

This information on the law firm data breaches is consistent with breaches generally - many are found by third-parties and many are discovered after an extended time. Mandiant has reported that in 2016, 47% of data breaches were discovered by an external party and 53% were discovered internally. The median time for discovery of a data breach in 2016 was 99 days, down from 146 days in 2015. In 2016 median time for external discovery was 107 days and 80 days for internal discovery.[44]

Lost and Stolen Devices

While the large-scale hacking attacks can make attention-grabbing headlines, law firms also continue to face smaller scale, yet still serious, security incidents, like lost or stolen laptops, tablets, smartphones, and USB drives. For example, a Maryland law firm lost an unencrypted portable hard drive containing medical information when an employee left it on a light rail train.[45] The idea was good – take it offsite for backup – but the execution was a security risk – it wasn't encrypted.

It happened again in June, 2014. A Georgia-based criminal defense firm reported that a backup drive containing personal information, including Social Security numbers, was stolen from an employee's locked trunk.[46] It was not encrypted.

Once again in January of 2015. A San Francisco attorney reported theft of a laptop "that contained identifying client information including names, social security numbers and dates of birth."[47]

And again, in April, 2015. A laptop owned by an attorney from a California law firm was stolen on a San Diego trolley. The laptop reportedly contained names, addresses, telephone numbers,

---

[42] D. Goodin, "A new ransomware outbreak similar to WCry is shutting down computers worldwide," *Ars Technia* (6/27/17), https://arstechnica.com/security/2017/06/a-new-ransomware-outbreak-similar-to-wcry-is-shutting-down-computers-worldwide.

[43] J. Booth, "DLA Piper Hit By Cyber Attack, Phones and computers Down Across the Firm," Law.com (June 27, 2017), www.law.com/sites/almstaff/2017/06/27/dla-piper-hit-by-cyber-attack-phones-and-computers-down-across-the-firm.

[44] Mandiant, *M-Trends 2016* and *M-Trends 2017,* www.fireeye.com/current-threats/annual-threat-report.html.

[45] Tricia Bishop, "Law Firm Loses Hard Drive with Patient Records," *Baltimore Sun* (October 10, 2010) http://articles.baltimoresun.com/2011-10-10/news/bs-md-stent-hard-drive-20111010_1_patient-records-law-firm-medical-records.

[46] Adam Greenberg, "Backup hard drive stolen from law firm contained personal information," *SC Magazine* (August 27, 2014) www.scmagazine.com/backup-hard-drive-stolen-from-law-firm-contained-personal-info/article/368427.

[47] https://oag.ca.gov/system/files/Security%20Breach%20Notice_0.pdf.

Social Security numbers, and possibly certain financial information or medical records. It does not appear to have been encrypted.[48]

These are some examples that made the press. There certainly have been many more.

Inside Threats

In addition to threats from criminals and hackers and loss and theft of laptops and mobile devices, law firms, like other businesses and enterprises, also face threats from the inside. The insider threat includes a spectrum of trusted employees and third-parties with access - ranging from criminal, to malicious, to disgruntled, to untrained, to careless, to bored, to honestly mistaken. It even includes dedicated employees who just want to use their own technology to better do their jobs. Unauthorized hardware, software, and services can be a threat from insiders in any of these groups. An international survey of IT security professionals reported that 41% of those surveyed viewed rogue employees as the biggest threats to their organizations.[49]

Another survey reported the following on the scope of the risk from employee use of their own technology:[50]

> It's out there: lurking in cubicles, infiltrating boardrooms, pulsing through desktops and laptops and tablets. Viral. Relentless. Unstoppable.
>
> Rogue IT is the name given to the informal, ad hoc software and devices brought by employees into the workplace. If you've ever taken your own iPad to work or used cloud-based software like Evernote or Dropbox in the office, you may well be an offender. And you're not alone. Some 43% of businesses report that their employees are using cloud services independently of the IT department, according to a recent survey of 500 IT decision makers.

A recognized security consultant has summarized the accidental insider threat this way:[51]

> Much is misunderstood today about the evolving insider threat. …In particular, senior leaders need to realize that their greatest risks aren't from rogue employees looking to cause damage, but rather from inadvertent breaches caused by staffers who simply stumble into costly mistakes.

---

[48] Adam Greenberg, "Personal data on laptop stolen from attorney from California law firm," SC Magazine (July 23, 2015) www.scmagazine.com/personal-data-on-laptop-stolen-from-attorney-with-california-law-firm/article/428222.

[49] Avetco Press Release (June 7, 2013), www.avecto.com.

[50] Ryan Holmes, "'Rogue IT' is About to Wreak Havoc at Work," *Fortune* (August 9, 2012) http://fortune.com/2012/08/09/rogue-it-is-about-to-wreak-havoc-at-work.

[51] Tom Field, "Insider Threat: 'You Can't Stop Stupid,'" *BankInfoSecurity*, Interview with Eric Cole (July 28, 2010) www.bankinfosecurity.com/insider-threat-you-cant-stop-stupid-a-2789/op-1.

The FBI's Chief Information Security Officer expressed the same concern in a presentation on the FBI's insider threat program at the 2013 RSA Security Conference.[52] The FBI's program was created after the 2001 Robert Hanssen incident in which an FBI agent was caught stealing information and selling it to the Russians. The CISO noted that authorized users with a level of organizational trust, who are doing legitimate activities with malicious intent, pose the biggest threat. But a quarter of the incidents that the FBI tracks in its systems on an annual basis are from "knucklehead" problems: unintentional acts in which employees compromise systems by not following procedures, losing equipment and sensitive data, clicking on spam, inappropriate e-mails or Web links, or mishandling passwords and accounts. He said the FBI IT staff spends about 35% of its response time on these types of incidents.

Insider security incidents are often not publicly disclosed unless they lead to criminal prosecution or were required by data breach notice laws. For this reason, the availability of statistics and examples is limited. There are several reported incidents of loss or theft of law firm laptops, smartphones and mobile devices. There likely have been many more.

There are also older examples of intentional insider threats in law firms that illustrate the risks. A former Manhattan paralegal was sentenced to prison after pleading guilty to downloading his firm's 400-page electronic trial plan for an asbestos case and offering to sell it to opposing counsel.[53] In another example, a college student who worked for a service provider at a law firm pled guilty to theft of intellectual property.[54] The student was brought in to help by his uncle, an employee of the service provider, because they were behind on the job. The firm represented DirectTV in litigation with one of its security vendors. The student worked in a secure area in the law firm's offices, where he copied paper and electronic data for production in the litigation. He found the technology that controlled access by customers to DirectTV, copied it to a CD, and posted it on a hacker bulletin board. In a third example, a former IT employee of a large law firm pled guilty to theft of 156 computers and monitors from the law firm that he sold on eBay for over $74,000.[55] More recently, a Pennsylvania law firm sued a former attorney, alleging that he took thousands of client files using Dropbox.[56]

Government Surveillance

In addition to these other growing threats, a current concern for security and confidentiality for attorneys, particularly those representing foreign clients or clients engaged in international transactions, is government surveillance – both by the U.S. government and foreign

---

[52] Ericka Chickowski, "5 Lessons from the FBI Insider Threat Program," *Dark Reading* (March 1, 2013).

[53] U.S. Department of Justice Press Release, "Manhattan Paralegal Sentenced for Theft of Litigation Trial Plan," (January 30, 2002).

[54] U.S. Department of Justice Press Release, "L.A. Man Pleads Guilty to Theft of Trade Secrets for Stealing Information to DirecTV 'Smart Card,'" (April 28, 2003).

[55] U.S. Department of Justice Press Release, "Second Former Law Firm Employee Sentenced in Connection with Theft of Computers from Law Firm," (April 20, 2009).

[56] Debra Cassens Weiss, "Suit Claims Ex-Partner Installed Software Allowing Continued Access to Law Firm Files, *ABA Journal Law News Now* (February 13, 2012).

governments. In August of 2013, the ABA adopted a resolution, recommended by the ABA Cybersecurity Legal Task Force, condemning intrusions into attorneys' systems and networks, including those by governments.[57] It included the following:

> **RESOLVED**, That the American Bar Association condemns unauthorized, illegal governmental, organizational and individual intrusions into the computer systems and networks utilized by lawyers and law firms.

In February of 2014, the *New York Times* reported that documents leaked by Edward Snowden showed that an American law firm had been monitored by the Australian Signals Directorate, an NSA ally, while the law firm was representing a foreign government in trade disputes with the U.S.[58] Following this report, ABA President James Silkenat wrote to the Director and General Counsel of the NSA about this incident, including:[59]

> I write to express our concerns over allegations raised in recent press reports concerning possible foreign government surveillance of American lawyers' confidential communications with their overseas clients, the subsequent sharing of privileged information from those communications with the National Security Agency ("NSA"), and the possible use of that information by the U.S. Government or third parties."

NSA Director, General Keith Alexander, responded, stating:[60]

> NSA is firmly committed to the rule of law and the bedrock legal principle of attorney-client privilege, which as you noted, is one of the oldest recognized privileges for confidential communications.
>
> ***
>
> Let me be absolutely clear: NSA has afforded, and will continue to afford, appropriate protection to privileged attorney-client communications acquired during its lawful foreign intelligence mission in accordance with privacy procedures required by Congress, approved by the Attorney General, and, as appropriate, reviewed by the Foreign Intelligence Surveillance Court."

---

[57] www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf.

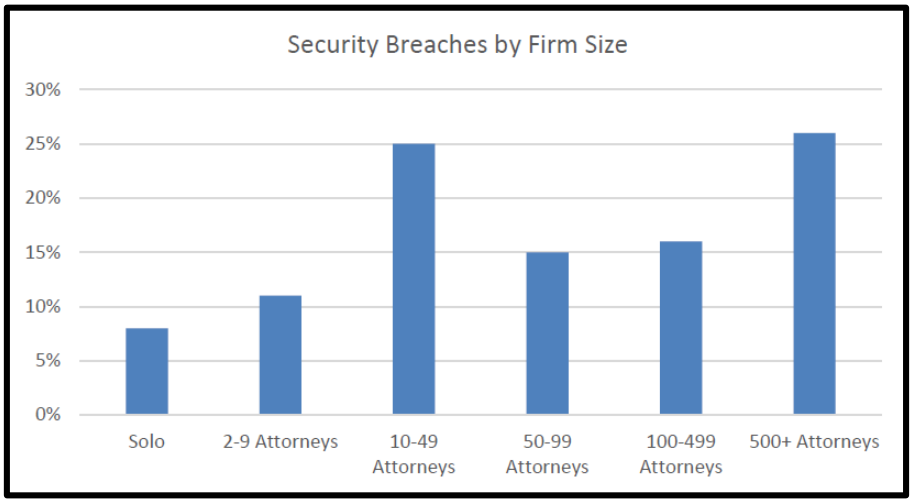
[58] James Risen and Laura Poitras, "Spying by N.S.A. Ally Entangles U.S. Law Firm," *New York Times* (February 15, 2014), www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0.

[59] Letter dated February 20, 2014, www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_privilegedinformation_l.authcheckdam.pdf.

[60] Letter dated March 10, 2014, www.americanbar.org/content/dam/aba/images/abanews/nsa_response_03102014.pdf.

Summary of Threats

As these examples of security incidents of all kinds demonstrate, law firm data faces continuing and growing threats. The American Bar Association's *2016 Technology Survey*[61] reports that 14% of all responding attorneys reported that their firm had suffered a security breach at some time in the past. This compares with 15% overall in 2015, 14% in 2014, and 15% in 2013— steady since 2013. "Security breach" is defined broadly, "lost/stolen computer or smartphone, hacker, break-in, website exploit." Data is broken down by size of firm, with the percentage reporting breaches generally increasing with firm size, with 25% for firms with 10 to 49 attorneys and 26% for firms with 500 or more attorneys:



Source: *ABA TECHREPORT Security* (2016)

A number of responding attorneys reported that they didn't know whether their firm had suffered a security breach in the past – 21% of all firms, increasing from 4 % for solos to 63% in the largest firms.

A recent article, providing a pre-release review of a cybersecurity survey of more than 200 law firms, found that more than 66% of firms reported having a breach of some variety – a substantially higher percentage than the ABA survey.[62]

Legal data is targeted in law firms, clients, and other businesses and organizations. *The 2016 SANS Incident Response Survey* reports that legal data was exfiltrated in 14.5% of data breaches in 2015 and 12% in 2016 in data breaches of all kinds of organizations.[63]

---

[61] *ABA TECHREPORT 2016 Security,* www.americanbar.org/groups/law_practice/publications/techreport/2016/security.html.

[62] M. Daniels, "How to Stay Safe in a World of Law Firm Data Breaches," *Law 360* (June 22, 2017), www.law360.com/articles/937681/how-to-stay-safe-in-a-world-of-law-firm-data-breaches.

[63] M. Bromiley, *Incident Response Capabilities in 2016 : The 2016 SANS Incident Response Survey* (June 2016), www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047.

The greatest security threats to attorneys and law firms today are most likely spearphishing, ransomware, and lost and stolen laptops and mobile devices.

Security threats to lawyers and law firms continue to be substantial, real, and growing – security incidents and data breaches have occurred and are occurring. It is critical for attorneys and law firms to recognize these threats and address them through comprehensive information security programs.

Duty to Safeguard

Attorneys' use of technology presents special ethics challenges, particularly in the areas of competence and confidentiality. Attorneys also have common law duties to protect client information and often have contractual and regulatory duties.

These duties to safeguard information relating to clients are minimum standards with which attorneys are required to comply. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service.

> **Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.**

A. Ethics Rules

The duty of competence (ABA Model Rule 1.1) requires attorneys to know what technology is necessary and how to use it. The duty of confidentiality (ABA Model Rule 1.6) is one of an attorney's most fundamental ethical responsibilities. Together, these rules require attorneys using technology to take competent and reasonable measures to safeguard client data. This duty extends to all use of technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

Model Rule 1.1 covers the general duty of competence. It provides that "A lawyer shall provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It includes competence in selecting and using technology. It requires attorneys who lack the necessary technical competence for security to consult with qualified people who have the requisite expertise.

Model Rule 1.4, Communications, also applies to attorneys' use of technology. It requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent." It requires notice to a client of a compromise of confidential information relating to the client.

Model Rule 1.6 generally defines the duty of confidentiality. It begins as follows:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b). . .

Rule 1.6 broadly requires protection of "information relating to the representation of a client;" it is not limited to confidential communications and privileged information. Disclosure of covered information generally requires express or implied client consent (in the absence of special circumstances like misconduct by the client).

The ABA Commission on Ethics 20/20 conducted a review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. One of its core areas of focus was technology and confidentiality. Its Revised Draft Resolutions in this area were adopted by the ABA at its Annual Meeting in August of 2012.[64]

The 2012 amendments include addition of the following underlined language to the Comment to Model Rule 1.1 Competence:

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>…

As of March 2017, 27 states have adopted the new comment to Model Rule 1.1, some with variations from the ABA language.[65] Andrew Perlman, the Reporter of the Ethics 20/20 Commission, has described cybersecurity as one of the critical competencies in attorneys' use of technology.[66]

The amendments also added the following new subsection (underlined) to Model Rule 1.6 Confidentiality of Information:

> <u>(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.</u>

This requirement covers two areas – inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop, or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, producing privileged documents or data in litigation, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

The amendments also include the following changes to Comment [18] to this rule:

> **Acting Competently to Preserve Confidentiality**

---

[64] www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.

[65] www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html.

[66] Andrew Perlman, "The Twenty-First Lawyer's Evolving Ethical Duty of Competence," *The Professional Lawyer* (December 2014) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2532995.

[18] Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

Significantly, these revisions make explicit what is already required rather than making substantive changes. They are consistent with the then existing rules and comments, ethics opinions, and generally accepted information security principles.[67]

Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) was amended to expand its scope. "Assistants" was expanded to "Assistance," extending its coverage to all levels of staff and outsourced services ranging from copying services to outsourced legal services. This requires attorneys to employ reasonable safeguards, like due diligence, contractual requirements, supervision, and monitoring, to ensure that nonlawyers, both inside and outside a law firm, provide services in compliance with an attorney's duty of confidentiality.

---

[67] ABA Commission on Ethics 20/20, *Report to Resolution 105A Revised* (2012): "The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent." (Model Rule 1.1.) "This duty is already described in several existing Comments, but the Commission concluded that, in light of the pervasive use of technology to store and transmit confidential client information, this existing obligation should be stated explicitly in the black letter of Model Rule 1.6."

Ethics Opinions

A number of state ethics opinions for over a decade have addressed professional responsibility issues related to security in attorneys' use of various technologies. Consistent with the Ethics 20/20 amendments, they generally require competent and reasonable safeguards. The most recent opinion, ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 2017) (discussed at the end of this section and in the following section) also requires competent and reasonable efforts to protect information relating to clients. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

An early example is State Bar of Arizona, Opinion No. 05-04 (July 2005) (Formal Opinion of the Committee on the Rules of Professional Conduct). It requires "competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence" and "competent and reasonable measures to assure that the client's electronic information is not lost or destroyed." It further explains that "an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence."

"…competent and reasonable measures to assure that the client's electronic information is not lost or destroyed."

Additional examples include New Jersey Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage and Access of Client Files" (April, 2006), State Bar of Arizona, Opinion No. 09-04 (December, 2009): "Confidentiality; Maintaining Client Files; Electronic Storage; Internet" (Formal Opinion of the Committee on the Rules of Professional Conduct); State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179; and New York State Bar Association Ethics Opinion 1019, "Confidentiality; Remote Access to Firm's Electronic Files," (August, 2014).

Significantly, California Formal Opinion No. 2010-179 advises attorneys that they must consider security ***before*** using a particular technology in the course of representing a client. It notes that attorneys "must take appropriate steps to evaluate," among other considerations, "the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security." Depending on the circumstances, an attorney may be required to avoid using a particular technology or to advise a client of the risks and seek informed consent if appropriate safeguards cannot be employed. The opinion covers use of a firm-issued laptop and use of public and home wireless networks.

***"Before* using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate the security."**

New York Opinion 1019 cautions attorneys to analyze necessary precautions in the context of current risks:

> Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including

> trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system.

The opinion leaves it up to attorneys and law firms to determine the specific precautions that are necessary:

> Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information.

Like California Opinion 2010-179, it requires attorneys to either make a determination that the selected precautions provide reasonable protection, in light of the risks, or to obtain informed consent from clients after explaining the risks.

ABA Formal Opinion 08-451, "Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services" (August 2008), covers attorneys' ethical duties when using outsourcing of all kinds, including technology. It lists as examples, among others, the retention of a document management company for the creation and maintenance of a database for complex litigation and the use of a third-party vendor to provide and maintain a law firm's computer system. The opinion expressly requires protection of confidentiality. These requirements are included in amended Model Rule 5.3.

Attorneys need to stay up to date as technology changes and new threats are identified. For example, following news reports that confidential information had been found on digital copiers that were ready for resale,[68] the Florida Bar issued Professional Ethics of the Florida Bar Opinion 10-2 (September, 2010) that addresses this risk. Its conclusion states:

> In conclusion, when a lawyer chooses to use Devices that contain Storage Media, the lawyer must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition. These reasonable steps include: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the

[68] E.g., Armen Keteyian, "Digital Copiers Loaded with Secrets," *CBS Evening News* (April 19, 2010). www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets.

> Device and confirmation or certification of the sanitization at the disposition of the Device.

There are now multiple ethics opinions on attorneys' use of cloud computing services like online file storage and software as a service (SaaS).[69] For example, New York Bar Association Committee on Professional Ethics Opinion 842 "Using an outside online storage provider to store client confidential information" (September, 2010), consistent with the general requirements of the ethics opinions above, concludes:

> A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6. A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.

Additional examples of opinions covering cloud services are Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200, "Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (November, 2011) and North Carolina State Bar 2011 Formal Ethics Opinion 6, "Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (January, 2012).

The North Carolina State Bar recently issued 2015 Formal Ethics Opinion 6, "Lawyer's Professional Responsibility When Third Party Steals Funds from Trust Account" (October 2015) that applies the duty of reasonable measures to safeguard client funds. Interpreting the state equivalent of Model Rule 1.15, Safeguarding Property, to 7 different inquiries. Its headnote states:

> *Opinion rules that when funds are stolen from a lawyer's trust account by a third party who is not employed or supervised by the lawyer, and the lawyer was managing the trust account in compliance with the Rules of Professional Conduct, the lawyer is not professionally responsible for replacing the funds stolen from the account.*

Significantly, in one example, the opinion concludes that the lawyer would have an ethical obligation to reimburse a client for real estate closing funds that the lawyer wire transferred to

---

[69] The ABA Legal Technology Resource Center has published a summary with links, "Cloud Ethics Opinions around the U.S.," available at www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

a hacker's bank account in response to a spoofed e-mail, where the lawyer did not verify the change in disbursement instructions.

The opinion is limited to a lawyer's professional responsibility requirements and does not opine on a lawyer's legal liability.

The most recent opinion in this area is ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 2017). While focusing on electronic communications (as discussed Section 2 D below), it also explores the general duties to safeguard information relating to clients, in light of current threats and the Ethics 20/20 technology amendments to the Model Rules. As noted above, it states the following about threats:

> At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of "when," and not "if." Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

It applies Model Rules 1.1: Competence and 1.6: Confidentiality of Information, as amended, to define the ethical requirements of competent and reasonable safeguards. Its conclusion includes:

> Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

The key professional responsibility requirements from these various opinions on attorneys' use of technology are **competent and reasonable measures to safeguard client data**, including an understanding of limitations in attorneys' competence, obtaining appropriate assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available safeguards evolve. They also require obtaining clients' informed consent in some circumstances.

Ethics Rules – Electronic Communications

E-mail and electronic communications have become everyday communications forms for attorneys and other professionals. They are fast, convenient, and inexpensive, but also present serious risks. It is important for attorneys to understand and address these risks.

In addition to adding the requirement of competent safeguards to protect confidentiality to the Comments to Rule 1.6, the Ethics 2000 revisions to the Model Rules, over 10 years ago, also added Comment 17 [now 19] to Rule 1.6. This comment requires reasonable precautions to

safeguard and preserve confidential information during electronic transmission. This Comment, as amended in accordance with the Ethics 20/20 recommendations (underlined), provides:

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. <u>Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.</u>

This Comment requires attorneys to take "reasonable precautions" to protect the confidentiality of electronic communications. Its language about "special security measures" has often been viewed by attorneys as providing that attorneys never need to use "special security measures" like encryption.[70] While it does state that "special security measures" are not generally required, it contains qualifications and notes that "special circumstances" may warrant "special precautions." It includes the important qualification - "if the method of communication affords a reasonable expectation of privacy." There are, however, questions about whether Internet e-mail affords a reasonable expectation of privacy.

Respected security professionals for years have compared unencrypted e-mail to postcards or postcards written in pencil.[71] A June 2014 post by Google on the *Google Official Blog*[72] and a July

---

[70] Encryption is a process that translates a message into a protected electronic code. The recipient (or anyone intercepting the message) must have a key to decrypt it and make it readable. E-mail encryption has become easier to use over time. Transport layer security (TLS) encryption is available to automatically encrypt e-mail between two e-mail gateways. If a law firm and client each have their own e-mail gateways, TLS can be used to automatically encrypt all e-mails between them. A virtual private network is an arrangement in which all communications between two networks or between a computer and a network are automatically protected with encryption. See, David G. Ries and John W. Simek, "Encryption Made Simple for Lawyers," *GPSolo Magazine* (November/December 2012).

[71] E.g., B. Schneier, *E-Mail Security - How to Keep Your Electronic Messages Private,* (John Wiley & Sons, Inc. 1995) p. 3, B. Schneier, *Secrets & Lies: Digital Security in a Networked Work*, (John Wiley & Sons, Inc. 2000) p. 200, and Larry Rogers, *Email – A Postcard Written in Pencil*, Special Report, (Software Engineering Institute, Carnegie Mellon University 2001).

[72] "Transparency Report: Protecting Emails as They Travel Across the Web," *Google Official Blog* (June 3, 2014).

http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html.

2014 *New York Times* article[73] use the same analogy – comparing unencrypted e-mails to postcard:

Reasonable expectation of privacy?

"The common metaphor for Internet e-mail is postcards: Anyone – letter carriers, mail sorters, nosy delivery truck drivers - who can touch the postcard can read what's on the back."

Bruce Schneier 1995

Email – A Postcard Written in Pencil

Larry Rogers 2001

SEI - Carnegie Mellon University

"Emails that are encrypted as they're routed from sender to receiver are like sealed envelopes, and less vulnerable to snooping—whether by bad actors or through government surveillance—than postcards."

***Google Official Blog* June 2014**

"Security experts say email is a lot more like a postcard than a letter inside an envelope, and almost anyone can read it while the note is in transit."

***New York Times* July 2014**

Encryption is being increasingly required in areas like banking and health care. Newer laws in Nevada[74] and Massachusetts[75] (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like these, it will become more difficult for attorneys to demonstrate that confidential client data that they transmit needs lesser protection.

---

[73] Molly Wood, "Easier Ways to Protect Email from Unwanted Prying Eyes," *New York Times* (July 16, 2014).

www.nytimes.com/2014/07/17/technology/personaltech/ways-to-protect-your-email-after-you-send-it.html?_r=0.

[74] Nev. Rev. Stat. 603A.010, *et seq.*

[75] Mass. Gen. Laws Ch. 93H, regulations at 201 CMR 17.00.

Comment 19 to Rule 1.6 also lists "the extent to which the privacy of the communication is protected by law" as a factor to be considered. The federal Electronic Communications Privacy Act[76] and similar state laws make unauthorized interception of electronic communications a crime. Some observers have expressed the view that this should be determinative and attorneys are not required to use encryption. The better view is to treat legal protection as only one of the factors to be considered. As discussed below, some of the newer ethics opinions conclude that encryption may be a reasonable measure that should be used, particularly for highly sensitive information.

Ethics Opinions – Electronic Communications

An ABA ethics opinion in 1999 and several state ethics opinions have concluded that special security measures, like encryption, are not generally required for confidential attorney e-mail.[77] However, these opinions should be carefully reviewed because, like Comment 19, they contain qualifications that limit their general conclusions. In addition, more recent ethics opinions, discussed below, are increasingly recognizing that encryption may be a required safeguard in some circumstances.

As an example of the earlier approach, New York Bar Association Committee on Professional Ethics Opinion 709 "Use of Internet to advertise and to conduct law practice focusing on trademarks; use of Internet e-mail; use of trade names" (September, 1998) concludes:

> We therefore conclude that lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidentiality … to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use e-mail for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an

---

[76] 18 U.S.C. §§ 2510 et seq.

[77] E.g., ABA Formal Opinion No. 99-413, *Protecting the Confidentiality of Unencrypted E-Mail* (March 10, 1999) ("based upon current technology and law as we are informed of it …a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a)…" "…this opinion does not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.") and District of Columbia Bar Opinion 281, "Transmission of Confidential Information by Electronic Mail," (February, 1998), ("In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.").

> extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail.
>
> A lawyer who uses Internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost. It is also sensible for lawyers to discuss with clients the risks inherent in the use of Internet e-mail, and lawyers should abide by the clients' wishes as to its use.

This opinion, like the Comment, concluded that attorneys may use unencrypted e-mail "in ordinary circumstances," but added some qualifications, including available safeguards to reduce risk.

Consistent with the questions raised by security experts about the security of unencrypted e-mail, some ethics opinions express a stronger view that encryption may be required. For example, New Jersey Opinion 701 (April, 2006), discussed above, notes at the end: "where a document is transmitted to [the attorney] … by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access."[78] This was over ten years ago.

California Formal Opinion No. 2010-179, also discussed above, notes that "encrypting email may be a reasonable step for an attorney in an effort to ensure the confidentiality of such communications remain so when circumstances call for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous."

An Iowa opinion on cloud computing suggests the following as one of a series of questions that attorneys should ask when determining appropriate protection: "Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?" Iowa Ethics Opinion 11-01.

A Pennsylvania ethics opinion on cloud computing concludes that "attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality." It discusses encryption as an additional precaution that may be required when using services like web mail. Pennsylvania Formal Opinion 2011-200.

Texas Ethics Opinion 648 (2015) takes the same approach:

> In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information

[78] File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip uses encryption to protect security. It is generally easier to use than encryption of e-mail and attachments. However, the protection can be limited by use of weak passwords that are easy to break or "crack."

will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication.

It includes examples of circumstances where encryption may be required.

Summarizing these more recent opinions, a July, 2015 ABA article notes:[79]

> **"The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue [ethics] opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required."**
>
> **ABA, *Eye on Ethics* (July 2015)**

ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 2017), consistent with these newer opinions and the article, concludes:

> Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.
>
> A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

The opinion lists 7 factors for the fact-based consideration of necessary safeguards:

1. Understand the Nature of the Threat.
2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.
3. Understand and Use Reasonable Electronic Security Measures.
4. Determine How Electronic Communications About Clients Matters Should Be Protected.
5. Label Client Confidential Information.
6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

---

[79] Peter Geraghty and Susan Michmerhuizen, "Encryption Conniption," *Eye on Ethics, Your ABA* (July 2015) www.americanbar.org/publications/youraba/2015/july-2015/encryption-conniption.html.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

The Opinion references the Ethics 20/20 amendments to Comment 18 to Rule 1.6, which lists the following factors for determining reasonable and competent efforts:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

It includes observations that:

- "What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method."

"…[P]articularly strong protective measures, like encryption, are warranted in some circumstances."

- "A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances."
- "Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication."
- "However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email."
- "Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable."

In addition to complying with any applicable ethics and legal requirements, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients (preferably in an engagement letter or other writing) about the nature of communications that will be (and will not be) sent electronically and whether or not encryption and other security measures will be utilized.

It has now reached the point where all attorneys should have encryption available for use in appropriate circumstances.

Common Law Duties

Along with these ethical duties, there are also parallel common law duties defined by case law in the various states. The Restatement (3rd) of the Law Governing Lawyers (2000) summarizes this

area of the law. See, Section 16(2) on competence and diligence, Section 16(3) on complying with obligations concerning client's confidences, and Chapter 5, "Confidential Client Information." Breach of these duties can result in a malpractice action.

There are also instances when lawyers have contractual duties to protect client data. This is particularly the case for clients in regulated industries, such as health care and financial services, that have regulatory requirements to protect privacy and security. Clients are increasingly recognizing, sometimes after being pressed by regulators, that law firms may be the weak links in protecting their confidential information. They are increasingly requiring specified safeguards, providing questionnaires about a law firm's security, and even requiring security audits.[80]

In March of 2017, the Association of Corporate Counsel (ACC) published the *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information.*[81] The Model Controls provide a list of baseline security measures and controls that legal departments can consider requiring from outside counsel. They include 13 areas of measures and controls, with subparts, that companies can select as requirements for outside counsel, such as Policies and Procedures, Data Handling (including encryption), Data Security Breach Reporting, and Physical Security.

Laws and Regulations Covering Personal Information

In addition to the ethical and common law duties to protect client information, various state and federal statutes and regulations require protection of defined categories of personal information. Some of them are likely to apply to lawyers who possess any covered personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses.

At least 14 states now have general information security laws that require reasonable measures to protect defined categories of personal information (including Arkansas, California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Nevada, New Jersey, New York, Oregon, Rhode Island, Texas, and Utah). While the scope of coverage, the specificity of the requirements and the definitions vary among these laws, "personal information" is usually defined to include general or specific facts about an identifiable individual. The exceptions tend to be information that is presumed public and does not have to be protected (e.g., a business address).

---

[80] Kenneth N. Rashbaum, Jason M. Tenenbaum and Liberty McAteer, "Cybersecurity: Business Imperative for Law Firms," *New York Law Journal* (December 10, 2014) www.newyorklawjournal.com/id=1202678493487/Cybersecurity-Business-Imperative-for-Law-Firms?slreturn=20141127155939 and Sharon D. Nelson & John W. Simek, "Clients Demand Law Firm Cyber Audits," *Law Practice* (November/December 2013) www.americanbar.org/publications/law_practice_magazine/2013/november-december/hot-buttons.html.

[81] Available at: www.acc.com/aboutacc/newsroom/pressreleases/outsidecounselcybersecurityguidelines.cfm.

The most comprehensive law of this type to date is a Massachusetts law,[82] which applies to "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." Covered "personal information" includes Social Security numbers, driver's license numbers, state-issued identification card numbers, financial account numbers and credit card numbers. With its broad coverage of "persons," this law is likely to be applied to persons nationwide, including attorneys and law firms, when they have sufficient contacts with Massachusetts to satisfy personal jurisdiction requirements. It requires covered persons to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards."

The implementing regulation[83] for the Massachusetts law became effective in 2010. In addition to requiring a comprehensive information security program, including a risk assessment, the regulation contains detailed requirements for the information security program and detailed computer system security requirements. The security requirements include:

- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly; and
- Encryption of all personal information stored on laptops or other portable devices.

Additional system security requirements in the Massachusetts regulation are secure user authentication, secure access control, reasonable monitoring to detect unauthorized access, reasonably up-to-date firewall protection, reasonably up-to-date security software (including current patches and virus definitions), and education and training of employees.

Lawyers and law firms should think about and understand the consequences of the Massachusetts law, as some observers believe that it will become a model for comprehensive protection of personal information.

Nevada also has laws that require "reasonable security measures" and encryption[84] although they are much less detailed than the Massachusetts law. Note too that encryption is already required for federal agencies that have information about individuals on laptops and portable media. As encryption becomes a legal requirement in areas like these, it is likely to become the standard of what is reasonable for lawyers.

---

[82] Mass. Gen. Laws Ch. 93H.

[83] 201 C.M.R. 17.00.

[84] Nevada Revised Statutes 603A.210 and 597.970.

California law requires "reasonable security procedures and practices" for defined kinds of personal information.[85] In the *California Data Breach Report 2012-2015*, the California Attorney General noted the following about what constitutes reasonable security:[86]

> The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.

The *CIS Controls for Effective Cyber Defense Version 6.1*. (discussed in Section IV B below) is a set of consensus security standards.

The legal obligations don't stop, however, at protecting the confidentiality of information. Forty-eight states and the District of Columbia and the Virgin Islands have laws that require notification concerning data breaches (all but Alabama and South Dakota). While there are differences in their scope and requirements, they generally require entities that own, license or possess defined categories of personally identifiable information about individuals to notify affected individuals if there is a breach. Like the reasonable security laws, many of these laws apply to covered information "about" residents of the state. Some require notice to a state agency in addition to notice to consumers. Most of these laws have encryption safe harbors, which provide that notice is not required if the data is encrypted and the decryption key has not been compromised.

To add to the web of issues involved, at least 19 states also now have laws that require secure disposal of paper and electronic records that contain defined personal information. The Federal Trade Commission's Disposal Rule[87] has similar requirements for consumer credit reports and information derived from them.

At the federal level, an attorney who receives personally identifiable protected health information (PHI) from a covered entity under the Health Insurance Portability & Accountability Act (HIPAA) will generally be a "business associate" and be required to comply with the HIPAA security requirements. The 2009 Healthcare Information Technology and Clinical Health (HITECH) Act enhanced HIPAA security requirements, extended them directly to business associates, and added a new breach notification requirement. Encryption is included as an "addressable" requirement, which means that it or an alternative must be implemented or a written explanation provided to explain why it is not needed.[88] In addition, the Federal Trade Commission has brought over 60 enforcement actions against businesses based on allegations that they failed to take reasonable measures to safeguard the privacy and security of personal information about

---

[85] Ca. Civil Code § 1798.81.

[86] Available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

[87] 16 C.F.R. Part 682.

[88] See, 45 CFR Parts 160 and 164.

consumers. In over half of them, settlements required the businesses to employ additional safeguards, including encryption of personal information in transmission and storage.[89]

Summary of Duties

The ethics rules and common law duties require attorneys to take **competent and reasonable measures to safeguard client data**, including an understanding of limitations in attorneys' competence, obtaining qualified assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available security evolve. **These ethical and common law duties, as well as any applicable contractual and regulatory duties, are minimum standards of conduct. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service.** While the risks of disciplinary proceedings, malpractice claims, and regulatory actions arising from security breaches are real, the greatest risks are often dissatisfied clients (or former clients) and harm to professional reputation.

Information Security Basics

Information security is a process to protect the confidentiality, integrity, and availability of information. Comprehensive security must address people, policies and procedures, and technology. While technology is a critical component of effective security, the other aspects must also be addressed. As explained by Bruce Schneier, a highly-respected security professional, "[i]f you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[90] The best technical security is likely to fail without adequate attention to people and policies and procedures. Many attorneys incorrectly think that security is just for the Information Technology department or consultants. While IT has a critical role, everyone, including management, all attorneys, and all support personnel, must be involved for effective security.

The best technical security is likely to fail without adequate attention to people and policies and procedures.

An equally important concept is that security requires training and ongoing attention. It must go beyond a onetime "set it and forget it" approach. A critical component of a law firm security program is constant vigilance and security awareness by all users of technology. As a recent ABA report aptly put it:[91]

---

[89] Patricia Bailin, "Study: What FTC Enforcement Actions Teach Us about Features of Reasonable Privacy and Data Security Practices," *The Privacy Advisor* (Sept. 19, 2014) https://iapp.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices.

[90] Bruce Schneier, *Secrets and Lies - Digital Security in a Networked World* (John Wiley & Sons, Inc. 2000) at p. xii.

[91] Joshua Poje, "Security Snapshot: Threats and Opportunities," ABA TECHREPORT 2013 (ABA Legal Technology Resource Center 2013).

> Lawyers must commit to understanding the security threats that they face, they must educate themselves about the best practices to address those threats, and **they must be diligent in implementing those practices every single day**.
>
> (Emphasis added.)

Information security is best viewed as a part of the information governance process. Information governance manages documents and data from creation to final disposition – including security and privacy.[92]

At the ABA Annual Meeting in August, 2014, the ABA adopted a resolution on cybersecurity that is consistent with this general approach:[93]

> **RESOLVED,** That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.

This resolution recommends an appropriate cybersecurity program for all private and public sector organizations, which includes law firms.

The first step for a security program is assigning responsibility for security. This includes defining who is in charge of security and defining everyone's role, including management, attorneys and support personnel.

Security starts with an inventory of information assets to determine what needs to be protected and then a risk assessment to identify anticipated threats to the information assets. The next step is development, implementation, and maintenance of a comprehensive information security program to employ reasonable physical, administrative, and technical safeguards to protect against identified risks. This is generally the most difficult part of the process. It must address people, policies and procedures, and technology and include assignment of responsibility for security, policies and procedures, controls, training, ongoing security awareness, monitoring for compliance, and periodic review and updating.

An information security program should cover the core security functions: **identify, protect, detect, respond and recover.** While detection, response, and recovery have always been important parts of security, they have too often taken a back seat to protection. Since security incidents and data breaches are increasingly viewed as sometimes being inevitable, these other functions have taken on increased importance. Gartner, a leading technology consulting firm, has predicted that by 2020, 60% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2014.[94]

---

[92] See the Information Governance Reference Model, published by EDRM, an organization operated by Duke Law School that publishes resources for e-discovery and information governance. www.edrm.net/frameworks-and-standards/information-governance-reference-model.

[93] Available at www.americanbar.org/content/dam/aba/images/abanews/2014am_hodres/109.pdf.

[94] http://blogs.gartner.com/anton-chuvakin/2014/02/24/new-research-on-dealing-with-advanced-threats.

The requirement for lawyers is reasonable security, not absolute security. For example, New Jersey Ethics Opinion 701 states "'[r]easonable care,' however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible…" Recognizing this concept, the Ethics 20/20 amendments to the Comment to Model Rule 1.6 include "…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."

Security involves thorough analysis and often requires balancing and trade-offs to determine what risks and safeguards are reasonable under the circumstances. There is frequently a trade-off between security and usability. Strong security often makes technology very difficult to use, while easy to use technology is frequently insecure. The challenge is striking the correct balance among all of these often-competing factors.

The Ethics 20/20 amendments to Comment 18 to Rule 1.6 provide some high-level guidance. As discussed above, the following factors are applied for determining reasonable and competent safeguards:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

This is a risk-based approach that is now standard in information security.

Attorneys and law firms will often need assistance in developing, implementing, and maintaining information security programs because they do not have the requisite knowledge and experience. For those who need assistance, it is important to find an IT consultant with knowledge and experience in security or a qualified security consultant. Qualified consultants can provide valuable assistance in this process. An increasing number of law firms are using service providers for assistance with developing and implementing security programs, for third-party review of security, and for services like security scans and penetration testing to identify vulnerabilities. A growing trend is to outsource **part** of the security function by using a managed security service provider for functions such as remote administration of security devices like firewalls, remote updating of security software, and 24 X 7 X 365 remote monitoring of network security.

Law firms are increasingly obtaining cyber insurance to transfer some of the risks to confidentiality, integrity, and availability of data in their computers and information systems. This emerging form of insurance can cover gaps in more traditional forms of insurance, covering areas like restoration of data, incident response costs, and liability for data breaches. Because cyber insurance is an emerging area of coverage and policies differ, it is critical to understand what is and is not covered by policies. The ABA Center for Professional Responsibility has published

Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy that provides guidance in this area.[95]

Details of security measures and controls are covered in the following section and in the security standards, frameworks, and consensus controls discussed in it.

Reasonable Safeguards

The greatest challenge for lawyers in establishing cybersecurity programs is generally deciding what security measures are necessary and then implementing and maintaining them. Determining what constitute "competent and reasonable measures" can be difficult.

The ethics requirements are the floor—anything less is a violation of attorneys' professional responsibility obligations. Attorneys should aim for stronger safeguards to protect their clients and themselves. They must meet legal requirements for personally identifiable information and protected health information like HIPAA or the Massachusetts law, if they apply, and any requirements to which attorneys have agreed by contract. In determining what is reasonable, attorneys can look to guidance from bar groups, legal standards in other areas, government publications, and consensus security frameworks and standards.

The American Bar Association regularly publishes materials and provides educational programs on information security. Examples include the Law Practice Division[96] (with resources like books, webinars, the Legal Technology Resource Center (LTRC), ABA TECHSHOW, and articles in *Law Practice* magazine and *Law Practice Today* webzine), the Cybersecurity Legal Taskforce, the Standing Committee on Law and National Security, the Section of Science and Technology's Information Security Committee and the Business Law Section's Cyberspace Law Committee. The Legal Technology Resource Center publishes an annual *Legal Technology Survey Report* that reports on attorneys' use of technology, including security incidents, practices and technology.[97]

Many state bar associations provide similar materials and programs. This kind of information is particularly helpful to attorneys because it is tailored to the practice of law.

ILTA (the International Legal Technology Association),[98] a professional organization devoted to technology for law firms and law departments, regularly provides security education and materials and has peer groups that regularly exchange information. ILTA has established the LegalSEC initiative that has been working for several years to provide the legal community with tailored guidelines for risk-based information security programs. It conducts an annual LegalSEC Summit and provides additional educational programs and resources. LegalSEC also sponsors an

---

[95] Eileen R Garczynski, *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy* (American Bar Association 2016). See also, Eileen R Garczynski, "Protecting Firm Assets with Cyber Liability Insurance," *Business Law Today* (September 2016), www.americanbar.org/publications/blt/2016/09/05_garczynski.html.

[96] www.lawpractice.org.

[97] www.americanbar.org/groups/departments_offices/legal_technology_resources/publications.html.

[98] www.iltanet.org.

annual *Study of the Legal Industry Information Security Practices* that is published by Digital Defense, Inc., a security service provider.[99]

Threat intelligence and information sharing is a growing part of security. Receipt of real time information on current threats enables law firms and other enterprises to quickly implement protective measures and recovery efforts. There are many sources of this kind of information, like information security service providers (some limited to customers), US-CERT,[100] the SANS Internet Storm Center,[101] the FBI's InfraGard program,[102] and ILTA's LegalSEC initiative.[103] The Financial Services Information Sharing and Analysis Center (FS-ISAC) is one of the mature organizations in this area. The FS-ISAC has started the Legal Services Information Sharing & Analysis Organization (LS-ISAO) to facilitate threat intelligence and information sharing for the legal industry.[104]

Details of security measures and controls are covered in the following sections and in the security standards, frameworks, and consensus controls discussed in them.

B. Security Frameworks and Standards

There are numerous security frameworks, standards and guidance documents that can be used for implementing law firm information security programs. It is important to select and use one or more that fit the size of the firm and the sensitivity of the information to use as an overall approach. This can be a daunting task with the alphabet soup of available resources: NIST, ISO, FTC, SANS, US-CERT, ILTA and more.

The NIST Framework

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, has published the *NIST Framework for Improving Critical Infrastructure, Version 1.0* (February 12, 2014).[105] While the *Framework* is aimed at security of critical infrastructure, it is based on generally accepted security principles that can apply to all kinds of businesses and enterprises, including law firms. The core security Functions in the *Framework* are **"identify, protect, detect, respond and recover."** Under these core Functions, the Framework includes details through Categories, Subcategories, and Information Sources. These core Functions should shape any law firm's cybersecurity program. It includes cross-references to other security standards, including the ones discussed below, in Table 2 in Appendix A of the *Framework*.

[99] www.iltanet.org/viewdocument/2016-study-of-the-le?ssopc=1.

[100] www.us-cert.gov/ncas/alerts.

[101] https://isc.sans.edu.

[102] www.infragard.org.

[103] www.iltanet.org/resources/legalsec?ssopc=1.

[104] www.fsisac.com/ls-isao.

[105] www.nist.gov/itl/csd. The *Framework* is available at www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

The *Framework* follows the evolving approach to security, which recognizes the **increasing importance of detection, response and recovery**. For years, the major emphasis was on protection. While detection and incident response have long been necessary parts of comprehensive information security, they have too often taken a back seat to protection. Their increasing importance is now being recognized. Some technology attorneys and security professionals have expressed the view that the *Framework* will become a or the *de facto* standard for an overall approach to reasonable security in the United States.

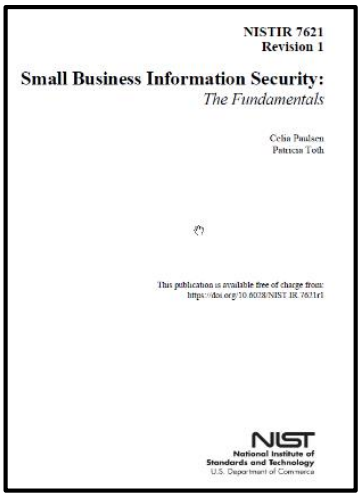
On January 10, 2017, NIST released for public comment Draft Version 1.1 of the Framework.[106]

ISO Standards

The ISO 27000 series of standards, published by the International Organization for Standardization (ISO), are consensus international standards for a comprehensive Information Security Management System (ISMS), including its elements, processes, and controls.[107] The systems are described in ISO/IEC 27000:2014 – *Overview and Vocabulary*. There are various standards in the series that provide additional details. Together, they provide the overall framework and details for establishing, implementing, monitoring, and continually improving an ISMS. The core standards include: ISO/IEC 27001:2013 - *Information Security Management Systems— Requirements*, ISO/IEC 27002:2013 - *Code of Practice for Information Security Management Controls,* and ISO/IEC 27005:2011 - *Information Security Risk Management*. There is a formal process under which an organization's ISMS can be formally certified under ISO/IEC 27001 by a qualified third-party. While a limited, but slowly growing, number of law firms report having or seeking formal certification under the ISO 27000 standards, a greater number report using these standards, or parts of them, as guides. ILTA's LegalSEC initiative has been focusing on aligning the legal community with the 27000 standards.

Other NIST Standards

In addition to the *Framework*, NIST has published numerous security standards and guidance documents and periodically updates them. While compliance with many of them is required for government agencies and government contractors, they can be used as guidance by other enterprises, including law firms. Many of them are very technical and more appropriate for government agencies and large companies (and large law firms), but some are basic and tailored for small and midsize businesses.


NISTIR 7621
Revision 1

Small Business Information Security:
The Fundamentals

Celia Paulsen
Patricia Toth

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) and standards referenced in it provide a comprehensive catalog of controls and a process for selection and implementation of them through a risk management process. While designed for federal agencies, the NIST process and various NIST standards can be used by law firms or businesses as guides. There is no formal

[106] www.nist.gov/cyberframework/draft-version-11.

[107] www.iso.org.

process for certification under NIST like there is under ISO 27001. Some law firms have reported that they are aligning their security programs with NIST standards.

There are NIST standards and guidance documents that are tailored to small and mid-size businesses. NIST's *Small Business Information Security: The Fundamentals, NISTR 7621, Revision 1* (November 2016) provides NIST's recommendations for small businesses to establish reasonably effective cybersecurity programs. It defines typical small businesses as ones with up to 500 employees, but recognizes that it may vary with the type of business.

US-CERT

US- CERT, a part of the U.S. Department of Homeland Security, has published a number of cybersecurity resources[108] for businesses, control systems, government agencies, and consumers, including ones for small and midsize businesses.[109] They include resources like a "Toolkit for Small and Midsize Businesses" and "Why Every Small Business Should Use the NIST Cybersecurity Framework."

Federal Trade Commission

The Federal Trade Commission's (FTC) Safeguards Rule under the Gramm-Leach-Bliley Act also provides a helpful framework for smaller firms, although it does not generally apply to lawyers as a legal requirement (unless they have agreed by contract to do so). The requirements in the rule, "Standards for Safeguarding Customer Information," 16 CFR, Part 314, are general and cover fewer than two pages in the Federal Register. They provide an overall approach, but not all the details. The FTC has also published "Protecting Personal Information: A Guide for Business" (October 2016) [110] and "Start with Security: A Guide for Business" (June 2015)[111] that contain the FTC's recommendations for safeguarding confidential personally identifiable information.

Consensus Security Controls

In addition to standards and frameworks for comprehensive security programs, there are consensus standards for sets of security controls that should be included in comprehensive programs, but do not define complete programs.

CIS Critical Controls

For example, the *SANS Top 20 Critical Security Controls,* first published in 2008, were developed as "an approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats." They were originally coordinated by the SANS Institute, a leading information research and education provider, and were agreed upon by a consortium including the National Security Agency, U.S.-CERT, the Department of Defense, Joint Task Force Global Network Operations (JTF-GNO) Command, the Department of Energy Nuclear Laboratories, the Department of State, the Department of Defense Cyber Crime Center, the

---

[108] www.us-cert.gov/security-publications.

[109] www.us-cert.gov/ccubedvp/getting-started-business.

[110] www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[111] www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

Federal Bureau of Investigation, leading commercial forensics consultants and pen testers, and others.

They are now managed by the Center for Internet Security and are now called the *CIS Controls for Effective Cyber Defense Version 6.1*.[112] They include 20 critical controls. They have evolved over time and it is important to consult the Center or SANS websites for the current version. The *Controls* do not define the requirements for a comprehensive information security program, but instead, are "a recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks." They remain current and relevant because "they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources." They "represent the most important cyber hygiene actions every organization should implement to protect their IT networks."

For law firms starting information security programs, the *Controls* can be used for setting priorities and making sure that the key controls are covered. They state that "Controls CSC 1 through CSC 5 are essential to success and are among the very first things to be done." They are necessary for a strong foundation for defense. They include:

CSC 1: Inventory of Authorized and Unauthorized Devices

CSC 2: Inventory of Authorized and Unauthorized Software

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 5: Controlled Use of Administrative Privileges

The first step in comprehensive security (CSC 1 and CSC 2) is identifying what needs to be protected.

CIS has recently published an *Implementation Guide for Small and Medium-sized Enterprises (SME) for CIS Controls* (September 2017).[113]

For those with established programs, the *Controls* can be used as part of the auditing and updating process.

The SANS Institute publishes a poster that demonstrates the Controls and details relating to them. It also includes a map that coordinates the controls with other security standards and requirements like NIST, ISO and HIPAA.[114]

Australian Signals Directorate

The Australian Signals Directorate, an intelligence agency in the Australian Government Department of Defence, publishes a set of *Strategies to Mitigate Targeted Cyber Intrusions*.[115]

---

[112] www.cisecurity.org/critical-controls.cfm.

[113] www.cisecurity.org/white-papers/cis-controls-sme-guide.

[114] www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf.

[115] www.asd.gov.au/infosec/mitigationstrategies.htm.

The current version (February 2017) lists 37 measures and provides details about them. The *Strategies* take an approach similar to the *Critical Security Controls.*

Significantly, the Signals Directorate reports that 4 of the measures, as a package, would have mitigated at least 85% of the incidents to which it responded. These *Top 4 Mitigation Strategies* are:

1. Application whitelisting,
2. Patching systems,
3. Restricting administrative privileges, and
4. Creating a defence in depth system.

Legal Cloud Computing Association

In March of 2016, the Legal Cloud Computing Association, an organization of cloud computing providers serving the legal profession, published the *LCCA Security Standards*.[116] Although it is a trade group publication rather than a consensus standard, it provides a helpful checklist of security measures that should be considered when using cloud services.

Association of Corporate Counsel

The Association of Corporate Counsel (ACC) *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential* Information (discussed in Section 2 E above) are likely to have increasing importance as consensus security controls for law firms.

Approaches for Attorneys and Law Firms

Attorneys and law firms should select and use one or more of the standards, frameworks, and sets of controls that fit the size of the firm and the sensitivity of the information. As noted above, the NIST *Framework* includes, in Table 2 in Appendix A, cross-references of its subcategories to other security standards and consensus controls, including the ISO 27000 series, NIST 800-53, the *Critical Security Controls*, and the *Strategies to Mitigate.*

Starting with the basics and then moving forward can have a prompt, strong impact on improving security - the *Verizon 2013 Data Breach Investigation Report* (covering 2012) reported that 78% of breaches were of low or very low difficulty for initial compromise.[117] This suggests that basic and intermediate safeguards may have prevented many of them. The effectiveness of implementing the first steps has been confirmed by the Center for Internet Security and the Australian Signals Directorate, as discussed above.

Inventory and Risk Assessment

The first step in developing and implementing an information security program is an inventory. It should include all information assets: data, software, hardware, appliances and infrastructure. You can't protect it if you don't know that you have it. Next is a risk assessment: a structured

---

[116] www.legalcloudcomputingassociation.org/standards.

[117] www.verizonenterprise.com/DBIR/2013.

process to identify, evaluate and prioritize threats to a law firm's information assets and operations and measures to mitigate the risks. The results are used to develop an information security program.

For the risk assessment function, it is best to use a framework or outline to make sure that everything is covered. The security standards and frameworks discussed above include risk assessment.

The *NIST Framework for Improving Critical Infrastructure* includes risk assessment as part of the Identify Core Function. ISO/IEC 27002:2013 includes basic risk assessment, with more complete details in ISO/IEC 27005:2011 - *Information Security Risk Management*. NIST Special Publication 800-53 also includes basic risk assessment, with more details in NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012).

A separate, formal risk assessment framework is CERT's OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation℠).[118] It is a good framework for large law firms and companies. OCTAVE-S is a version of OCTAVE that is tailored for smaller organizations with 100 or fewer people. For very small law firms, the OCTAVE-S framework can be scaled down. The latest version of OCTAVE is OCTAVE Allegro. It is a streamlined version that supplements, rather than replaces the other versions.

Many IT consultants and security professionals have their own risk assessment frameworks and checklists.

The identified risks have to be addressed in the information security program. There are four options for addressing each risk or area of risk.

1. Apply security policies and controls to manage the risk.
2. Transfer the risk (e.g., through a cyber insurance policy or contract).
3. Eliminate the risk (by stopping the activity or doing it in a different way).
4. Accept the risk.

A distinction is frequently made between risk assessment and risk management. *Risk assessment* or *risk analysis* is used to describe a single step in the security process (often repeated periodically) in which risks are identified, the likelihood of occurrence and impact are analyzed, and mitigation measures are evaluated. *Risk management* is a broader, ongoing process in which risks and mitigation measures are continuously reviewed, evaluated, and addressed. Risk assessment is the evaluation phase; risk management includes evaluation, as well as implementation, maintenance, review, and updating.

As discussed above, cyber insurance is increasingly being by attorneys and law firms as part of the risk management process.

---

[118] www.cert.org/resilience/products-services/octave.

Laptops and Portable Devices

"Considering the high frequency of lost assets, encryption is as close to a no-brainer solution as it gets for this incident pattern."

Protection of laptops, smartphones, tablets, and other mobile devices presents a good example of application of the requirement of "reasonable efforts" to a specific category of technology. Mobile devices present a great security risk because they can be easily lost or stolen. The *Verizon 2014 Data Breach Investigation Report* (covering 2013) explains the risk and a solution to it – encryption – this way:[119]

> ***PHYSICAL THEFT AND LOSS***
> ***RECOMMENDED CONTROLS***
>
> *The primary root cause of incidents in this pattern is carelessness of one degree or another. Accidents happen. People lose stuff. People steal stuff. And that's never going to change. But there are a few things you can do to mitigate that risk.*
>
> *Encrypt devices*
>
> *Considering the high frequency of lost assets,* ***encryption is as close to a no-brainer solution as it gets for this incident pattern****. Sure, the asset is still missing, but at least it will save a lot of worry, embarrassment, and potential lawsuits by simply being able to say the information within it was protected.*
>
> (Emphasis added.)

While each attorney and law firm should determine what is reasonable in their circumstances, this raises the question, does failure to use encryption for mobile devices - a no-brainer solution – comply with the duty to employ reasonable safeguards?

Security Checklists

Based on these information security basics, standards, frameworks, and controls, attorneys and law firms should **develop, implement and maintain a comprehensive information security program**, including:

- **Assignment of responsibility for security,**
- **An inventory of information assets and data,**
- **A risk assessment,**
- **Appropriate administrative, technical and physical safeguards,**
- **Training,**
- **An incident response plan,**

[119] www.verizonenterprise.com/DBIR/2014.

1. **A backup and disaster recovery plan,**
2. **Management of third-party security risks, and**
3. **Periodic review and updating.**

The following measures should be included in a comprehensive security program:

- ☐ Use secure, common configurations for servers, desktops, laptops, and mobile devices.
- ☐ Control use of administrative privileges.
- ☐ Use strong passwords or passphrases.
- ☐ Use multifactor authentication, particularly for administrator accounts and remote access.
- ☐ Segment and limit access to sensitive data.
- ☐ Promptly patch the operating system, all applications, and all plug-ins.
- ☐ Use strong encryption.
- ☐ Use only secure wireless networks.
- ☐ Use strong security appliances and software and keep them up to date.
- ☐ Conduct vulnerability assessment and remediation.
- ☐ Back up important files and data.
- ☐ Address third party security risks.
- ☐ Provide for secure disposal of electronic data and paper.
- ☐ Address security for new, current, and departing employees.

Conclusion

Attorneys have ethical and common law obligations to take competent and reasonable measures to safeguard information relating to clients and often have contractual and regulatory requirements. Compliance with these duties requires developing, implementing, and maintaining a comprehensive information security program. Important considerations for attorneys include understanding limitations in their knowledge and experience, obtaining appropriate, qualified assistance, continuing security training, and ongoing review and updating as technology, threats, and available security evolve over time. Particularly important is constant security awareness by all users of technology – every day, every time they're using technology.

Additional Information

American Bar Association, Business Law Section, Cyberspace Law Committee, http://apps.americanbar.org/dch/committee.cfm?com=CL320000

American Bar Association, Cybersecurity Resources, www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/resources.html, provides links to cybersecurity materials and publications by various ABA sections, divisions and committees

American Bar Association, Cybersecurity Legal Task Force www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html

American Bar Association, Law Practice Division, www.lawpractice.org, including the Legal Technology Resource Center www.americanbar.org/groups/departments_offices/legal_technology_resources.html

American Bar Association, *A Playbook for Cyber Events, Second Edition* (American Bar Association 2014)

American Bar Association, Section of Science and Technology Law, Information Security Committee http://apps.americanbar.org/dch/committee.cfm?com=ST230002

John T. Bandler, *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security* (American Bar Association 2017)

Center for Internet Security, a leading security organization that publishes consensus-based best security practices like the *CIS Critical Security Controls* and *Secure Configuration Benchmarks*, www.cisecurity.org

Daniel Garrie and Bill Spernow, *Law Firm Cybersecurity* (American Bar Association 2017)

Federal Trade Commission, Data Security Resources for Business, www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

ILTA (International Legal Technology Association) LegalSEC, , provides the legal community with guidelines for risk-based information security programs, including publications, the LegalSEC security initiative, peer group discussions, webinars, an annual LegalSEC Summit conference and other live programs; some materials are publicly available while others are available only to members, http://connect.iltanet.org/resources/legalsec?ssopc=1

National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications, numerous standards and publications, including the *Framework for Improving Critical Infrastructure Cybersecurity* (February 2014), www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

SANS Institute, www.sans.org, a leading information research, education, and certification provider, includes resources like the *SANS Reading Room*, the *Critical Security Controls*, *Securing the Human*, and OUCH! (a monthly security newsletter for end users)

Sharon D. Nelson, David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015)

Sharon D. Nelson, David G. Ries and John W. Simek, *Locked Down: Practical Information Security for Lawyers, Second Edition* (American Bar Association 2016)

Jill D. Rhodes and Robert S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition* (American Bar Association 2017)

The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers* (November 2015)

Thomas J. Shaw, Editor, *Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists* (American Bar Association 2011)

US-CERT, part of the U.S. Department of Homeland Security, www.us-cert.gov, includes resources for implementing the NIST Framework (businesses www.us-cert.gov/ccubedvp/getting-started-business) and (small and midsize businesses www.us-cert.gov/ccubedvp/getting-started-smb)

David G. Ries is Of Counsel in the Pittsburgh, PA office of Clark Hill PLC, where he practices in the areas of environmental, technology, and data protection law and litigation. For over 20 years, he has increasingly focused on cybersecurity, privacy, and information governance. He has used computers in his practice since the early 1980s and since then has strongly encouraged attorneys to embrace technology - in appropriate and secure ways. He is a co-author of *Locked Down: Practical Information Security for Lawyers, Second Edition* (American Bar Association 2016) and *Encryption Made Simple for Lawyers* (American Bar Association 2015) and a contributing author *to Information Security and Privacy: A Legal, Business and Technical Handbook, Second Edition* (American Bar Association 2011).

Cyberinsurance: Necessary, Expensive and Confusing as Hell

by Sharon D. Nelson, Esq. and John W. Simek
© 2018 Sensei Enterprises, Inc.

Setting the stage

The title of this article was also the tile of a session presented at ABA TECHSHOW this year. And each part of the title is true. It is absolutely necessary to have cyberinsurance in order to manage your risk. No amount of technology, policies or training can guarantee that you will not be breached. Expensive? Oh yes. Get ready for sticker shock when you purchase cyberinsurance. Because we teach CLEs on cyberinsurance, we can tell you with some assurance that lawyers are very confused about what specific insurance they need. Insurance companies are not very helpful– the various policies offered across the industry are not at all standardized – and of course they are written in complicated language which often obfuscates their meaning.

Where are we today?

Not in a great place. According to a 2017 survey by the data analytics firm FICO, half of U.S. business have no cyberinsurance, 27% have no plans to buy coverage and only 16% report having a policy that covers all cyber risks. There is a certain justified cynicism about cyberinsurance. The news is rife with companies who had cyberinsurance, but found – after being breached – that a substantial portion of their damages were not covered.

A 2017 report by Deloitte called "Demystifying Cyber Insurance Coverage" called the market "promising" but "problematic" for the insurance companies as well as customers. We don't have a lot of data going back in time to help us construct reliable predictive models. With threats evolving daily and many different kinds of damages possibly occurring, perhaps over a broad swath of insurance company customers, insurers are "flying blind" – something you can see for yourself when you look at widely varying prices for widely varying coverage. As a result, many insurers are focused on PII (personally identifiable information) coverage which may or may not be the primary need of an organization. Chubb Group, a well-known and early entrant into the cybersecurity market, paid some of the losses for P.F. Chang's point-of-sale data breach but it did not cover the required $1.9 million Payment Card Industry Data Security Standard assessment. If you don't even know what that means (and many lawyer do not), take a deep breath and do a search on PCI-DSS fines . . .

And after all this time, many law firms and other entities mistakenly believe that their general liability or business interruption policies fully cover data breaches. Some of them have learned the hard way how very wrong they were.

Given the fact that law firms are generally not models of strong cybersecurity practices, it would be prudent of law firms to up their game, especially since both clients – and potential insurers – are asking hard questions about firms' security. In 2017, legal technology firm LogicForce gave the legal industry only a 42% rating on its cybersecurity health. The score was based on twelve factors, weighted differently, including information on information security executives, polices, multifactor authentication, cyber training (we have seen a big uptick there), cyberinsurance, penetration testing, vulnerability testing, third-party risk assessments, information governance, cyber investment, full disk encryption, and data loss prevention technology and software.

Apples to apples comparisons?
Fuggedaboutit. The best you can probably do is to consult a trusted insurance advisor who is accustomed to dealing with cybersecurity policies. Once you get over the aforementioned sticker shock for the costs of the policy and absorb the grim reality of the high deductibles, you've got to get into the nitty gritty of a subject that is very hard to understand if you are not in the insurance business with a keen understanding of cybersecurity.

In many cases when lawyers ask where to get impartial advice, we are apt to recommend that lawyers ask their colleagues for references – not so much here because, unless your colleagues have suffered damages from a cyber attack or breach, they really don't know how good their policies are.

Most lawyers have professional liability insurance, which will undoubtedly get you some cyberinsurance coverage since you are holding data because you are rendering legal services. However, more than 50% of the cost of a data breach may come from digital forensics and the data breach lawyer you hire – which are not covered by the LPL (Lawyers' Professional Liability) policy. Other costs which are likely not covered include public relations coverage, data breach law compliance/notification costs, regulatory investigations costs, including subsequent fines and penalties.

What will cyber insurers likely need to know before giving you a quote?
Clearly, the information sought will vary from insurer to insurer, but here is a likely list of questions they might ask and things they will require:

1. Have you had an independent 3rd party cybersecurity audit? And yep, they'll want the results and an accounting of any remediation that was performed.
2. Do you have e-mail encryption available for use? Is it used?
3. Do you employ full disk encryption?
4. A description of how your backup is engineered – to make sure, if you contract ransomware, that you have a reliable backup that you can restore your data from.
5. Do you train your employees in cybersecurity and how often you train?
6. Your security-related polices.
7. What kind of enterprise level security software and hardware are deployed, including firewalls, data loss prevention, incident detection software, etc.?
8. Have you ever experienced a data breach or other major cybersecurity incident? Yes, they will want details, including how long it took to discover any breaches.
9. A description of the physical security of your premises.
10. Do you comply with any national/international cybersecurity standards?
11. Have you ever made an insurance claim involving cybersecurity? Details will be required.
12. Has any other insurer canceled your cybersecurity policy or refused to renew one?
13. Mobile device security in place, which can cover a lot, but they will certainly want to know if you can remotely wipe lost or stolen devices.
14. Details of vendor management for those who have any degree of network access or who hold your data by design – are audits of those vendors required?
15. When employees are processed out of your firm, what measures are taken to secure your data?

16. Do you do background checks on new employees? Are they trained in security policies?
17. Awareness of facts which might give rise to a possible claim at the time the application is filled out.
18. The amount of your annual cybersecurity budget (particularly true for larger firms).
19. Are you following general best practices regarding passwords, access control, patching and upgrading outdated software which is not receiving security patches?
20. A description of the kind of data you hold (health data, credit card data, banking records – any sort of protected data).
21. Financial data about your firm, including assets, revenues, number of employees and any proposed merger or acquisitions.
22. Is logging enabled? What is the retention period of log files?

The list of possible insurer questions can seem daunting, especially if you become aware that your truthful answers (and failure to be truthful may invalidate coverage) will not please the prospective insurer.

What should you be asking a prospective insurance company?
This can be a hard question, but we have found it useful to set forth specific scenarios with specific damages and ask the insurance agent to show us what language covers what damages. For instance, virtually all insurance policies cover actual loss or damage to your computers, but not the loss of the data. Can you sometimes negotiate the coverage itself? Absolutely. Of course, that may come with a price tag. Taken together, the premium, the deductible and the coverage should give you a fairly clear idea of how well you are managing the risks you cannot wholly protect against – and the price for doing so. And if you don't like one proposal, well, there are now more than 60 carriers offering cyberinsurance, so you certainly have alternatives.

If your data is in the cloud or otherwise held by third parties, you are certainly going to need third party coverage. If your firm is active with social media coverage, you may need media liability coverage. And when regulatory fines loom, and they often do these days, you certainly want coverage for regulatory fines.

Ask your insurer as many questions as you can think of, but here are a few starters.

1. Is the coverage retroactive? How far back, if so?
2. Does the insurer believe your limits of coverage are adequate for your needs, especially given the nature of the data you hold and the size of your firm?
3. Does the policy cover both the loss and the compromise of data (e.g., make sure data encrypted by ransomware is covered)
4. Is there a discount if you have a 3rd party independent audit and remediate any critical vulnerabilities found by the audit?
5. Are you covered if a vendor holding your data suffers a breach?
6. For an additional premium, does the insurer offer a subrogation waiver? We know some of you are asking "What's this?" Google it for the full explanation and why such a waiver may be desirable. Where is cyberinsurance going?

Final Thoughts

Fitch Ratings said the industry grew by 35% in 2016. Allied Market Research predicted that the global market may reach $14 billion (now that's a big number) by 2022. But if you want a queasy stomach as you fork over huge premiums, consider this quote from Tim Francis, a vice president and enterprises lead for cyberinsurance at Travelers: "There's so much new coverage out there that hasn't been tested . . . One day there will be certain claims and we'll figure if the words we used to convey coverage actually say what we thought they meant, which is often up to a lot of lawyers." Not very reassuring, is it? The world of cyberinsurance is evolving – think how little we have by way of precedents. Combine that with the rapid changes in attack surfaces, cyber weapons and tactics, etc. and it is a bit unsettling. As we have now reached the point where many firms have been breached – and will be breached again - the one thing we can tell you for sure is that cyberinsurance is essential risk management for law firms.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

The Basics of Backup

by Sharon D. Nelson, Esq. and John W. Simek
© 2018 Sensei Enterprises, Inc.

Protecting Your Practice

Is backup a particularly sexy topic? No, but it sure generates a lot of questions when we lecture. And lawyers have begun to comprehend the significance of backing up wisely – especially after the data catastrophes caused by the natural disasters of 2017. Lawyers are increasingly keen to learn how to backup their data well.

Moreover, lawyers are ethically compelled to protect the confidential data entrusted to them by their clients. That means much more than securing their networks from external attacks and other cybersecurity incidents. Ransomware infections could cripple law practices by encrypting data and rendering it inaccessible. Every lawyer needs to be prepared to recover from a security incident, including those caused by Mother Nature.

Backup

Backup is an essential operation for every law firm – and yet, often poorly understood. Having an adequate backup is implicit in the ABA Model Rules for Professional Conduct and their state counterparts, as any legal ethicist will tell you. One of the lawyer's duties is to competently represent clients. How can you do that if your case files and communications are lost? You could have a hardware failure of your server or a disk crash. What if your cloud provider shut its doors, rendering client data inaccessible? Perhaps your laptop is stolen from your vehicle with client data for a pending matter. There are all kinds of situations where you could lose data or not be able to access it. That is where your backup comes into play. Should you have a catastrophe, you would restore data from your backup and be back in business.

A local backup is also a necessity if you use cloud services and your Internet connection goes down. You could certainly take your laptop to a public open Wi-Fi and get to your data that way, but having a local backup of your data is a good idea too. It gives you a safety net should something catastrophic happen to your cloud provider.

These days, the threat of ransomware is foremost in many attorneys' minds, no doubt because more than half of business surveyed have suffered a ransomware attack. For those that have been living under a rock, ransomware is basically malware that encrypts your data with an encryption key that you **do not** have. You must pay the ransom in order to get the decryption key and hence access to your data. The sad reality is that even though you pay the ransom, you may not get the decryption key. The latest statistics are that you will get a valid decryption key in less than 50% of the cases after paying the ransom. The scary part is that we are beginning to see some forms of ransomware that do not encrypt data, but rather destroy it! There is no option to decrypt the data since it no longer exists. Most lawyers have not heard about this terrifying form of attack but once again, backups may be your salvation.

In order to recover from a ransomware attack, backup is your friend. If you are unlucky enough to contract ransomware, just restore your data back from your backups. Of course this implies that you have good backups and have done test restores to make sure you could actually recover from an attack or failure. Test restores are crucial to verify that the data is restorable and not corrupted. All too often

we hear of law firms that have no backup or the backup is corrupted. One solo practitioner, who used a cloud backup, lost five years of law firm data – he had never done a test restore so he never knew that there was anything wrong with the backup. In such cases, you might sue the service provider – but that doesn't get your data back!

External USB Drives

Many solo and small firm attorneys use external USB drives for their backup. That is a perfectly good solution, but disconnect the drive once the backup is completed. Also, you should have at least two backup drives in case one of them is connected at the same time your computer experiences a ransomware infection. We have dubbed this advice "virgin backup" – you must have a backup which is not connected to your network – therein lies your peace of mind.

Hopefully your computer is equipped with a USB 3.0 port, which will allow for faster backups due to the faster transfer speeds versus a USB 2.0 connection. That means you should be only looking at purchasing an external USB 3.0 hard drive. You may want to consider getting a USB drive with built-in hardware encryption. Hardware encryption will ensure that the data is protected when the device is disconnected and powered off. Some external USB drives also come with backup software for no additional charge.

Tape

At this time, we consider tape backup systems to be obsolete. We have come across some law firms that still use tape, but we wish they would convert to a more economical and dependable hard disk type of system. Tape capacity can't come close to the amount of data you can fit on a hard disk. The data transfer rate to tape is also very slow when compared to disk transfers (even with USB). Tape is fragile as well and doesn't have a long life.

Since backing up to tape is not very reliable, it is a best practice to verify the backup after it completes. Verification further increases the amount of time to backup data. Hopefully we've made the case to abandon tape as backup medium and convert to an alternative method.

Backup Appliance

Another solution is to use a backup appliance that is agent-based. This means that you install a software agent on the computer to be backed up and data is transferred over the network to the appliance by using the agent. Think of it as communication software. The agent gathers the data to be backed up and transfers it to the appliance. This communication connection is not seen as a drive letter or a network share, which makes it impervious to ransomware attacks.

Typically, the backup appliance solution is used to backup local servers. The software is configured to periodically take snapshots of the server and stores the backup data on the appliance. In addition, consider sending an encrypted version of the backup data to the cloud, another best practice. Some appliances have the ability to virtualize the server should the actual server suffer a hardware or software failure. As an example, the backup appliances that we implement can take snapshots every 15 minutes and virtualize a server within a few hours. This has been a lifesaver for some of the law firms we work with.

Since the appliance is essentially a server customized for backup, expect to pay up to a few thousand dollars for the initial investment. A lot of the backup appliance providers provide the agents on a

monthly subscription basis. The cost may be per agent or based on the amount of data (size of server) that is being backed up. Off-site storage may also be included in the cost or priced on a per terabyte basis. Expect to pay on average somewhere around $100 a month per server being backed up. It could be as low as $50/month or up to $200/month depending on how the provider bases its charge (per device or by size volume). Off-site storage should run around $150-$200 per terabyte per month.

Cloud Backup

Using a cloud-based backup solution will also allow you to restore data following a ransomware attack. Just like the external USB drives, make sure you have at least two backup sets in the cloud.

There are many good backup solutions using the cloud. If possible, you should look to a cloud provider that allows you to control the encryption key used to encrypt the data. Carbonite is a good backup cloud provider that has that capability. A best practice would be to have multiple versions of the backup data in the cloud. That way if one gets corrupted or suffers a ransomware infection, you'll have alternate backup sets to restore from. Another highly reviewed backup provider is Backblaze.

Target Data

Selecting the appropriate technology is just one piece of the backup puzzle. The first thing you need to do is determine what you will back up. If you are looking for a disaster recovery option (total loss of equipment or service), you'll need a method that will allow you to recover quickly and preserve not just the data, but possibly applications as well. You'll probably end up with some sort of backup appliance if disaster recovery is your goal.

Risk Assessment

Once you have determined what needs to be protected, the next analysis is to determine the likelihood of data loss or inaccessibility. How likely is there to be a hardware failure? Perhaps your risk is fairly low if you have new hardware. However, failures can occur beyond hardware issues. Data could become corrupted. Someone could inadvertently delete a file. You could overwrite a file with the wrong version thereby destroying the original contents and of course, ransomware could render data inaccessible.

No matter what the scenario, you should perform a risk assessment and determine action steps to mitigate that risk.

Data Location

Another consideration is data location. Where is your important data being held? Many lawyers still have on premise equipment and keep their data on local storage devices. They just don't trust losing control of the data by putting it in the hands of a third party. Others are using cloud services and confidential client data is out of the lawyer's direct control. Different methods are needed if you have direct access to the data or it resides on some external service.

No matter where the data resides, the challenge is to find it all. You would be surprised at all the places law firm data ends up. Employees take data home. It exists on flash drives. It may be sent as attachments to a personal web-based e-mail account. Spend a little time to inventory all or the data sources. You can't back it up if you don't know you have it. "Dark data" – data a law firm doesn't know it has – has grown by leaps and bounds in recent years. It presents all kinds of risks – you can't protect that data, you can't back it up and if you don't know you have it, you may fail to disclose it when required to do so by laws and regulations or in litigation.

What about personal devices such as smartphones? You'll have to decide if the information on a personal device is at risk of being lost and should be backed up. This may be a good time to rethink your BYOD (Bring Your Own Device) policy and what devices can access firm data. If you do decide that smartphone information needs to be backed up, there are software solutions to accomplish this. Should you leave the process up to each individual or should you invest in a MDM (Mobile Device Management) system?

How Much?

Finally, how much data do you need to back up? That can radically impact your backup strategy. Hard drive space is fairly cheap these days, but you can't defy the laws of physics. Transfer times are only so fast. You can't make the electrons move any faster. Network speeds will limit the amount of data transfer as well. Perhaps now is a good time to upgrade your network cabling and hardware. If you are only backing up to the cloud, hard drive space is not an issue. However, you will need to know the data volume in order to determine how much the off-site storage is going to cost.

Last words

We worry about backup for lots of reasons. The natural disasters of 2017 were a great reminder of the need for having backups, as many lawyers painfully discovered.

Beyond that, ransomware has been on a wild roller-coaster ride, causing havoc everywhere, including in law firms. Ransomware really is a global epidemic today. The "bad guys" are constantly updating code and discovering new vulnerabilities to exploit. We hope you never have to experience a ransomware event or a system failure. But if you do, make sure you have properly engineered your backup so you can get back in business with minimal effort and pain. Engineering a good backup system is one of the smartest things any law firm can do to protect its confidential data.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Are You Ready for a Ransomware Attack?

by Sharon D. Nelson, Esq. and John W. Simek
© 2018 Sensei Enterprises, Inc.

Ransomware is growing by leaps and bounds. There are reports that ransomware attacks have increased by 748% over the last year. A major international study found that almost forty percent of businesses were hit by ransomware last year. Those are some staggering numbers. Law firms are not immune to ransomware attacks either. Any business is at risk, including the solo attorney. What can we do about ransomware attacks?

In order to understand how to deal with a ransomware attack, we need to understand what ransomware is, how it is contracted, and what impact there may be on your law practice.

What is ransomware?
Let's start with a quick lesson. Basically, ransomware is malware that encrypts your data with a key that you don't have. You can't access the data since it's encrypted and won't be usable until it is decrypted. Effectively, your data is held hostage until you pay the ransom to get the decryption key from the criminals that distributed the ransomware. Normally, there is a countdown timer indicating how long you have to pay the ransom. After the timer expires, the ransom may increase (doubling is not uncommon) or the ability to obtain a decryption key expires forever. There is big money in ransomware. Cybercriminals pocketed more than $1 billion in 2016 alone.

The ransom is requested to be paid in cryptocurrency. Bitcoin is the most requested method of payment. Currently, the average payment is from $650 to $2000. A couple of years ago, you could get by with a $300 payment, but not anymore. At a CLE we were presenting in rural Virginia, a solo attorney told us that he paid $2500 to get the decryption key. Don't worry if you don't know anything about cryptocurrencies. The writers of the ransomware code have very good help files to assist you in creating an electronic wallet and telling you where to go to convert your actual money into bitcoin or whatever other type of virtual currency is acceptable. You probably don't want to pay the ransom these days as you'll only get the decryption key about 50 percent of the time. So much for honor among thieves . . .

You don't even have to be a proficient programmer to take part in the ransomware movement. Some criminal groups are offering ransomware-as-a-service. Instead of charging a fee for the code, they take a portion of the ransoms paid. Typically, they ask for fifty percent of the collected fees.

How do you contract ransomware?
Generally, ransomware is contracted via a malicious attachment or link delivered in a phishing e-mail. It is just amazing how many people will open an attachment from an unknown sender. Some ransomware requires that a second step be taken in order to launch the attack.

One example would be the Locky ransomware. A common way for Locky to be delivered is as a Word document attachment. Once you open the document, the text is unreadable except for a message instructing you to enable macros "if the data encoding is incorrect." Seriously? You shouldn't have opened the attachment to begin with and you certainly shouldn't enable macros, which would launch Locky and start the encryption of your data.

Several ransomware campaigns have been very successful over the years. Locky and Cryptowall have found success for a long time. Their success is due to the regular updates to the code that allow avoidance of detection. Locky has even been updated to support 30 different languages meaning it can target specific countries and the ransom demand will be understood.

Ransomware has morphed

As previously mentioned, ransomware is normally invoked by opening a malicious attachment or link. That thinking changed in May of 2017 when the WannaCry ransomware attack spread like wildfire across the globe. WannaCry "was easily the worst ransomware attack in history," says Avast's Penn. "On May 12th, the ransomware started taking hold in Europe. Just four days later, Avast had detected more than 250,000 detections in 116 countries."

The really scary part about WannaCry is that it is the first ransomware attack that spreads across devices on the network WITHOUT any user interaction. No clicking. No opening of attachments. To be technically correct, WannaCry is classified as a worm because of the self-propagation. WannaCry exploited a vulnerability in Microsoft's implementation of the SMB (Server Message Block) protocol. Microsoft had already issued a patch for the vulnerability, but many people hadn't installed it yet. Lesson one…patch your software as soon as possible.

Another reason WannaCry spread so quickly is that many companies were allowing port 445 (the port used by the SMB protocol) through their firewalls, thereby exposing themselves to the Internet. Lesson two…don't configure your firewall to allow traffic that isn't needed.

According to Kaspersky Lab's APT Trends report for Q2 2017, the next big threat facing the enterprise is destructive malware **disguised** as a simple ransomware attack. That threat is already here. We first saw it with the WannaCry attack and then again in June with the NotPetya (also known as ExPetr) attack. It is alleged that both attacks were nation-state backed. Even though the attacks were originally thought to be typical ransomware campaigns looking for money, further research determined that the real goal was to destroy data. Specifically for NotPetya, analysis of the encryption routine would not allow decryption of the victim's data even if payment was made for the key.

Business impact

To bring things closer to home for the legal profession, it is believed that a NotPetya attack is what brought DLA Piper to its knees and virtually shut down the law firm for days. Some of the shutdown was done as a precaution, but DLA Piper's e-mail was "offline" for several days. As most of us know, e-mail communications is critical to a law firm.

Further, cybersecurity company Malwarebytes found that as many as one third of small to medium businesses were hit with ransomware last year. In addition, one in five had to shut down operations immediately. Not a very pleasant experience if you are the unlucky one to get hit.

Prevention

Obviously, the best thing is not to be the recipient of a ransomware attack at all. We believe that is the ostrich in the sand approach. Employees are human beings and somebody is going to do something they shouldn't do at some point. Ransomware is constantly evolving and taking advantage of vulnerabilities we don't even know exist. Our belief is that we need to be prepared for the inevitable attack and position ourselves in the best way to recover.

One of the first steps would be training. Since a very large portion of the ransomware attacks happen as a result of a phishing e-mail, training employees to recognize those e-mails is a good thing. Some are fairly obvious with misspelled words and poor grammar, but don't count on that to be the only sign. We've seen some very good phishing e-mails that have no errors and appear to come from someone we know. There are several free services that can test employees with phishing e-mails. Take a look at the free phishing services available at OpenDNS, Duo Security or SonicWall.

As previously mentioned, another step is to install all updates and patches as soon as possible. Of course your computer operating systems and software should be updated, but don't forget about the network components as well. Router and firewall manufacturers also distribute updates for their products. Make sure you install them too.

You should also have some sort of security suite installed. The modern day security suites include features such as anti-virus, anti-malware, firewall, anti-phishing, etc. There are other technologies you can utilize to reduce your chance of a ransomware attack. One very simple step is to practice the concept of least privilege mode. Users should have the least amount of permissions required for them to do their job. Unfortunately, we see far too many firms configuring user IDs with administrator access. Avoid this temptation and only logon as an administrator when absolutely necessary. You should also consider restricting user IDs to prevent installation of applications. We guarantee that move will not be very popular, but it will significantly reduce your chance of any ransomware attack being successful.

Recovery

No matter how much training you do or how much technology you implement, there is no solution which will stop a ransomware attack 100% of the time. That means we must operate on the assumption that some data will get encrypted or be destroyed at some point. It's not a question of preventing the attack, but being able to recover from it. You could always pay the ransom (assuming you have requisite bitcoins available within the time period), but that does not ensure you'll even get the decryption key. Paying the ransom also encourages the cybercriminals to continue ransomware attacks.

However, some companies may elect to pay the ransom - as did the Hollywood Presbyterian Medical Center in Los Angeles following systems getting infected with the Locky ransomware. Allen Stefanek, CEO of the hospital said, "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key."

Backups are your friend. Having a backup of your data unconnected from the network allows you to recover from a ransomware attack. If your data does get encrypted, you can just restore from your backup. However, the important part is to make sure your backup solution is engineered properly. We'll run through a few of the choices here.

Many solo and small firm attorneys use external USB drives for their backup. That is a perfectly good solution, but disconnect the drive once the backup is completed. Also, you should have at least two backup drives in case one of them is connected at the same time your computer experiences a ransomware infection. Using a cloud-based backup solution will also allow you to restore data following a ransomware attack. Just like the external USB drives, make sure you have at least two backup sets in the cloud.

Another solution is to use a backup appliance that is agent-based. This means that you install a software agent on the computer to be backed up and data is transferred over the network to the appliance by using the agent. Typically, the backup appliance solution is used to backup local servers. The software is configured to periodically take snapshots of the server and stores the backup data on the appliance. In addition, consider sending an encrypted version of the backup data to the cloud. Some appliances have the ability to virtualize the server should the actual server suffer a hardware or software failure. As an example, the backup appliances that we implement can take snapshots every 15 minutes and virtualize a server within a few hours.

Last words

Ransomware really is an epidemic today. The “bad guys” are constantly updating code and discovering new vulnerabilities to exploit. We hope you never have to experience a ransomware event. But if you do, make sure you have properly engineered your backup so you can get back in business with minimal effort and pain.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Practical Cybersecurity for Law Firms: How to Batten Down the Hatches

By Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke
© 2017 Sensei Enterprises

Setting the stage

We're quickly approaching 2018 and a week doesn't go by without another variant of malware causing havoc across the globe. First it was the WannaCry ransomware worm, which infected more than 230,000 computer systems in over 150 countries demanding ransom payments in exchange for the decryption of files. More recently, a new variant using code from the Petya ransomware (named "notpetya") struck first in Ukraine followed by other European countries and disabled critical utility services such as the radiation monitoring system at the Chernobyl Nuclear Power Plant, as well the affecting the countries' banks and metro systems.

What caught the attention of lawyers was that an apparent infection in one of DLA Piper's European offices brought the law firm's normal operations to a halt. As we write, the extent of the damage is still unclear.

The times have changed since Cryptolocker first ran wild in 2013, but the results are still as devastating. The costs of ransoms have significantly gone up from a few hundred dollars to the $1,000+ plus range now for the decryption key to unlock the affected files – and more than half of those who pay up do not receive the decryption key. So much for honor among thieves!

Ransomware has continued to evolve and is the primary security concern for businesses of all types and sizes.

How do you protect your firm from ransomware, malware and other cyber threats? Before we get started, as we say all the time (and it rates all caps), **THERE IS NO SILVER BULLET THAT PROTECTS AGAINST ALL RANSOMWARE.** Or all malware for that matter. If a vendor promises you a 100% solution, you are being sold a bill of goods.

Backups

Backups are key. Backup all of your data. Don't forget to periodically conduct a test restore of the data and make sure your backups are impervious to ransomware – either backed up in the cloud or agent-based (talk to your IT provider to learn more) Backups should be encrypted with a user-defined encryption key, whether on-site, off-site or stored in the cloud. If using a cloud vendor, the vendor should not have access to the decryption key. Encryption should be treated as a must – no questions about it.

The simple solution for most solo/small firm lawyers? Use an external USB hard disk. Unplug the external USB hard disk after the backup job completes. Just make sure you have at least two USB hard disks and rotate them in case you are attacked while one disk is connected.

Passwords

Next up, passwords. Develop a password policy. The recommendations for password policies have recently changed. We still live in a password driven world, but the final guidelines from the National

Institute of Standards and Technology (NIST) for the federal government have now been published – see SP 800-63-3: Digital Identity Guidelines which you may find at https://pages.nist.gov/800-63-3/.

While this publication applies to government agencies, it represents new thinking that is sure to be embodied in the NIST Cybersecurity Framework, draft version 1.1, which is in the process of being finalized as we write – we expect the Framework to be finalized by the time this article is published. NIST is phasing out the requirement of periodic password changes – which has been the foundation of password policies for many, many years. Other recommendations include using a length of a least eight characters or more and choosing a passphrase rather than a "password." Some applications and devices allow users to include spaces and even *emojis*, which users can now include when setting their passphrase. As always, do not use dictionary words as these are easy to brute force and please, please force computers to require screen-saver passwords and ensure that passwords are required after a reasonable period of inactivity. Newly included is checking all passwords against a database of known compromised passwords, which will of course eliminate all of the dreadfully easy passwords that users are so fond of employing.

Users should never share their password, write it down or reuse the same password anywhere. It is particularly important that credentials used to access a law firm network **never** be used anywhere else. The use of a password manager can make this task quite easy. Consider enabling two-factor authentication (2FA) when available. Biometrics alone is not a good solution – once your biometrics are owned, they will always be owned. Remember the 5.6 million fingerprints stolen in the U.S. Office of Personnel Management data breach? You can't change your fingerprint.

A password policy should be part of an overall comprehensive security program, which should also encompass an incident response policy, disaster recovery plan and social media policy to name a few.

Patches and updates

Firms need to prioritize efforts to keep hardware and software as current as possible. Keeping up-to-date doesn't always have to cost money – see Windows Security Updates. You don't need to be first in line for the latest and greatest, but don't be the last in line either. Once software becomes unsupported, it is unethical to use it because it is no longer receiving security updates and is vulnerable to attacks. In January 2017, Microsoft stated that Windows 7 is so outdated that patches can no longer keep it secure. Extended support ends 1/13/20, so the operating system will not get any further enhancements and will receive security updates only. What does this mean? It is time to plan an upgrade to Windows 10 if you haven't migrated already. Windows 10 security is leaps and bounds better than what Windows 7 provides.

Firms need to apply patches **as soon as they are available** to reduce the vulnerability to attack or compromise. A perfect example – "notpetya" ransomware – attacks a vulnerability of Windows' Server Message Block (SMB) which is first believed to have been developed and exploited by the NSA – released by hackers in April 2017. Microsoft released a patch to address this security vulnerability in March of 2017, so if a computer system hasn't been updated with security updates since then, it could be vulnerable to this ransomware variant. If you have a Windows Domain environment, have your IT provider configure Windows Server Update Services to download and push out Windows Security Updates to all of your client computers and servers as they are released – a free solution to keeping your operating systems updated.

Encryption

Encryption, once just technical-jargon or something the German World War II Enigma machine used, is now becoming the de facto recommendation from cybersecurity companies. Why? It's no longer cumbersome and time-consuming, but is cheap and easy to set up and use (and maybe ethically required for attorneys – see the ABA's Ethics Opinion 477 (May 11, 2017) on encryption of attorney-client email. Your laptop should be protected with whole-disk encryption – no exceptions. Ditto for any external USB flash drive or hard drive used to store firm information. Stolen and lost laptops are one of the leading causes of data breaches. Many of the newer laptops have built-in whole-disk encryption. To state the obvious, make sure you enable the encryption, or your data won't be protected. For others, Windows BitLocker and Apple FileVault II are free encryption options included with Windows and macOS systems – there is no excuse for not using this free protection.

Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe at power on. Failure at that point leaves the computer hard drive fully encrypted.

The same applies to mobile devices - encrypt, encrypt, encrypt. For modern phones – just enable a PIN or password lock code. We recommend six or more characters. Yes, if you use an Apple iPhone, the recommendation is still the same as these devices are not inherently more secure than other devices. You would not believe how many users (and attorneys) still believe that Apple products aren't capable of contracting malware. Apple itself refutes that thought. For the Samsung Galaxy S8, users can use a fingerprint, iris scan or facial recognition (don't use the selfie – this form of 'protection' was compromised within 24 hours!). And don't forget anti-malware software on your mobile devices, such as Sophos, Lookout, Kaspersky or McAfee – ransomware attacking mobile devices is on the rise.

Sometimes convenience causes issues. Providing remote or mobile users with access can create more vulnerabilities than you might realize. To combat this, mandate that all work-related Internet sessions be encrypted. Prohibit the use of public computers and unsecured open public Wi-Fi networks. Access to the office network must always occur through the use of a VPN, MiFi, smartphone hotspot or some other type of encrypted connection. For users that need to connect directly to their work computer, use an encrypted remote control solution such as Citrix, LogMeIn or GoToMyPC. The setup of this kind of software couldn't be any easier and we've seen many attorneys accomplish this on their own.

Employee security awareness training

Malware loves to prey on uninformed users. These victims are the primary cause for the continuing propagation of malware infections, with users clicking on things that they shouldn't be. Why, you might ask? Curiosity, fear, urgency, recognition (such as being named for an award) are generally recognized as the top four motivations for clicking. Over 91% of all hacking attacks begin with a phishing e-mail, which is why it's imperative that you train all of your employees.

Sadly, one of the most often-overlooked aspects of an organization's security readiness is end-user training. It is just as important that your employees know what not to click on as it is to have security software installed to help prevent malware outbreaks. Firms should provide mandatory social engineering and safe computing awareness training to everyone at the firm at least once a year. And make it mandatory!

Technology alone cannot protect your data. The greatest vulnerability comes from your greatest asset - the folks who use your network. Cyberattacks are successful because someone usually did something

stupid like clicking on a link, opening an e-mail attachment, or verifying an ID and password when they shouldn't have. With education and practice comes a more informed and safe user. Look into services that provide phishing assessments, such as Duo Insight (www.duo.com/resources/duo-insight) as a way to test and educate your employees against phishing e-mails. Integrating this testing into annual training is a great way to get your employees to learn, to have a fun competition and to identify those employees that may need some extra "attention" and practice. By the way, a single training session has been shown to reduce the risk of a successful phishing attack by 20% - not a bad return on your money.

Technical solutions

You can also augment your training with technical solutions. There are e-mail scanning services such as Mimecast, which convert attachments into a "safe" format such as PDF. There's also an option to scan URLs in messages and warn of any suspicious links.

There are some free and not so free solutions that your firm can implement to increase your security posture against ransomware and other malware threats. Much of what we describe is probably included in the software that your firm has already purchased. It is just a matter of turning the security settings and requirements on. Our list of security recommendations could fill a book, but we have tried to include the primary essentials above.

Doing nothing makes no sense - you are just begging to be "owned" by the next piece of ransomware or malware. By implementing some of the solutions described above, you are doing your "due diligence" to batten down the hatches, protecting your firm from becoming the victim of the threats that will continue to wreak havoc for the foreseeable future. Cybersecurity is a moving target – as threats morph, so will the defenses – keeping yourself educated on information security issues is a very high priority for all lawyers.

The authors are the President, Vice President and CEO of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Security Awareness Training for Law Firm Employees

by Sharon D. Nelson, Esq. and John W. Simek

© 2017 Sensei Enterprises, Inc.

Introduction and stats

Sadly, your greatest asset – your employees – are also the greatest threat to your cybersecurity. We know this because we regularly see data breaches and ransomware infections caused by click-happy employees. You also have rogue employees determined to use their own devices, go where they want on the Internet, irrespective of firm policies. When we train them, they tell us that they are scared – and you know what? That means we did our job. One of the great fallacies that employees believe is sometimes called "The IT Shepherd" – they simply have faith that the flock (employees) is protected no matter what they do by the shepherd (technology). You need to make them understand that no technological defenses are ironclad.

Let's look at a few statistics. The Computing Technology Industry Association (CompTIA) released the results of a study of 1200 full-time employees in October of 2015. 63% used work mobile devices for personal activities. 94% used mobile business devices to connect to public Wi-Fi networks. 78.5% used public Wi-Fi to check work e-mail and 60% access work documents.

45% have never had any cybersecurity training from employers. 41% don't know what 2FA is. If you don't know, it is two-factor authentication, a more secure way to protect data than using a password alone. 27% know the name 2FA but not how it works.

When researchers salted 200 unbranded USB drives in public, at airports, coffee shops, and parks in Chicago, Cleveland, San Francisco and Washington D.C., 17/% were picked up and used. The flash drives had a trackable link and a text file to tell them to mail an e-mail address. Even IT workers did this – and they should know better!

The Association of Corporate Counsel published *The State of Cybersecurity Report* in December of 2015: Over 1000 General Counsels responded. The dismal result of the survey included the fact that only 1 in 3 track attendance at mandatory cybersecurity training, only 19% give a test, and only 17% have "simulated security events."

Who should do the training?

Certainly not law firm owners. Even if they think they know something about cybersecurity. The biggest hammer is a third-party consulting firm that clearly knows what they are talking about and can answer a fusillade of questions, which generally come fast and furious during training sessions. They bring credibility with them because of their credentials.

If you are an Am Law 200 firm, you are likely going to hire one of the big guns with a hefty price tag. If you are a smaller firm, there are likewise plenty of smaller companies who do cybersecurity training. You want a company that has something of a specialty in training. Hopefully, they have sample phishing e-mails and tests they can give your employees to demonstrate that they are aware of security risks. If an employee repeatedly fails such tests, is that really an employee you want around sensitive data?

Using paper manuals to train is worthless. Online training is not as engaging or effective (our opinion) but 32% of employers use it. In-person group workshops seem to work best. And for heaven's sake,

don't bellyache about the loss of billable time. If you think training is costing you money, just think about what a data breach would cost you – that may put it in perspective.

Training Tips

It sounds silly, but make training (as much as you can) fun. Encourage interactivity – make sure you ask your outside training company HOW they train. You want to hear about sample phishing e-mails, post-training testing, on-the-fly interactive responses as to whether an e-mail shows any evidence of being a phishing e-mail (the number one way law firms are breached). Better yet if you hear that they make a contest out of it, have a whiteboard to list the phishing methodologies they discover – even giving out small prizes. Use real life scenarios. They should tell stories. They may have attendees watch short security videos from YouTube (Sophos makes great ones). We love their tag line: "Skip the book and just watch the movies." And they are right – this is a vital part of effective training.

Time of day? Best done in the morning, when folks are most alert. Spring for breakfast and keep the coffee coming. Cybersecurity can be mind-numbing if not done right.

Make it mandatory? Absolutely. Take attendance. When we trained at one law firm, the managing partner told us he had sent around a memo stating bluntly that the training was mandatory and that he would be at the training and expected to see everyone from the firm there. Splendid idea –and everyone did indeed show up.

How often should you train? At least annually. Threats change and defenses to threat change. Both technology and security policies change. You should assess these changes and your security policies on a regular basis to stay ahead of the curve. You can never "set it and forget it" in cybersecurity.

One famous story that may give you pause: Weeks after falling victim to a data breach in 2015, JPMorgan sent a fake phishing e-mail, which 20% of its employees clicked on. If your results are anything like that, you are in desperate need of cybersecurity training for your employees. JPMorgan got the point – having spent $250 million on cybersecurity in 2014, it vowed to double its cybersecurity budget to $500 million over the next two years.

Physical security

Trainers should be talking about physical security too – not leaving files in stacks around the office, being aware of strangers in the office, etc. One of our friends dressed as a custodian and followed a real custodian right into an office building and got into a law firm. Easier than you think. The infamous "office creeper" in the D.C. area during 2015 got into all sorts of "secure" buildings, once getting into a law firm. She was a standard issue thief, taking money from drawers and purses, lifting laptops and cameras which were easy to pawn. But what if she had been after data?

She got through building security by piggybacking and tailgating. Your trainer will explain those terms if you don't know them. And we're betting most readers do not.

Don't be stupid!

This is the essential message of training. Above, we told you about "salted" flash drives in public places. That's called "baiting" – and people fall for that tactic all the time.

Likewise, if you know that another employee is engaging in insecure behavior, you should inform a supervisor. “See something? Say something” doesn’t apply just to possible terrorism, but to cybersecurity as well.

Encryption

Every training session is going to include encryption. Not the math, which employees don’t need to understand, but the critical need for encryption to protect confidential data. They will learn about encryption on all of their devices and e-mail encryption. There was a day when encryption was costly, cumbersome and a royal pain, but those days are long gone. It is now cheap, simple and easy. More and more ethicists are stating that lawyers should use encryption “where appropriate” – which is pretty much anywhere that data which ethically must be protected exists.

Don’t be mad at your employer!

Employees dislike many aspects of information security. A good trainer will have your back on this one. They will explain why your security policies are needed and why they must be enforced. They’ll talk about how the firm may protect its data through application whitelisting, logging of certain events, installing software or hardware that “reports” when certain files (or a certain large number of files) are accessed. They will talk about the dangers of bringing your own device, bringing your own network and bringing your own cloud. They will explain why such things may be forbidden or why they are tightly managed.

They will explain if your technology prohibits employees from opening attachments without asking for the attachment to be released by your IT or information security department. If you control where they go on the Internet, they’ll explain that too. They will explain why employees have to give up their beloved (name your software of choice) because it is no longer receiving security updates.

Trainers explain the importance of strong passwords, especially log-on, screen saver and financial credentials. They will encourage the use of two-factor authentication where it is available and they will report on the new Carnegie Mellon studies showing that password length is more important than complexity, which is agreeable news since it is easier to remember a lengthy passphrase than a complex password. There is a new draft document from the U.S. National Institute for Standards and Technology (NIST) which recommends password length over complexity. The rules keep changing, don’t they? But that too is why you train on a regular basis.

And trainers will preach the value of encrypted password managers – darn near a necessity if you are going to follow the cardinal rule of not reusing passwords everywhere which often leads to one breach compromising your security, and that of the law firm, in many places rather than just one.

Social engineering

People who are experts at penetrating businesses through social engineering say it generally takes them less than an hour to get into your network. We are so anxious to be helpful. Your employees need to know that Microsoft Tech Support will never call and ask for access to their machine (yes, we’ve seen lawyers duped). They also need to understand that someone who calls and says they are from your IT company and need log-in credentials to fix a problem may not really be from your IT company, even if they know the company name.

Phishing

As we said before, phishing is the easiest way into law firms. Even good enterprise anti-malware software doesn't catch everything – and there are plenty of zero day (no known defense) exploits sold on the Dark Web every day. Lots of studies have shown that roughly 20% of phishing e-mails will be opened.

The worst threat comes from targeting phishing attacks, where the hackers are specifically targeting your law firm. Law firms are at a disadvantage here – so much legal data is public. A hacker may know what cases you are involved with, who the attorneys are, which courts cases are in, etc. And they can spoof the e-mail address of an attorney or a court – how many folks can resist opening something that appears to come from a court?

Law firms are also at a disadvantage because they are "honey pots" – they hold the data of so many clients. Hackers may do a little research on the firm's website or on an attorney's LinkedIn page where they may find personal information that they can insert into a targeting phishing e-mail. Trainers will get them to PAUSE, THINK, INSPECT and REPORT before clicking on any attachment or links in the e-mail.

There are obvious phishing clues to pass on to employees:

- You don't know the sender
- You do know the sender but if you look closely, the address is one letter off (this one happens a lot)
- Nothing in the note seems personal to you
- You weren't expecting the e-mail
- Reference is made to a bank/product/service you don't use
- Words are misspelled
- The grammar is poor
- The e-mail doesn't address you by name
- The message asks for personal information
- There is an attachment which seems suspicious in conjunction with other factors or a link to a website (and no, hovering over the link doesn't necessarily ensure that you will go to the address shown – drive-by malware infections from visiting malicious sites are quite common)

The list goes on and on – you need to advise your employees to be alert to anything suspicious and not to be quick to click!

If they end up with malware, they may not know it. But some possible signs might include, sudden slowness of devices, strange messages appearing on the screen, the inability to open a file, machine crashes, running out of hard drive space, a high volume of machine activity, suddenly having a new browser home page or tool bar the employee didn't install, new programs appear that start automatically, etc.

Ransomware

Ransomware is an international epidemic. Your employees need to understand that it is usually contracted via phishing e-mails. Click on a link in the e-mail or an attachment and the malware is downloaded invisibly irrespective of what you see on the screen. Then it sets about encrypting the firm's data, file by file. If the backup is connected to the network at the time, it will encrypt that too.

Employees really need to understand how dangerous ransomware can be, how prevalent it is, how the ransom to get your data back is more and more expensive – and that you are out of business until you slog through trying to figure out how to get sufficient funds in bitcoins (which the hackers generally want as payment) – and then there is a delay after receiving the decryption key in restoring the files (assuming you do in fact get the key).

While you can be protected from ransomware by having a properly engineered backup, if you get ransomware, you still have to live through some period of time while the files on an unaffected backup are restored. And we are now seeing ransomware on mobile devices, including phones – most from downloading apps from unsanctioned app stores, a very common practice among employees!

Business e-mail compromises

These are also known as CEO scams and the FBI reports that they have netted more than 3 billion dollars thus far. From January 2015-June 2016, there was an increase of 1500% in successful attacks. That's one heck of a statistic. Basically, someone who has authority to order money wired appears to be e-mailing someone who actually does the wiring. Law firms have been hit hard by these scams, so it is critical that employees understand how they work and that they be conditioned to seek affirmation of any order to transfer significant monies.

More in the Morass

Clearly, there is a wealth of threats that employees need training on – more than we can possibly address in a single article. Employees need to be trained on the dangers of metadata, the safe use of public Wi-Fi, the safe use of file syncing software in the cloud, the perils of using social media, the need to protect all devices (including Apple devices), the malware that may be present on public computers in hotel business centers, public libraries and Internet cafés, the need to make sure (if they work from home without a VPN) to make sure that their home Wi-Fi is secure, how to secure their smartphones (especially if they are allowed to connect personal devices to the firm network), and the need for managed vendor access.

Hopefully, you have a sense of how critical it is that you train your law firm employees on cybersecurity. We know of one firm in California that averted disaster because all employees had recently received training on phishing e-mails and when they were on the receiving end of a targeted attack against their law firm, the employees recognized the phishing e-mails and quickly spread the word. Disaster averted. We have no doubt that the firm invested time and money in the training, but we're betting that, having survived the attack, the firm counted every dollar as well spent!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com

Secure Computing Abroad: Evolving Law Firm Policies

by Sharon D. Nelson, Esq. and John W. Simek

© 2017 Sensei Enterprises, Inc.

Traveling abroad? Worried about pickpockets? We have far bigger worries these days. If you travel abroad, you also have to worry about foreign governments – and our own – which may be interested in our data. Lawyers are not only not exempt from that interest – they are magnets. And when *The New York Times* published an article early this year about safeguarding data when crossing the border, we knew we were seeing a new hot cybersecurity topic – one that has primarily been considered at very large firms, until all the recent stories caught fire in the news. This article will focus on the dangers presented by our own government (the current runaway headline), but the advice is generally applicable to the risks presented by foreign governments, risks which may increase as there seems to be a worldwide ratcheting up of device seizure and examination at borders.

Three U.S. Border Incidents

There have been many, many border incidents, but here are three that caught our attention. A U.S.-born NASA scientist, Sidd Bikkannavar, returned to the U.S. in January of 2017. A seasoned international traveler, he flew back from Santiago, Chile to the George Bush Intercontinental Airport in Houston, Texas on Monday, January 30th, just over a week into the Trump administration.

Bikkannavar says he was detained by U.S. Customs and Border Patrol (CBP) and pressured to give the CBP agents his phone and access PIN. Since the phone was issued by NASA, it may have contained sensitive material that wasn't supposed to be shared. A Customs officer presented Bikkannavar with a document titled "Inspection of Electronic Devices" – which mentioned detention and seizure - and explained that CBP had authority to search his phone.

Bikkannavar was not allowed to leave until he gave CBP his PIN. Ultimately, feeling pressured, he agreed to hand over the phone and PIN. The officer left with the device and didn't return for another 30 minutes. The phone was returned to Bikkannavar, though he's not sure what happened during the time it was in the officer's possession. When it was returned, he immediately turned it off because he knew he had to take it straight to the IT department at NASA's Jet Propulsion Laboratory (JPL). The cybersecurity team at JPL was not happy about the breach.

Haisam Elsharkawi, an American citizen, was about to travel from Los Angeles to Saudi Arabia in February of 2017 when he was stopped at the airport, questioned, handcuffed, questioned some more and then released without charges three hours after his flight had departed. He reported that officers from the United States Customs and Border Protection repeatedly pressured him to unlock his cellphone so that they could scroll through his contacts, photos, apps and social media accounts. He said they threatened to seize the phone if he did not comply.

Also a veteran international traveler, he was appalled but felt pressured to unlock his phone and a Homeland Security agent looked through it for about 15 minutes.

In October of 2016, border agents seized phones from a Canadian photojournalist. He refused to unlock the phones, citing his obligation to protect his sources – he was blocked from entering the U.S.

As of March 13, 2017, NBC News had examined 25 cases in which American citizens said that CBP officials demanded that they hand over their phones and their passwords – or unlock them. In 23 of the 25 cases, these individuals were Muslim.

Keeping Private Data Private

Stories like these prompted *The New York Times* to investigate how to protect private data. As the paper states, U.S. citizens are not required to unlock their phones or share passwords with U.S. government officials. However, rules may vary depending on where you are traveling to and from. But being detained and intimidated is not an experience any traveler wants to go through.

So the *Times* recommended traveling with clean phones (so-called "burner" phones are often available at airports, as are phones you can rent) and clean tablets or laptops. It is recommended that you disable fingerprint readers because, in the U.S., law enforcement agencies can use warrants to compel you to unlock your phone with your fingerprint. We would go further and advise disabling all biometrics used to get into your phone, such as iris scans and facial recognition.

If you tell an official that you will not give up your password, the official may not be happy - to put it mildly. Better to use a password manager and tell the agent that you don't remember your one very long master password. And to avoid complications, don't have your password management software loaded on your devices. It is best to store the password vault (encrypted of course) in a cloud service like Dropbox and get access to it when you reach your destination.

If you are asked for passwords to your social media accounts or your e-mail, you can protect yourself by having two-factor authentication enabled – assuming that you have left your phone at home. Since the text code will be sent to that phone, officials will be unable to get into your accounts even with your password. You could leave your phone with someone you trust and get those codes that way but the general advice is to forego the use of social media while abroad.

When dealing with e-mail, do not install and configure any e-mail client on your laptop or cell phone. You don't want to have any e-mail on your devices. You should use some sort of remote access solution (e.g. Citrix, LogMeIn, etc.) to access your e-mail. Even using a browser could leave remnants of confidential information on your device.

Any device you use while abroad should be encrypted. The best way to ensure that your data remains secure is to back up your data to a cloud service and then wipe all of your devices before you return home. Once home, you can restore your data from the backup.

No matter what device you use abroad, assume that all electronic communication is subject to interception. This means you should always be using a secure encrypted connection. Make sure you have a properly configured VPN available and know how to use it.

The Authority of U.S. Customs and Border Protection Agents

Not only were we almost completely ignorant about the authority of CBP agents, it turns out that most lawyers have little knowledge of how expansive CBP authority really is. CPB officers have search power extending 100 air miles inland from any external boundary of the U.S. They can stop and question people at fixed checkpoints dozens of miles from U.S. borders. They can also pull over motorists whom they suspect of a crime as part of roving border patrol operations.

You might say - But doesn't the Fourth Amendment protect us from "unreasonable searches and seizures?" Yes – however, those protections are lessened when entering the country at international terminals at airports, other ports of entry and any location within 100 air miles of a U.S. boundary.

According to federal statutes, regulations and court decisions, CBP officers have the power to inspect, without a warrant, any person trying to gain entry into the country – and their belongings. The CBP's authority extends to examining computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices. That cuts a wide swath.

Current CBP policy dictates that officials should search electronic devices with a supervisor in the room when feasible and also in the presence of the person being questioned "unless there are national security, law enforcement or other operational considerations" that take priority. We already know that this language has been invoked to examine devices outside the presence of the person being questioned. CBP says it can conduct these searches "with or without" specific suspicion that the person possessing the items is involved in a crime.

With the approval of a supervisor, CBP officers can seize an electronic device – or a copy of the information on the device – "for a brief, reasonable period of time to perform a thorough border search." Typically, such seizures should be no more than five days (which seems a lot to us), but officers can apply for extensions in up to one-week increments. If the review of the device and its contents doesn't manifest probable cause for seizing it, CBP says it will destroy the copied information and return the device to the owner.

What if you are a lawyer? CBP has recognized that lawyers have an attorney-client privilege, but all this seems to mean is that agents have to get approval from an agency attorney before proceeding with the search. Not terribly comforting – and we suspect this is the reason why we have seen so many firms begin specifically to address the potential problems of re-entering the U.S.

What Have the Courts Said?

Unfortunately, the Supreme Court has not directly ruled on whether the CBP can search electronic devices without any specific suspicion that the owner might have committed a crime. In 2013, a decision for the U.S. Court of Appeals for the Ninth Circuit (http://cdn.ca9.uscourts.gov/datastore/opinions/2013/03/08/09-10139.pdf) affirmed that a cursory search of a laptop – for instance, having an owner turn on his/her devices and examining their contents – does not require any specific suspicions about the traveler. The court raised the bar for a "forensic

examination" of the devices such as using "computer software to analyze a hard drive." For these more comprehensive and intrusive searches, including password-protected information and other private data, officials must have a "reasonable suspicion" of criminal activity. That court decision applies only to the nine Western states in the Ninth Circuit.

We like this quote from the court's decision: ""Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives . . . It is little comfort to assume that the government — for now — does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome."

During the 2016 fiscal year, CBP officials conducted 23,877 electronic media searches, five times as many as in 2015. That's a striking escalation.

What Law Firms Are Doing

As part of our research for this article, we were given access to one law firm's security precautions when traveling abroad. They included the following guidelines:

- Use one of the firm's "clean" loaner laptops, wiping the laptop before returning home
- Store all documents on the firm's network – store nothing on the laptop
- Use a burner phone (not a smart phone) for calls and texting.
- Access the firm's network via Citrix for e-mail and documents from the laptop - do not access the network from the phone.
- Do not use Bluetooth.
- Lock the laptop in the hotel room safe or in locked luggage.
- Make sure microphones and cameras are turned off.
- Change your network password before leaving the U.S., change it again once you return, after you have turned in your loaner laptop.

We have boiled the essential instructions down – as you can imagine, the instructions are far more detailed. A guiding principle is that authorities cannot search what you don't have. For those who want to chance it and have their device/data with them, make sure the device is encrypted and that it is powered down before going through Customs.

Several experts have published arcane methods of protecting your data, but we have not included them as being beyond the ken of most attorneys. And none of them will protect you from actually facing an angry CBP (or foreign) agent telling them that you really don't have any way to get to your data. We much prefer the "they can't search what you don't have" way of thinking.

In March of 2017, The Electronic Frontier Foundation published a fairly lengthy guide called "*Digital Privacy at the U.S. Border: Protecting the Data on Your Devices and in the Cloud*" which is worth reading and may be found at https://www.eff.org/wp/digital-privacy-us-border-2017.

Conclusion

In an article, it is impossible to examine every possible precaution that lawyers might use to protect client data while abroad. And though we've focused on the U.S. border because of current events, we have spent years watching videos of the Chinese spies accompanying maids to hotel rooms and inserting a flash drive in a businessman's computer. And we've heard stories from our large law firm friends of laptops coming back from abroad with "a little something extra" – that transmits data back "home". If you are a mid-to-large firm lawyer, your firm probably has very competent IT/cybersecurity help to assist you – don't be afraid to ask questions! And if you are a solo or small firm lawyer, make sure you engage someone who has both technical and security certifications to help you make sure you have the necessary security precautions in place.

The authors would like to thank their friend, journalist Ben Kerschberg, for his kind assistance in researching some aspects of this article.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Securing Your Law Firm's Website: A Critical Cybersecurity Task

by Sharon D. Nelson, Esq. and John W. Simek

© 2017 Sensei Enterprises, Inc.

One of a law firm's most critical assets is its website – and yet protecting it is a priority that is often overlooked. Reading this and you're not in a law firm? The same rules apply, so keep reading!

A lot of lawyers simply don't think about protecting their websites. They ask why anyone would target them, especially if they are solos or small law firms. The sad truth is that, today, the majority of attacks against websites are automated. The bad guys throw out a net looking for websites with vulnerabilities and pull in whatever insecure fish they can find – along with any data held on your website.

If you are targeted, the risk is much greater. In all likelihood, you are now facing a more sophisticated attacker with a clear agenda who is likely to have more sophisticated tools.

One of the threshold questions is "Where is your website held?" Are you hosting your own website or is someone else hosting it?

For many years, we have advised law firms not to host their own websites. Some years ago, one client decided to ignore our advice. The managing partner came to work one day to find that the law firm website home page said "F*** the U.S. Government!" Not precisely the best image for a law firm website!

Also, if you host your own website on your network, ALL of your data may be compromised if the website is breached. Another very unhappy thought. Much better to put the security of your website in the hands of another company which has experience in providing website security.

Remember that many websites have been taken over by hackers – and the results are never pretty. Your website is your public face – any compromise of that face, which is generally your primary advertising vehicle, is going to constitute a gut punch to your law firm's reputation.

So if (yes, it has happened) your website is redirected to a pornography site, you will be tearing your hair out trying to fix the mess. Sometimes, things like this are done because a hackivist (a hacker with a political agenda) doesn't like one of the

clients you've represented. Sometimes, they may try to extort money in exchange for putting things right or for not using the data they were able to harvest.

In this day and age, websites can have a lot of functions. Many collect information from prospective clients, including e-mail addresses, phone numbers, etc. This is information which can be sold on the Dark Web. If you have a client portal through your website and that gets breached, the extent of the disaster is compounded exponentially.

Larger websites of big law firms have a considerable amount of computing power at their beck and call – it is possible for a bad guy to use that power to screw with you, or to attack someone else (with you in the middle of the mess). If indeed you are collecting e-mails on your website, cybercriminals may use those e-mails for phishing purposes, sending messages far and wide in the hopes of compromising someone else.

The problem with websites is that you want everyone to have access to your website which makes it public and vulnerable. If you have a lot of applications and interactivity on the website, it is that much more vulnerable because there is code running those functions, which heightens the possibility that the code has vulnerabilities. Custom coding is often riddled with weaknesses.

Hackers routinely probe websites for vulnerabilities – a weak coding practice by a developer which adds functionality is a potential gold mine. The hacker may be able to submit commands to extract data from your database not in a way that the developer intended. This particular nightmare is known as a SQL injection – and boy oh boy, have we seen a lot of those.

Then there is cross-site scripting (XSS) in which an attacker uses XSS to inject client-side scripts into web pages viewed by others. The attacker can use XSS to control a web browser and/or modify how content is displayed on a website. You can only imagine the mischief that the attacker can create.

Even the old-fashioned brute force attacks have been known to work. It's a dangerous world – and there are now over one billion websites out there waiting to be compromised.

Frequently, websites run on open source software and people download software that comes with vulnerabilities in it. You must be careful to proactively patch your site as security updates become available.

As we sit typing this article, here is a headline from *Naked Security*: "Critical Vulnerabilities Pose a Serious Threat to Joomla Sites." The post says "Joomla, the world's second most popular web content management system (CMS), has been under sustained attack for several days, thanks to a nasty pair of vulnerabilities . . . "

Apparently, flaws in Joomla's user registration code could allow an attacker to "register on a site when registration has been disabled" and then "register … with elevated privileges." This mean that the vulnerabilities could be used to unlock any site running Joomla, anywhere on the Internet, with little more than a request detailing what you'd like to be called and how much power you want. And there are millions of vulnerable Joomla sites.

The culprits here were "incorrect use of unfiltered data" and "inadequate checks" – we've been reading those words for the last 20 years of web vulnerabilities. The solution, for anyone running an unpatched version of Joomla is to upgrade to version 3.6.4 (which removes the vulnerable code) and then test their website for any indication that it has been compromised.

How many times have WordPress websites been impacted? A lot, due to the popularity of WordPress. In one 2014 incident, more than 100,000 websites were impacted. And a heck of a lot of legal website use WordPress.

So what do you need to do to avoid this morass? You need website vulnerability detection and management. Some website providers offer this, but many do not. There are products that identify and remove malware from your website. There are website firewalls that you can use to block attacks – targeted or not. Tools today tend to be affordable for law firms of any size – some are even free, though we would be suspicious of their quality. To find examples, Google "website malware scanners" and "website firewalls."

Everyone would like a security blanket that is 100% effective, but "wanting ain't getting" and there is no such thing as 100% effective cybersecurity solutions. If a vendor claims to have a 100% solution, beat a hasty retreat.

So what if the worst happens and your website is compromised? You should be as prepared for a website breach as a breach of your network. You manage the risk in part by simply planning. An Incident Response Plan should cover website breaches and detail the legal authorities to be notified, steps to take to comply with state data breach notification laws, and processes for notifying those whose data may have been compromised.

In this new era of websites, we are seeing law firms trying to achieve a great interactive experience for their clients. Clients love client portals and love the interactivity, but the more complicated the site and the more interactive it is, the greater the "attack surface" and the more likely the site is to have vulnerabilities making it susceptible to attack. All the neat whiz bang features are wonderful, but you need to work with experts to secure those features. And those wonderful web applications? They (and their custom coding) account for 80% of website vulnerabilities.

We recently had the opportunity to talk with Neill Feather, the President of SiteLock, a firm which specializes in website security in the course of recording a *Digital Detectives* podcast for Legal Talk Network. Disclosure: SiteLock is a sponsor of that podcast. It was a fascinating conversation because we frankly had never interviewed anyone who specialized specifically in website security. To find other such companies, just Google "website security company" – and make sure you get references.

As Neill said, firms continually underestimate the risk of being attacked. He hears them say, "I didn't know this was something I needed to be worried about." When we asked him about making a prediction about the future of website security, always a risky proposition, he said (and we agree) that the Internet of Things is revolutionizing security. He expects IoT devices to make website attacks more frequent, with less opportunity to bask in obscurity thinking one is safe. More and more, website owners – law firms included – will need to take proactive steps to protect their websites.

Lawyers tend to view security as an unwelcome chore – and having to deal with website security as well as network security just gives them a monumental headache. But the flip side is to think of website security as enabling. You can do neat stuff with a client portal and other website features giving clients a better

experience. This feeds into very successful marketing and ultimately, client satisfaction born of a great website experience.

You have a lot to gain by building an interactive website with a client portal. But never lose sight of security or you may tarnish your brand's reputation if your website is compromised. Hindsight may not be much of a balm if that happens!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Are Alexa and Her Friends Safe to Use in Your Law Office? The Pros and Cons of Personal Assistants

by Sharon D. Nelson and John W. Simek

© 2017 Sensei Enterprises, Inc.

Many commentators have predicted that 2017 will be the year of Amazon's Alexa. Alexa is one of several virtual voice assistants that are working their way into our everyday lives. The Amazon Echo and the smaller Echo Dot had a great sales year in 2016 and finished off the holiday season as the best-selling items on Amazon. Estimates by Forrester indicate that 6 million Amazon Echo devices were sold by the end of 2016. That's a lot of hardware.

Alexa is just one of the virtual assistants available for lawyers today. There's also Google Home/Google Assistant, Siri, Cortana and Samsung's Bixby on the Galaxy S8 and S8+. Siri was the first on the market but has rapidly lost ground to Alexa and Google Assistant, the two big players in the virtual assistant offerings. Google has the advantage for research since it has access to the power of Google search. Alexa is a better integration device, especially with the addition of "skills" that allow it to connect to other services and apps. Bixby is the newest player in the virtual assistant space and promises to have some unique features that don't exist in the others. One such feature is the ability to take a picture of something in a foreign language (e.g. road sign, business advertisement, etc.) and Bixby will translate it for you.

There have been many articles about how a lawyer would use a virtual assistant. Some of those uses could include accomplishing simple tasks such as adding entries to calendars, setting reminders, calling people in your contacts, getting directions, obtaining weather conditions, obtaining answers to questions, making purchases, controlling items (e.g. turn on/off lights), reading news items, playing music and the list goes on and on.

Cybersecurity and Personal Assistants

The obvious question revolves around the security of these types of devices. Is Alexa safe to use in a law office? That's a question we get quite often these days. The short answer is yes if you take certain precautions and understand the pros and cons of the technology. Let's start with how Alexa works. Alexa is tied to your Amazon account. That means it is already associated with you and is not anonymous. Alexa is constantly in listening mode, waiting for the wake word to be spoken. You configure Alexa to respond to one of the four (Alexa, Amazon, Echo, Computer) wake words. Amazon has announced that they are working on allowing users to define custom wake words, but no delivery date is currently available.

Once Alexa "hears" the wake word, it starts recording just a few seconds before the wake word and sends the data to the cloud. Amazon performs a speech to text conversion and tries to properly respond to the command or question. Amazon stores the actual recorded session so that you can play it back from your account. That means Amazon also has a recording of any ambient noise that may have been picked up as well.

It is unclear how long Amazon may store the recorded sessions. You do have the ability to delete individual Alexa requests or delete them all. Think of it as clearing up your Internet history. Unfortunately, Amazon uses all of the history to make Alexa "smarter" by learning what you ask for and how you ask it. If you delete all the voice history, Alexa will effectively revert back to a new factory setting. That's the tradeoff between privacy and usability. Maintaining your privacy means less usability.

Alexa can't differentiate between voices either. Some people think that's an advantage since all of your family members or law firm personnel can talk to Alexa using a single account. We believe not differentiating voices is a disadvantage and a big security hole. Anybody within hearing distance of Alexa can ask for information that may be related to your account. As an example, a nosy relative could ask what is on your to-do list, read your mail, send a text message or access any other information that is linked to your account. Amazon has announced that it is working on differentiating voices, but no timetable has been given for delivery of the enhancement.

Samsung has taken a different approach to always-listening devices like Alexa. By default, Bixby won't listen until you press a button. This means the user is in control of the data. With always-listening devices, you really don't know what is being stored by the vendor.

Tips for Keeping Your Data Secure

Because Alexa cannot distinguish voices and it is always on, a best practice would be to physically secure Alexa in your law office. That means it should be in a room away from typical conversations and probably even behind a locked door. Physically securing Alexa gives you much greater control over access, especially since you can command Alexa without giving it a user ID or password. It's another trade-off between security and convenience. If you had to give Alexa your login ID and password every time you asked a question, you would probably ask for your money back within 24 hours.

Another security configuration is controlling purchasing through the Alexa app. By default, Alexa will allow purchases using your Amazon Prime account, where you have already registered a credit card. It's probably not a good idea to leave this at the default setting. Anybody within earshot can make a purchase using your account. You may have heard the San Diego news story about a girl in Texas that ordered a doll house and four pounds of cookies using Alexa. The problem was that a bunch of Alexa devices in the San Diego area "woke up" when they heard the wake word and tried to order doll houses. Humorous, but you see the danger. You can configure Alexa to require a 4-digit PIN confirmation code to complete a purchase or turn off voice purchasing all together.

You have the option of restricting when Alexa listens by muting the seven microphone array. It is a manual process to press the mute button, which effectively disables Alexa. You know that Alexa is in a muted state by the red ring that glows around the edge. Pressing the mute button again puts Alexa back in listening mode and removes the red ring. It would be a best practice to mute Alexa if it is in a conference room where you are having a confidential conversation with your client to ensure that no part of the discussion is inadvertently recorded.

The Pros of Personal Assistants

One of the pros for using voice assisted technology is making tasks more efficient. Rather than opening a program on a computer and typing in data, you can just speak what you want to do and it happens. Control of devices is extremely easy using the technology. Google Home is the hardware that is "powered" by Google Assistant. It was originally designed to work with home smart devices such as thermostats, smart appliances, light controls, security systems, etc. Think of it as remote control on steroids. You can operate all sorts of smart devices just by using voice commands. Adjust the temperature in your office by saying "Set the thermostat to 72 degrees." When leaving the office for the day, you can command all the lights off with one statement like "Turn off all office lights." Even smart appliances can be controlled by voice. As you get ready to leave the house, just tell your voice assistant to turn on the office coffee maker. Fresh coffee will be ready when you arrive.

Another popular usage of personal assistants is access to a music library. Alexa can access music in your Prime library as well as Spotify, Pandora, iHeartRadio and TuneIn. Google Home can access audio tracks from YouTube Music, Spotify, Pandora, TuneIn and Google Play Music. You can play specific tracks, artists, genres, etc. Alexa can read books from Audible or your Kindle library. The Amazon Echo is a more expensive device ($179.99) that projects sound in 360 degrees using the included 2.5 inch woofer and 2.0 inch tweeter. The Echo Dot is a cheaper alternative ($49.99) and only includes a small built-in speaker. You can improve the sound quality by connecting external speakers using a 3.5 mm audio cable or over Bluetooth. In contrast, Google Home is $129.99 for the white version. You can add different color bases for an additional $10.

Siri and Cortana are more limited in what they can do for you. As an example, Siri only supports a handful of uses such as photo search, video and audio calling, payments, messaging and ride booking. Siri has begun to work with some third-party apps with the release of iOS 10, but usage is fairly limited. Apple is trying to get into the smart home control market with its HomeKit connected solution, which is still in its infancy.

Google Home has the edge for lawyers, especially when it comes to research. That's because Google Home has access to the vast database and power of Google search. Using Google Home is like using your voice to search Google instead of typing the search phrase in a Google search box. Alexa will respond with "Sorry, I couldn't find the answer to your question" for things that it doesn't know about. You do have the option of using Bing for searching if it can't find the answer to your question, but you have to use the Alexa app for that. The reality is that Alexa is pretty poor at searching. If you want to use your voice assistant as a legal research tool, you're better off with Google Home. Who knows? Perhaps some developer will release a "skill" for Alexa allowing the use of Google instead of Bing for searching.

What happens to your personal assistant data?

The big concern among lawyers is the potential evidence that a voice assistant may capture. We know that Amazon stores the requests to Alexa since you can see them in your Alexa app. As previously stated, you do have the option of deleting them. We already know that prosecutors in Arkansas have issued a search warrant for data from an Amazon Echo that was in the home of James Bates, who was accused of strangling and drowning a man in his home last year. Amazon has rejected the request as

being overly broad. We don't know if Amazon will be compelled to release the data, but the point is that Amazon does have data that can be used as evidence.

Apple reportedly stores your Siri data for two years. Supposedly, the data is anonymized to protect the users' identity, but do we really know for sure? Like Alexa, you can view your Google Home history and delete it if you want. Google does save your queries so the situation is very similar to Alexa. What if law enforcement wants access to your Google Home data? How long does Google keep the information and will they turn it over? Even though the vendors say they are concerned about users' privacy, the point is that technically your information can be stored for a long time and turned over to the government or law enforcement. The devices themselves (e.g. Echo, Google Home, etc.) don't store the user requests. The information is sent to the cloud. The situation is a little different if you are using a voice assistant on a mobile device. There is the possibility that some data resides on the mobile device as temporary storage in addition to being sent to the cloud.

Another best practice for lawyers is to periodically inspect the stored history. Deleting the history on an occasional basis is probably a good idea too, but that would impact the efficiency of using voice assisted technology.

What's a lawyer to do?

Lawyers have specific ethical duties, so they have to be more careful than the "who gives a darn about privacy?" masses. We have found that lawyers rarely think about keeping data confidential with respect to their personal assistants, which tend to be compellingly addictive. Just as it took a while to get used to the notion that we need to be serious about protecting confidential data on our computers and phones, it will likely take a while for the legal profession to wrap its head around the dangers of personal assistants – and the rich lode of potential evidence that may be found in the clouds that store questions or commands addressed to personal assistants.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Can You Trust Your Expert Witnesses with Confidential Data?

by Sharon D. Nelson, Esq. and John W. Simek
© 2017 Sensei Enterprises, Inc.

Not always. There was a recent case in which confidential data was not, to put it mildly, well handled. The corporate defendant, a mortgage servicer, was accused of violating a consumer's privacy rights based on the manner in which it handled collection calls. The defendant protected its customer data with layers of network security consistent with best practices and ISO guidelines. During discovery, the plaintiff's experts received the calling data and copies of the customer service call recordings.

Both experts had unrelated full-time day jobs. Their expert witness work was a side business run out of their homes. Neither expert had a technical degree, and neither had taken a course in data security for over a decade. Both experts stored the sensitive case data in their homes. There were no locks on the doors to their home offices, so anyone in the houses had access to the drives. Neither expert was familiar with the basic ISO standards relating to data security. Neither had a written data security plan for their home network, and no outside company had ever performed vulnerability or penetration testing on their networks. One expert had no automatic intrusion detection software on his network. Both routinely produced data with sensitive PII (personally identifiable information) in unencrypted form.

The produced debt-collection calls included highly personal discussions in which debtors explained why a mortgage was in default, such as health or financial problems. One expert testified that he kept these recordings on an unencrypted portable laptop and accessed it on his home and public Wi-Fi networks. He also produced the call recordings to a third party to obtain technical assistance. The third party was not asked to execute the protective order, and that data presumably still resides on the third party's servers.

Well, you get the message. Expert witnesses, including us, routinely receive highly sensitive PII for review and analysis. Sensitive PII (SPII) is data that, if lost, compromised or disclosed without authorization, could result in substantial harm or embarrassment to the individual.

Attorneys cannot ignore how their experts manage the data produced to them. When highly sensitive data is produced in a lawsuit, it is removed from the protected network environment built by the data's owner and produced to the lawyers on the other side. The manner in which it is produced is up to the producing party. Sometimes the data is scrubbed of identifying information, such as names and dates of birth, but not always. Sometimes it is produced on encrypted drives, but again, not always. Instructions are rarely given to an expert regarding the manner in which to store the data or the type of security controls that need to be employed to keep it safe from unauthorized disclosure. That is certainly true. I can only recall a handful of cases where attorneys have given us explicit instructions.

Confidential data produced in a lawsuit is often subject to a protective order that contains generic language that the data will be kept confidential. Protective orders typically do not specify the security measures that the receiving party needs to have in place. The promise to keep the data protected is considered enough.

Under most protective orders, the receiving party has the right to produce the confidential information it receives to its experts in the case. Those experts are in turn required to sign the protective order and promise to protect the data. Again, the promise to keep the data protected is considered enough.

Experts at sophisticated firms generally have very competent IT and cybersecurity support. They could still be breached, but it is less likely than when engaging experts who are self-employed or who work in small firms with limited support.

Concrete suggestions?

Pay attention to physical security. Our forensics lab requires a prox card and a registered fingerprint to enter. Entries into or out of the lab are video recorded. There is a dual authenticated safe in the lab for high profile cases. Only three of us have access to that safe. We have a security system with motion sensors – and the police will be summoned unless someone with authority quickly acknowledges an equipment problem or a mistake (such as arming the system when someone is still in the lab – and yes, of course that has happened). We have a human receptionist monitoring the front door – in addition to more surveillance cameras. The building itself is locked nights and weekends.

Pay attention to logical security. Our evidence is on standalone offline hard drives or on a NAS unit which has no Internet access. The local network in the forensics lab is dedicated to forensic usage, unconnected to our corporate network. There are software and hardware protections for the lab network as well.

Pay attention to production security. It is the way of the world that most of our productions, by the instructions of our clients, are made via Dropbox. It makes sense since it is instantly available though one must trust that authorized access is not given by the receiving party to anyone who shouldn't have it. All production files are encrypted using 7-Zip before being placed in Dropbox with the password given via phone or a separate e-mail (not the e-mail containing the Dropbox link). If a file is not so large that it cannot be accommodated by Mimecast's Large File Send, we may use that – the data is encrypted as part of the process.

If we use the old school method of shipping drives, they are always encrypted.

There may be more security measures that are not coming to mind, but those are the basics. And, of course, if there is a court order with specific mandates, that order must be strictly adhered to. Most of them, as noted, do not require specifics measures.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

How Does A Law Firm Find a Good Cybersecurity Company?

by Sharon D. Nelson, Esq. and John W. Simek

© 2016 Sensei Enterprises, Inc.

Thanks to our friend and colleague Courtney Kennaday, the Director of South Carolina's Practice Management Advisor Program, for suggesting the topic of this article. As she accurately noted, information security companies "are springing up like weeds." She also asked, "How's a lawyer to know who is good? What should they be looking for in the company's resume?"

Excellent questions Courtney. We hear law firms bemoaning the difficulties of finding reputable (and affordable) cybersecurity companies all the time. Since our company, Sensei Enterprises, Inc., provides those services, hopefully we have some insights to guide law firms in their selection.

Managed security services is an ongoing effort, generally addressed with a long term contract, and not addressed here. That would require an article of its own. We're talking about companies that investigate data breaches and provide security assessments and implement recommendations from those assessments. Let's start with the first question we hear all the time.

Why Do I Need a Cybersecurity Firm?

Almost all law firms have an IT consultant, whether an outside consultant or in-house employee. All too often, lawyers believe that information technology wholly embraces information security. It does not. While there is a lot of crossover between the two fields, most IT providers are aware of basic security best practices – they are not actually cybersecurity specialists – though they may feel that they are!

As technology has gotten more and more complex, it has become critical to have access to folks who do a "deep dive" into security. A security specialist who is all textbook and has no practical experience with IT is no good to you. All the certifications in the world are no substitute for experience.

As we go to press, 25 states have now ratified some version of the ABA 2012 changes to the Model Rules of Professional Conduct, which require technology competence and mandate that a lawyer "shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."

Between the enhanced ethical duties and the flood of data breaches throughout all businesses, law firms have recently recognized the need to focus on keeping client data secure. Hence the proliferation of cybersecurity firms. But as Courtney asked, "How's a lawyer to know who is good?"

The Big Dogs

If you run with the big dogs (AM Law 200), you are probably going to select a large provider of information security services. They cost more, but they offer a large range of services and a depth of knowledge and industry certifications. Among those we see most often are Mandiant (a division of FireEye), Dell SecureWorks, RSA, IBM Security and Root9b.

The Rest of the Pack

We know that the vast majority of lawyers reading this article will be from solo, small or mid-sized practices. The jaw-dropping prices of the large cybersecurity firms are well beyond your reach. But take heart, there are plenty of smaller businesses that provide information security at a price point you can live with. So what are you looking for when you search for this kind of help?

Recommendation, Recommendations, Recommendations

We can't stress this too strongly. Talk to other lawyers and law firms. Who have they used and liked? Did their pricing seem fair considering the work done? What services did they provide? Did they meet their deadlines? What kind of certifications did they have? Were they professional and responsive? If they provided a security assessment, was their deliverable a good report? Did they also make recommendations for remediating security vulnerabilities with pricing? Any negative feedback? Did they play well with your IT folks? This is pretty critical because your IT folks are going to feel threatened the moment they learn that cybersecurity experts are being brought aboard. Good experts will expect a certain amount of tension and know how to defuse it and emerge with a "we're all on the same team" mentality.

References

Any good information security company will be ready with references. Our advice is to be a bit wary. These will be cherry-picked happy customers. You can ask them all the questions above and your instincts about whether the information you're given may be accurate, but we still prefer reaching out to other law firms as referenced above. We've seen too many folks do an Internet search for a cybersecurity company (and of course the company looks awesome on their website) and the references do check out – but then they are disappointed by poor work, a failure to be responsive, escalating costs, etc.

Better, we think, to follow the Beatles' advice and get by with a little help from your friends.

Certifications

You might think that the certifications held by cybersecurity experts would be a real measurement of their skills, but not always. There are certifications you can essentially buy (no testing), certifications with easy tests or open book tests, certifications which aren't true certifications (for instance, a 'certification' that you attended a course) and certifications which are bookish rather than practical.

Real experts get their hands dirty fast. They want to delve into the inner recesses of your network after looking at your network diagram (you have one, right?). You may not understand what they say – the good ones translate cyberspeak into English pretty well – but it's usually clear when you ask a question

and they answer immediately and confidently that you probably have someone who knows what they are doing. If you ask a supposed expert how to engineer your backup to guard against ransomware and they fumble for an answer (and you can learn the answer on the Internet yourself), you'll know pretty quickly who you don't want to hire.

Here's a list of some of the information security certifications that we think are most valuable in evaluating a company's credentials – along with a brief statement of what the certification provides:

CISSP (Certified Information Systems Security Professional) – an independent vendor neutral certification from the International Information System Security Certification Consortium, also known as $(ISC)^2$. It is globally recognized and covers competence in eight domains including:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

The certification requires a passing grade of 700 to 1000 points from a test comprised of 250 questions. You must have at least five years of security work experience (one year may be waived for a college degree) to qualify as an exam candidate. Ongoing education is also required to keep the CISSP current and valid.

CEH (Certified Ethical Hacker) – a certification that assesses the security of a computer system by using penetration testing techniques. The CEH is administered by EC-Council. Similar to the CISSP, the CEH requires two years of information security experience before being eligible to take the exam. The experience requirement is waived if the candidate attends official EC-Council training at an Accredited Training Center, via the iClass platform, or at an approved academic institution. Penetration testing is one technique to help assess security vulnerabilities.

GSE (GIAC Security Expert) – a very rigorous two part exam administered by GIAC (Global Information Assurance Certification), an entity that specializes in technical and practical certification. Part 1 of the GSE is a multiple choice exam. Part 2 is a 2-day lab exam consisting of hands-on exercises.

EnCE (EnCase Certified Examiner) – a digital forensics certification administered by Guidance Software. Forensic examinations are used to attempt to determine what data may have been compromised and how the breach may have occurred. Other forensic certifications such as the **CCE (Certified Computer Examiner)** and the **GCFE (GIAC Certified Forensic Examiner)** are also commonly seen in the cybersecurity world.

There are certainly other reputable security certifications, but these are some of the ones we see most often and they are highly respected within the industry.

People Skills

You want someone you can understand. You want someone who doesn't "speak from high" making you feel like an idiot. You want someone who will work well with senior partners as easily as staff, and who will make friends with your IT support staff.

A telephone call to interview an expert is a good thing. Better yet, see if they will agree to an initial meeting. Most companies are happy to offer a free consultation for an hour or so. We wouldn't hire anyone who wasn't willing to do that. And don't let them send a sales person. You don't need charm and snake oil from someone who doesn't understand security. You want one of their experts who would actually be working with you. In the course of an hour, you'll probably have a good sense of whether this is someone you'll be comfortable working with and whether they are a good match in all other respects as well. It is worth the time – in part because cybersecurity isn't cheap and this is a bad place to make a mistake.

Does location matter?

Location doesn't matter a whit to larger law firms because they can afford travel expenses associated with a remote expert. With respect to smaller firms, the answer is more variable. Without going into granular detail, your expert is not going to need to spend a lot of time on your site. What the expert needs to do onsite is to perform such tasks as assessment of physical devices and equipment, collect logs and configuration files, review physical security, connect test equipment to the internal network, etc. This will generally only take a day. Almost any size firm can afford the travel expenses associated with an expert within driving range. Someone who has to fly in will add that cost plus reasonable meals and a night's hotel stay in most cases.

Solos and very small firms will prefer someone more local for cost reasons. However, if you have really found an expert you trust and you have the monies to engage them, we think the modest expenses involved with a one-day visit are well worth it. Of course, you should also consider whether you will want the expert back to discuss the final report and its recommendations – some laws firm do, but others are satisfied with a video conference. It truly is amazing how technology has made selecting remote experts far less costly as the vast majority of the work can be done remotely.

Costs

There is not a lot of transparency in information security pricing yet, something we hope will change over time. But you can force the hands of companies. If they don't have flat fee pricing based on number of users (or devices), tell them that you will only sign a contract with a company that offers flat fee pricing or certainly a not-to-exceed amount.

Be sure you define the scope of work correctly. But if you are reacting to a data breach, this advice goes out the window. You'll have to trust someone because the expert has no idea what he/she is walking into after a data breach (see the paragraph on recommendations above). You should have a digital forensics expert (these are often cybersecurity experts as well) in mind in the event of a breach. Better to be proactive because you'll be in full-blown panic mode if there's a breach.

But let's assume you are trying to secure your crown jewels (your confidential data) with no breach in play. Now you are looking for a security assessment – and then remediation. We see folks all the time

who want them both in one contract but that's not possible. Experts have to do an assessment before they know what needs to be remediated.

Understand, if you are comparing companies, what is in the scope. They should not be looking at servers only, but at all mobile devices. Is an assessment of physical security included? What about the review of security policies? Are the objectives to be met clearly stated in the scope of work?

So . . . you get a flat fee for the assessment. From smaller companies, this will not be a massive outlay. And of course you may get several flat fee quotes (but do remember that it is indeed often true that you get what you pay for). We think your gut feel after your meeting with the expert may guide you on how significant the monetary difference is. You have that Goldilocks "just right" feeling when you meet the right expert.

Once you get your assessment report back, it will normally come with recommendations – and any smart company is going to offer a proposal with pricing as well. This is where sticker shock may come in. Here's how to help yourself a bit. Make sure the report identifies, in order, critical vulnerabilities, serious vulnerabilities, and low to moderate vulnerabilities. Have the price listed for each remediation action to be taken (including equipment and labor). This will allow you to address the most serious problems first, as your budget allows – but if you've got truly major problems, you may consider dipping into a line of credit. Hopefully you won't find yourself in that situation, but there are firms who hover on the edge of disaster without ready funds to cure their problems.

And you know what? Once you have the report and that company's pricing, if you think it's way off base, take it to another cybersecurity company. If you did not choose wisely in the first instance, another company may find the recommendations or the prices to be out of line. Needless to say, you have to be careful of companies who simply want to bash someone else's work and then lowball their own pricing to get in the door. Even if company #2 gives you a good flat fee quote, be wary of the tone taken to someone else's work – is it respectful? Also, be watchful for signs that the level of protection is being lowered as a tradeoff for lower costs.

Final Thoughts

Go get those recommendations from friends. Have we said this already? Nonetheless, it bears repeating. If your friends have had a really good experience with a company, the chances are that they won't steer you wrong.

The kicker is that you'll have to go this process more than once. In April of 2016, *Legal TechNews* had a headline that read "Through Human and Conventional Openings, Successful Breaches Happening at Dizzying Speeds." That headline was spot on.

The means of attacking law firms morph from day to day, as do the defenses to such attacks. You can never set up your cybersecurity, think you're done and walk away. There is no "set it and forget it" in fast moving field. As a cost of running a law firm, cybersecurity is here to stay.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com

Law Firm Data Breaches: The Cone of Silence Shatters

By Sharon D. Nelson, Esq. and John W. Simek
© 2016 Sensei Enterprises, Inc.

For years, the authors (and many others) have been saying that law firms generally keep mum about data breaches. While we have seen a few small firms abide by data breach notification laws, the larger firms generally have not, usually hanging their hat on the "we don't know what data was compromised" or the "we had an incident, but no evidence of an actual breach or misuse of data" excuses. In fairness, not all data breach notification laws are equal – in some cases, they may not have to disclose Whether they have told their clients is unknown, but speculation has been rising that they often have not, for fear of a mass client exodus.

Two Am Law 100 Firm's Breaches Announced

The "Cone of Silence" around law firm data breaches began to shatter on March 29, 2016, when the *Wall Street Journal* reported that Cravath Swaine and Weil Gotshal, two members of the Am Law 100, were breached in the summer of 2015. Other firms, not named, were reportedly breached as well.

The Manhattan U.S. attorney's office and the FBI are probing the breaches. It isn't clear what information may have been compromised. The information in the article came from "people familiar with the matter." Because the story came from the *Wall Street Journal*, we are quite confident that they verified the information.

Cravath acknowledged that there was a "limited breach" but said that the firm is "not aware that any of the information that may have been accessed has been used improperly." The firm said it was working with law enforcement and outside consultants to assess its security. A spokeswoman for Weil Gotshal declined to comment.

Declining to comment is not a security strategy but it sure has been used as one in the legal world, where breaches are off the record, on the QT and very hush-hush. We bore witness to this when we were once invited, as digital forensics experts, to a very elite meeting of law firm CIOs who didn't mind admitting breaches amongst themselves, but we were sworn to silence, even forbidden to mention the firms represented in the meeting.

Russian Cybercriminal Targets Major Law Firms, Seeks Hacker Partner

March 29th was a tough day in the legal world. Not only did the *Wall Street Journal* publish its article on the breach of two Am Law 100 firms, but *Crain's Chicago Business* reported that a Russian cybercriminal called "Oleras," living in the Ukraine, had been trying since January 2016 to hire hackers to break into the computer networks of nearly 50 elite law firms (almost all U.S. firms) so he could trade on insider information. The source of the story was a February 3rd alert from Flashpoint, a New York threat intelligence firm.

Oleras posted on a cybercriminal forum that he planned, once the law firms were compromised, to use keywords to locate drafts of merger agreements, letters of intent, confidentiality agreements and share

purchase agreements. His list of targeted law firms included names, e-mail addresses and social media accounts for specific law firm employees.

Oleras hoped to hire a black-hat hacker to handle the technical part of breaking into the law firms, offering to pay $100,000, plus another 45,000 rubles (about $564). He offered to split the proceeds of any insider trading 50-50 after the first $1,000,000. Sporting of him.

On February 22nd, another Flashpoint alert said that Oleras had singled out eight lawyers from top firms for a sophisticated phishing attack. The phishing e-mail appeared to come from an assistant at trade journal *Business Worldwide* and asked to profile the lawyer for excellence in mergers and acquisitions.

The firms targeted reads like an entry from Who's Who Among Law Firms. Targets included Akin Gump, Allen & Overy, Baker & Hostetler, Baker Botts, Cadwalader Wickersham & Taft, Cleary Gottlieb, Covington & Burling, Cravath Swaine (which we now know suffered a breach last summer), Davis Polk, Debevoise & Plimpton, Dechert, DLA Piper, Ellenoff Grossman, Freshfields Bruckhaus, Fried Frank, Gibson Dunn, Goodwin Procter, Hogan Lovells, Hughes Hubbard, Jenner & Block, Jones Day, Kaye Scholer, Kirkland & Ellis, Kramer Levin, Latham & Watkins, McDermott Will & Emery, Milbank Tweed, Morgan Lewis, Morrison & Foerster, Nixon Peabody, Paul Hastings, Paul Weiss, Pillsbury Winthrop, Proskauer Rose, Ropes & Gray, Schulte Roth, Seward & Kissel, Shearman & Sterling, Sidley Austin, Simpson Thacher, Skadden Arps, Sullivan & Cromwell, Vinson & Elkins, Wachtell Lipton, Weil Gotshal (which also suffered a breach last summer), White & Case and Wilkie Farr.

Why list the firms? First, because smaller firms express skepticism about threats to law firms in general. This is a wake-up call. Second, because there is no secret about which firms hold M&A data that could allow insider trading – two had already been breached and who knows how many more? If we were a client of any of the firms listed above, we would be asking some hard questions about possible previous data breaches and data security – and no doubt some of their clients are doing exactly that.

A Class Action Suit Against Law Firms Failing to Report Breaches?

Inflaming the consternation, *Law360* reported on March 31st that privacy class action law firm Edelson PC was planning to file class action legal malpractice litigation against major law firms over the exposure of confidential information. Jay Edelson, the firm's founder, says the firm began investigating a class action against as-of-yet unnamed law firms over client data breaches nearly a year before the article was published.

Edelson said, "We've heard story after story from our friends on the defense side – it's a worst-kept secret that there are data breaches all the time at law firms, and there are a ton of state laws which require notification of data breaches, and the law firms seem to not care about those laws."

Our own spin is slightly different – we think the firms have weighed the risks and determined that the risk of non-compliance with state data breach laws (and why oh why isn't there a federal law?) is small – in Virginia, as an example, your risk is $150,000 per breach – chump change. The greater risk for law firms (we are sure) is the horrifying thought of major clients beating a path to the exit door.

On May 6th, The Global Legal Post revealed that Edelson had already filed a privacy class action suit against a Chicago law firm under seal (because the breach was not then resolved) and is now asking the court to unseal the complaint.

Edelson also said that as his firm plans a class action, he anticipates state attorneys general and even the Federal Trade Commission may start to investigate law firm cybersecurity reporting practices. Probably true – and that sidebar note no doubt added fuel to the raging fire.

The Panama Papers: The World's Largest Law Firm Data Breach

Enter the jaw-dropping revelations in early April from what has become known as the Panama Papers. The Panamanian law firm that was breached was Mossack Fonseca, which provides services including incorporating companies in offshore jurisdictions such as the British Virgin Islands. It is the fourth largest provider of offshore services. 2.6 terabytes of data – some 11 million files – were exposed, along with the sort of offshore hiding of monies that has become the stuff of legend in the last few decades. The documents span an almost 40-year period from 1977 when the law firm was formed.

An anonymous source passed the data to the German newspaper *Suddeutsche Zeitung*, which has shared them with the International Consortium of Investigative Journalists (ICIJ). The Consortium has assisted in analyzing the files for over a year. The *BBC* says the documents show how the law firm helped clients launder money, dodge sanctions and evade taxes.

Iceland's Prime Minister resigned, the first prominent political fallout from the leaks. But the firm itself is coming under scrutiny, the *BBC* reporting that it worked with 33 individuals or companies who have been placed under sanctions by the U.S. Treasury, in some cases continuing the representation after the sanctions were in place.

Vladimir Putin was apparently involved with $2 billion in offshore accounts. A member of FIFA's Ethics Committee (that has GOT to be a misnomer) was exposed. Others included drug dealers, arms traders, human traffickers and fraudsters.

Round two of the Panama Papers was released in searchable format on May 9th.

While the ICIJ did not include a "data dump" of the original documents or the large-scale release of personal data, it proclaimed the dump likely to be "the largest ever release of secret offshore companies and the people behind them."

You can search the Panama Papers by name or country at https://offshoreleaks.icij.org/ – more than 200,000 entries are included including some of the world's most venerable law firms. Named in the Panama Papers are:

- Akin Gump Strauss Hauer & Feld in New York
- Arnold & Porter, via legacy firm Howard Rice Nemerovski Canady Falk & Rabkin in San Francisco
- Ashurst, via legacy firm Blake Dawson Waldron in London and Sydney
- Baker & McKenzie in Bangkok, Hong Kong, Singapore, Stockholm, Taipei and Zurich
- Bryan Cave in New York and St. Louis
- Coudert Brothers, now defunct, in Denver, Los Angeles, New York and Singapore
- Dentons, via legacy firms Denton Wilde Sapte in Gibraltar and Salans Hertzfeld & Heeilbroun in Paris
- DLA Piper in Hong Kong and Singapore
- Dorsey & Whitney in Hong Kong
- Freshfields Bruckhaus Deringer in Singapore
- Greenberg Traurig in Miami and New York
- Hogan Lovells, via legacy firm Hogan & Hartson in Moscow
- Hughes Hubbard & Reed in Miami
- Jones Day in Hong Kong and Tokyo
- K&L Gates in Hong Kong
- Kaye Scholer in Los Angeles
- Katten Muchin Rosenman in Chicago
- King & Wood Mallesons, via legacy firms Arculli Fong & Ng in Hong Kong and Mallesons Stephen Jaques in Hong Kong
- Kramer Levin Naftalis & Frankel in New York
- Linklaters in Hong Kong
- Morgan, Lewis & Bockius in Singapore

- Norton Rose Fulbright, via legacy firms Fulbright & Jaworski in Hong Kong and Macleod Dixon in Calgary
- Orrick, Herrington & Sutcliffe in Singapore
- Perkins Coie in Taipei
- Schiff Hardin in New York
- Snell & Wilmer in Costa Mesa, California
- Squire Patton Boggs, via legacy firms Deacons Graham & James in Kowloon/Hong Kong and Squire, Sanders & Dempsey in Hong Kong and Los Angeles
- Troutman Sanders in Hong Kong
- White & Case in Los Angeles and Singapore
- Wilmer Cutler Pickering Hale and Dorr, via legacy firm Wilmer, Cutler & Pickering in Washington, D.

The ICIJ noted in a disclaimer that there are "legitimate uses for offshore companies and trusts" and that it does not "intend to suggest or imply that any persons, companies or other entities have broken the law or otherwise acted improperly." We reiterate that disclaimer!

How Did Mossack Fonseca Get Hacked?

While Mossack Fonseca blamed "an e-mail server attack," no one really believed it. It certainly appears that the firm had no intrusion detection or data loss prevention systems in place or it would have known about the breach. If true, that in itself is a disgrace given their clientele and the kind of work the firm was doing.

As others began to investigate, *The Register* reported that a SQL vulnerability (allowing database commands and values to pass to an application without any validation) was found at the firm. *Naked Security* reported that, aside from the e-mail server hack which the firm acknowledged, the company's WordPress website included a buggy plug-in and that the firm's customer portal was running a long-outdated version of Drupal. Some experts still believe insiders were involved but the firm denies it and we have as yet seen no proof of it.

The New York Times revealed on April 13th that the government had raided the offices of Mossack Fonseca, accompanied by financial analysts and digital forensics experts, looking for evidence of illegal activities, including assisting clients in laundering money and avoiding taxes.

More firms have been named in connection with the Panama Papers, including JP Damiani & Associates (Switzerland), Child & Child (UK), Junod Muhlsteing (Switzerland) and Krinzman Huss (US). This should not be construed as an accusation of illegal activities by those firms. The dust hasn't settled on that either.

The New Yorker observed that other countries tended to use the services of Mossack Fonseca more than U.S. entitles; however, of the fourteen thousand intermediaries—banks, law firms, company-incorporation firms, and other middlemen—with which Mossack Fonseca worked over the years in order to set up companies, foundations, and trusts for its customers, six hundred and seventeen were based in the United States. Most of these are now identifiable from the searchable database.

The FBI Sends Cybersecurity Alerts via the ABA

On April 12th, many ABA members were surprised to find an e-mail from ABA President Paulette Brown in their Inbox. She was advising them that the FBI had requested the ABA to share FBI Private Industry Notification cybersecurity alerts with the legal community. It no doubt startled a lot of lawyers that the FBI was so specifically worried about the vulnerabilities in the legal industry that it would seek the cooperation of its largest association in getting the word out about threats and defenses.

It has taken law firms a very long time to wake up to the depth and breadth of the threats to their data. The FBI issued its first alert to law firms in 2009, advising them they were being targeted because of the nature of the data they hold on behalf of so many clients and because their security is weaker than that of their clients. A number of such alerts from the FBI have been distributed via the ABA.

More on Law Firm Data Breaches

InfoRisk Today cited yet again on April 7th the reason why law firms are such attractive targets for hackers. Remember the bank robber Willie Sutton? When asked why he robbed banks, he replied, "Because that's where the money is." Likewise, for hackers, law firm networks are where client secrets exist – and that too is where the money is. The post cites the fact that cybersecurity firm Mandiant (now a division of FireEye) estimated that 80 law firms were hacked in 2011 alone.

Bloomberg reported in February of 2016 that Fox Rothchild, Holland & Knight, Hunton & Williams, Simpson, Thacher & Bartlett, Thompson Hine and Wilson Sonsini were all victims of trading schemes that involved employees attempting to compromise and profit from client data. Insiders or outsiders, the myth of law firms carefully guarding client data is vaporizing.

Where Law Firms Should Go From Here

This is going to be a "drip, drip, drip: story as journalists and government authorities seek to connect the dots. As NBC News has already reported, the IRS has warned Americans named in the Panama Papers to come clean before it fully analyzes the Panama Papers. The Treasury Department estimated last year that more than $300 billion dollars of illicit proceeds are generated in the United States annually, with criminals using such companies here and abroad to launder funds. It also intends to issue a long-delayed rule forcing banks to seek the identities of people behind shell-company account holders.

Meanwhile, NBC news reports that federal agents and prosecutors are "chomping at the bit" to exploit the Panama Papers and launch prosecutions according to a senior federal law enforcement official.

You may recall that *60 Minutes* did a segment recently exposing how helpful U.S. lawyers might be in concealing questionable funds. The results were dismal, with only one lawyer flatly refusing to have any part of concealing such funds. Our guess is that the breach of Mossack Fonseca will lead to investigations of involvement in illegal activities by a number of American companies, including law firms. The data leaker here appears to have been a "moral" leaker who wanted to disclose wrongdoing.

As law firm breaches proliferate, more and more will be known about the unethical or illegal conduct of some lawyers/law firms. State-sponsored hackers from China, Russia, North Korea, etc. may well reveal such information for reasons of their own. For those U.S. firms that may have been involved in questionable activities, it is time to clean house – or to take proactive steps to make sure that the house stays clean. In a breach driven and almost entirely digital world, there really is no place to run and no place to hide if you are caught engaging in unethical or illegal activities.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Recent Egregious Data Breaches: How They Happened

by Sharon D. Nelson and John W. Simek

© 2016 Sensei Enterprises

We should be grateful for other peoples' data breaches – they help us to improve our own security. In our breach-a-day world, we seem to have more data breaches than ever. They come fast and furious – rare is the day when we don't hear of one or more breaches on the evening news or through online media. Attack vectors change constantly – those of us in information security have a deep sense of humility in the face of constant changes in threats as well as technology, policies and training to defend against those threats.

Herewith, a few of the famous data breaches of 2015 (and one from 2014) with lessons to be learned from how they happened.

Office of Personnel Management

This was probably the most controversial breach of 2015. In May, the federal Office of Personnel Management (OPM) reported a breach affecting 4.2 million current and former federal employees. A few days later, it revealed a second breach (lesson here: don't speak too quickly about data breach specifics). The second breach brought the number impacted to 22 million people who had applied for government jobs or security clearances. Data from some applicants' family members was also compromised. The data taken included names, addresses, names of relatives, employment histories and health care histories. There was a lot of talk about the fact that 5.6 million digital fingerprints were compromised, giving rise to concern about the security of biometrics. Members of law enforcement, the intelligence community and the federal court system were all impacted. Some of the data included information on peoples' sex lives, drug and alcohol problems and debts, all of which could be used for blackmail.

The press confirmed through multiple sources that the government had concluded that China was behind the hack. But it declined to overtly accuse China because revealing technical details of how they attributed the breach to China would tip off hackers to the ways that American intelligence agencies track them.

Computer security firm CrowdStrike, which has close ties to U.S. law enforcement, said it had traced the breach to hackers it said were "affiliated with the Chinese government," using forensic information from the hack provided by the government. The Director of OPM resigned.

The breach went undetected for 343 days – it was ultimately discovered when anomalous SSL traffic and a decryption tool were observed within the network.

Though the U.S. has not talked publicly about how the breach happened, U.S. Department of Homeland Security official Andy Ozment testified that the attackers had gained valid user credentials to the systems they were attacking, likely through social engineering.

VTech Holdiings

This Hong Kong digital company was the victim of one of the year's biggest hacks in November when its Learning Lodge database was compromised, permitting hackers to get adults' profile information, e-mail addresses, passwords, chat logs and audio files - and the names, home addresses, first names and

birthdates of millions of children and their photographs. Some of the audio recordings were of children's voices from VTech's Kid Connect, a service that allows parents and kids to chat via a mobile phone app and a VTech tablet. The release of the information of children was particularly disturbing and garnered a lot of publicity.

So how did the information of over 6 million people get exposed? According to security researchers, the hacker used a SQL injection to gain root access to VTech's web and database servers. Users' passwords weren't properly scrambled and hashed. The MD5 algorithm that VTech used had been known to be vulnerable for a decade or more. Worse yet, the company stored customers' security questions and answers in plain text, a clear security no-no. The reported hacker said that the entire purpose of the hack was to expose the security flaws and said he would not use or publish the data.

Besides mishandling the data from a security perspective, one wonders why the company needed to store this much data to fulfill its business purposes. It is a common problem – storing data one does not need, which itself creates a potential vulnerability.

Anthem

In February, heath insurer Anthem said that hackers had accessed its servers and downloaded the personal data of employees and those who were insured by Anthem. Even those who were not Anthem customers may have been impacted because Anthem handles paperwork for smaller insurers. Data stolen included names, addresses, birthdates, Social Security numbers, and employment information, including salaries. 79 million records were compromised and dumped online – this was the largest data breach of 2015.

This breach occurred because the hackers had gained access to the login credentials of employees with system access. How? Reportedly, the credentials were obtained through a watering hole attack. A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

In this case the attackers created a bogus domain name "we11point.com" (based on Wellpoint, the former name of Anthem). In this cases, the hackers set up subdomains which were designed to mimic real services such as human resources, a VPN and Citrix server. By then sending phishing e-mails, users may have been lured to infected websites and entered their log-in credentials. A number of security companies believe the hack came from Deep Panda, a Chinese-based hacking group.

The breach was undetected for nine months and was discovered when a systems administrator noticed that a legitimate account was querying internal databases but without the legitimate user's knowledge.

There are similarities between this attack and the breach of Premera Blue Cross in 2015, impacting 11 million people – are they related? Impossible to say, but another bogus domain name "prennera.com" was discovered in the Anthem investigation.

Pentagon

In July, alleged Russian hackers hacked an unclassified e-mail server of the Pentagon. U.S. officials announced that Russia had launched a "sophisticated cyberattack" against the Pentagon's Joint Staff unclassified e-mail system. The officials added that the cyber-attack compromised data belonging to 4,000 military and civilian personnel who worked for the Joint Chiefs of Staff.

As the attack was later described a “spear phishing attack”, it doesn’t on the face of it sound all that sophisticated. However, Department of Defense officials continued to call it the "most sophisticated" cyberbreach in U.S. military history. Officials spent 10 days scrubbing the system and creating mock hacking scenarios before giving military personnel access to it again. The spear phishing attack targeted the personal information of scores of users. What may have made this attack sophisticated is that the hackers used “an automated system rapidly gathered massive amounts of data and within a minutes distributed all the information to thousands of accounts on the Internet.” Encrypted social media accounts were used to coordinate the attack. If true, that might qualify this attack for the adjective “sophisticated.”

Ashley Madison

The Ashley Madison dating site breach impacted 37 million people and gave high-value entertainment fodder to pundits everywhere. This was an unusual hack, in that it seemed to be rooted in the moral convictions of the hackers, called The Impact Team. They wanted the site, whose tagline is “Life is short. Have an affair,” to take the site down. They also wanted Avid Life Media’s “EstablishedMen.com” site taken down. When the site’s owner refused to take the sites down, the data was made public in spurts.

The breach was reported in July, and data compromised included e-mails, names, home addresses, sexual fantasies and credit card information. All of the user data released on August 18, 2015. More data (including some of the CEO's emails) was released on August 20, 2015. The release included data from customers who had earlier paid a $19 fee to Ashley Madison to allegedly have their data deleted. It turned out to be a boon to divorce lawyers everywhere. No doubt many members were shocked to find out that most of the women on the site were “bots” – employees who pretended an interest in an affair as part of inducing additional payments to Ashley Madison – and of course users had no clue that they had agreed to the use of bots when they accepted the terms of service.

The data was made vulnerable by a bad MD5 hash implementation. We are not sure how the hack actually happened but The Impact Team itself said this: “Nobody was watching. No security. Only thing was segmented network. You could use Pass1234 from the internet to VPN to root on all servers.”

In an interesting side note, as of January 1, 2016 Ashley Madison’s membership has supposedly increased by more than 4 million since the breach. Go figure.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com, snelson@senseient.com; jsimek@senseient.com.

Clients Demand Law Firm Cyberaudits

by Sharon D. Nelson, Esq. and John W. Simek

© 2016 Sensei Enterprises, Inc.

Bank of America Merrill Lynch Audits Law Firm Cybersecurity

Three years ago, there was a collective gasp heard ‘round the country the day the press reported that Bank of America Merrill Lynch was auditing the cybersecurity policies at its outside law firms, partly under pressure from government regulators.

Assistant General Counsel Richard Borden stated that Bank of America is "one of the largest targets in the world" for cyberattacks, and that law firms are "considered one of the biggest vectors that the hackers, or others, are going to go at to try to get to our information."

Regulators at the Office of the Comptroller of the Currency, which oversees BofA and other financial services companies, "have focused on law firms," according to Borden. "They are coming down on us about security at law firms. So we have no choice but to check the information security and to audit — to actually audit — the information security of our law firms that have confidential information. We spend a lot of money and use a lot of law firms, so this is casting a very wide net."

Amid much hand-wringing, the prophecy that law firms would be forced to confront their data security shortcomings has finally come true. Clients now want, as do regulators, assurance that law firm data is being adequately protected. The receipt of information security audits, more politely termed “assessments”, is now a regular occurrence at many law firms. They come not only from clients, but from insurance companies offering cyber insurance – but they want to know what they are getting into first!

Pay Now or Pay Later

Though law firms are not thrilled about lifting their data security skirts for inspection, this move was inevitable. For way too long, most law firms have paid

scant attention to information security. We are hoarse from explaining that it is a "pay now or pay later" proposition – either law firms get serious about guarding their client data and spend the monies to do so – or they will pay later when a data breach causes them to require the services of digital forensics experts to investigate the breach and an outside lawyer to advise them of their legal responsibilities. They will also incur the costs of remediating the vulnerabilities and the costs associated with complying with state data breach notification laws (currently, 47 states have such laws).

The big firms have gotten the word. Previously, some clients have wanted to see law firm security policies. Some have allowed law firms to effectively audit themselves. Today, clients want to see if security policies and plans are actually being followed. And they want independent third party audits, sometimes including penetration testing.

As clients have woken up to the potential vulnerabilities of law firms, they are demanding much, much more in the way of security – it is clear that clients are leaving firms which don't meet their security expectations. Hence the fairly sudden desire to get secure. In the AmLaw 200 in 2015, firms were reported to be spending an average of 1.9% of gross revenues on cybersecurity – and that can amount to as much as $7 million a year. That is an extraordinary change, to say the least.

A Small Question of Ethics

This whole topic is hot, hot, hot – and it shows on the lecture circuit. Colleague Dave Ries sent a hypothetical currently being used for discussion in a CLE. The bulk of it was developed by the General Counsel of Buchanan Ingersoll & Rooney. It goes like this:

Prior to being hired as counsel for GRU [Genetics-R-Us], DCH [Dewey, Cheatham & Howe] must meet certain GRU security requirements. GRU has stringent security requirements for its service providers, including law firms. Lawyer 1 and Lawyer 2 are meeting with DCH's Technology Director to discuss GRU's security requirements and a questionnaire about security that GRU has asked the law firm to complete. Tech Director says that the firm meets most of the requirements, but not all of them. It will take weeks, or perhaps months, to comply with all of them. Lawyer 2 tells him "we have to tell the truth, but put our best foot forward and

stretch things a little if you have to. I'd hate to lose this work because you haven't done your job. Just fill it out so we pass and sent it back to GHR. It's all tech stuff, so Lawyer 1 and I don't need to review it."

So what happened to the duty to supervise? Is the lawyer implicitly sanctioning deceit? Can you be competent under the new rules of professionalism when you say "it's all tech stuff" as though you had no need to investigate and understand it? This has all the makings of an ethical disaster.

Today, when we lecture on encryption, we have standing room only audiences. The people who come to our live sessions radiate a hunger for cybersecurity knowledge. They are genuinely scared – and perhaps more so because of the new versions of the ABA Rules of Professional Conduct 1.1 (Competence) and 1.6 (Confidentiality of Information), which together require competent and reasonable measures to safeguard information relating to clients. As we go to press, Virginia has just become the 18th state to adopt the changes to those rules – and it is clear that more states will be following suit soon.

How Do You Survive a Cyberaudit?

1. Be prepared for everything (including telling the truth).
2. Review your ethical responsibilities (better now than when you are before a Disciplinary Board).
3. Make sure you have a diagram showing where all your data is.
4. Be especially careful about third parties holding your data – you may need to audit them! At the very least, you need to understand their security precautions and procedures.
5. Do an annual review of all policies and plans which impact data security and update them as needed. These may include but not be limited to:
    - Business continuity plan
    - Disaster recovery plan
    - Incident response plan
    - Remote access policy
    - Employee termination policy
    - Password policy

- Encryption policy
- Data access policy (including access by guests/vendors/clients)
- Physical security plan
- BYOD/BYON policy

6. At least once a year, get a full-blown security assessment by an independent third party security company (if you are a smaller firm, use a smaller security firm – the prices are much less). Remember that these firms are in the business of making assessments – their own credibility is on the line, so their assessments carry more weight. As a bonus, you may get a discount from your insurer on your premiums.
7. Consider whether you need penetration testing – actual attempts by experts to breach your network. Penetration testing can include network attacks and/or physically attempting to penetrate your facility to access the computing infrastructure. This may be overkill for a small firm, but certainly not for a large firm.
8. Be prepared – make sure you have cyberinsurance that will protect you fully in the event of a data breach – most policies will not and require a specific rider.
9. Stop kowtowing to the demands of lawyers that they want to BYOD (bring their own device) or BYON (bring your own network). This is serious stuff, not a parlor game where willful children should rule.
10. Our advice? And yes, we're serious – law firm business should only be conducted on devices issued by the law firm – and no personal business should be allowed on those devices. Not many firms will have the gumption to do this (see the willful children remark above) but this will be a key measure valued by clients and regulators.
11. Encryption is not complicated. Make sure lawyers use it where needed!
12. If a cloud provider has a master decrypt key, encrypt before depositing any sensitive data there (e.g. Dropbox).
13. Install hardware and software that does realtime intrusion detection – if you are a smaller firm that can't afford this, make sure you enable logging so there will be a trail to follow.

14. Twice a year, have mandatory security training to keep employees advised of new security threats and to underscore the need for vigilance, including being watchful for suspicious e-mails, texts, hyperlinks etc. as well as social engineering ploys.
15. Document all your security measures so you can produce it as part of an audit.
16. Even if you are allowed to self-audit, don't. The human tendency is to cut corners or say "I think so" which translates to "yes" in the audit when you are not really sure "yes" is the full or correct answer.
17. If you're big enough, have an audit committee with players from IT, Compliance, Management, and Security. They will all have a part to play and it is important to get buy-in across the board.

It is impossible in a short article to describe all of the steps a law firm should take when confronted by an audit – they will likely be spelled out for you by your clients. With a little help from Google, search for "security audits checklist" and you'll find plenty of reference material.

Final thoughts

The time to get started on all this is yesterday. And we predict with a fair amount of confidence that many law firms will sashay into the future as vulnerable as ever unless clients force them to take security seriously.

We have all but throttled audiences in our passion to get them to understand how real the problem of data security is but in the end, perhaps Matt Hooper said it best when he prophesied in the original *Jaws* movie.

"I'm familiar with the fact that you are going to ignore this particular problem until it swims up and bites you in the ass!"

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Excerpts from Locked Down: Practical Information Security For Lawyers

by Sharon D. Nelson, Esq. David G. Ries and John Simek
ABA, 2016
available from the ABA Web Store:
http://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=238368703

Security Certifications and Security Audits

In 2015, *The American Lawyer* reported that 18 large law firms in the U.S. had received the ISO 27001 certification. This certification has become a way of assuring clients that law firms are indeed protecting their clients' data. The yearly audits to maintain the certification offer clients a lot of comfort and offer law firms the continuing opportunity to assess and respond to new risks.

We certainly predict that the number of law firms seeking that certification will grow – and that other certifications may be sought. You will likely see statements made that the law firm is compliant with some of the security standards referenced earlier in this book. Likewise, some clients are somewhat skeptical of law firms doing their own audits, even on the forms provided them by clients. There is a deeply human tendency to give the clients the answer they want. More and more frequently, clients are likely to be demanding an independent third party audit – or even sending in their own elite team of information security experts to make an assessment.

The bottom line is that clients who are unsatisfied with their law firm's security are going to require changes or take their business elsewhere. Some law firms are trying to get out ahead of the demands and ramping up their security so they can point to it and use it as marketing leverage.

Policies and Plans

Expect more policies and plans as more security incidents take place in law firms. There is a great interest by clients in seeing a law firm's Incident Response Plan. Insurance companies want to see it as well – and information security policies generally. While all the large firms are likely to have Incident Response Plans, they are fairly rare in solo and small firms. As the authors have seen these firms

become more and more interested in securing their data, their interest in policies and plans is bound to increase as well.

Clients are asking for stricter policies to be put into place, and that will likely continue. They may ask that no sensitive data be placed on a flash drive, or that only "clean devices" be taken to countries where state-sponsored hacking is common. They may forbid any linkage between a law firm's network and networks in another country, although there is the practical element since the majority of networks are connected to the Internet. All sorts of demands by clients are being made – and we predict that the initial trickle of demands will increase to a river. You may recall that, in 2012, information security company Mandiant (a division of FireEye) put out a report estimating that 80% of the 100 largest American law firms had experienced some form of a data breach in 2011 – is it any wonder that clients are so demanding in light of estimated numbers like those? We look for far tighter information security controls to be employed by law firms in response to client concerns.

Passwords and Multifactor Authentication

Passwords aren't dead yet and probably won't be for the foreseeable future. But they have to die ultimately because they offer such scant protection. The move to multifactor authentication is clearly mandated by its far greater ability to secure data. Solos and small firm lawyers may not move that way as fast, but clients are demanding tighter and tighter protection for their data and multifactor authentication is one robust and obvious solution.

Encryption

This train left the station very fast in 2015 as the word spread that clients were demanding encryption – and as products emerged that were very simple to use and don't cost a lot of money either. No math skills required and you don't have to understand encryption. You just have to point and click an "Encrypt and Send" button – or something similar. The most Luddite of American lawyers are beginning to understand this and we anticipate a widespread adoption of encryption everywhere before we "set pen to paper" for the next edition.

Social Media

The social media chapter of this book is brand new with this edition. Social media is now a mainstream form of communication for most people – and they spend a

lot of time on social media. We expect to see more attack vectors using social media as a weapon for hackers. They are practicing what every fishing boat captains knows – they are fishing where the fish are. We expect our Social Media chapter to be very volatile in the next edition of this book.

Mobility

We expect an even greater increase of mobile access. Wireless connections are all the rage and we move towards an increased usage of tablets, smartphones and wearable technology. More and more of the younger generation will impose pressure for BYOD (Bring Your Own Device), BYON (Bring Your Own Network) and BYOC (Bring Your Own Cloud). The access to any data from any place using any device will create new challenges for information security. Detection tools will be needed to identify when a device is connected to the firm network. You can't protect it if you don't know it exists.

File-Syncing Software – Dropbox and its Brethren

Though there are many kinds of file syncing software, lawyers have glommed on to Dropbox in droves. The Washington Post reported that 33% of its users in Washington D.C. were sharing files. We are hearing repeatedly of e-discovery productions being made via Dropbox and similar services. We expect to see breaches via services like Dropbox – some users misunderstanding how to use these kinds of services securely and some keeping data (like those e-discovery productions) around as "dark data" that they don't remember they have which may be hacked, inadvertently shared, etc.

Policies and Plans

Expect more policies and plans as more security incidents take place in law firms. There is a great interest by clients in seeing a law firm's Incident Response Plan. Insurance companies want to see it as well – and information security policies generally. While all the large firms are likely to have Incident Response Plans, they are fairly rare in solo and small firms. As the authors have seen these firms become more and more interested in securing their data, their interest in policies and plans is bound to increase as well.

Clients are asking for stricter policies to be put into place, and that will likely continue. They may ask that no sensitive data be placed on a flash drive, or that only "clean devices" be taken to countries where state-sponsored hacking is

common. They may forbid any linkage between a law firm's network and networks in another country, although there is the practical element since the majority of networks are connected to the Internet. All sorts of demands by clients are being made – and we predict that the initial trickle of demands will increase to a river. You may recall that, in 2012, information security company Mandiant (a division of FireEye) put out a report estimating that 80% of the 100 largest American law firms had experienced some form of a data breach in 2011 – is it any wonder that clients are so demanding in light of estimated numbers like those? We look for far tighter information security controls to be employed by law firms in response to client concerns.

Incident Response Plans

This core of the response function is advanced planning. This means attorneys and law firms need a plan, usually called an Incident Response Plan (IRP), which is often focused on data breaches, but "incidents" can refer to responding to ransomware, fighting attempted hacks, an insider accessing data without authorization or a lost or stolen laptop or mobile device.

Most large firms now have these plans in place, but many smaller firms do not. More and more, clients and insurance companies are asking to review law firms' IRPs. In the face of ever-escalating data breaches, now is a good time to develop and implement a plan or to update an existing one. After all, football teams don't get the playbook on game day!

The problem with all plans is that they may not survive first contact with the enemy. That's OK. Far worse is having no plan at all and reacting in panic with no structure to guide your actions. The first hour that a security consultant or law enforcement spends with a business or law firm after a data breach has been discovered is a very unpleasant time. Kevin Mandia, the founder of Mandiant, a leading security firm, has called it "the upchuck hour." It is not a happy time.

Don't rely on a template IRP. While templates may be a starting point, no two law firms are identical and all have different business processes, network infrastructures and types of data. An IRP must be customized to fit the firm – the

smaller the firm, the shorter the plan is likely to be. For a solo practice, it may just be a series of checklists, with who to call for what. Books and standards have been written about IRPs. They can be reviewed and qualified professionals can be consulted for more details. The following is a condensed and, hopefully, digestible overview.

The Elements of an IRP

- Identify the **internal personnel** responsible for each of the functions listed in the IRP. Identify them by position titles rather than by name, since people come and go. It will require a broad-based team for a firm of any size – management, IT, information security, human resources, compliance, marketing, etc. Have a conference call bridge line identified in case a breach happens at night or on a weekend and include home/cell phone numbers and personal as well as work e-mail addresses. This list will need to be updated regularly as people join or leave the firm.

- Identify the contact information for an experienced **data breach lawyer** – many large firms now have departments that focus on security and data breach response and some smaller firms have a focus on the area. Don't think you can handle this without an attorney who is experienced in data breaches. Your data breach lawyer (if you selected a good one) will be an invaluable quarterback for your IRP team – and he or she may be able to preserve under attorney/client privilege much of the information related to the breach investigation.

- Identify the location of your **insurance policy** (which darn well better cover data breaches). You need to make sure you are covered before you start and list the insurer's contact information because you are going to need to call your insurer as soon as you are aware of a possible breach.

- Identify the contact information for **law enforcement** – perhaps your local FBI office – often the first folks called in.

- Identify the contact information for the **digital forensics consultant** you would want to investigate and remediate the cause of the breach. Often, a firm has been breached for seven months or more before the breach is discovered – it will take time to unravel what went on.

- Include in the IRP **containment and recovery** from a breach. A law firm that has been breached has an increased risk of a subsequent (or continuing) breach – either because the breach has not been fully contained or because the attacker has discovered vulnerabilities that it can exploit in the future.
- Determine the **data that has been compromised** or potentially compromised. You'll want to know if all data that should have been encrypted was indeed encrypted in transmission and in storage. If it was, this may lessen the notification burden. Identify any PII (Personally Identifiable Information) that may have been compromised.
- Identify and preserve **systems logs** for your information systems. If logging functions are not turned on or logs are not retained, start maintaining them before a breach.
- If you have **intrusion detection or data loss prevention** software, logs from them should be preserved and provided to your investigators immediately. If you don't, you may want to think about implementing such software.
- Identify the contact information for **your bank** in case your banking credentials have been compromised.
- (Optional but often useful) Identify the contact information for a good **public relations firm**. If you are not required to make the breach public, you may not need one, but if it does go public, you may need to do some quick damage control. Your insurance coverage may provide for this, in which case the insurance company will put you in contact with the appropriate firm.
- How will you handle any **contact with clients and third parties**, remembering that you may wish not to "reveal all" (if notice is not required) and yet need to achieve some level of transparency? Be forewarned that this is a difficult balance. You will feel like the victim of a data breach, but your clients will feel as though you have breached their trust in you. A data breach that becomes public can cause a mass exodus of clients so work through your notification planning with great care. Be wary of speaking too fast before facts are fully vetted – this is a common

mistake, trying to limit the damage and actually increasing it as the scope of the breach turns out to be far greater or different than first known.

- How will you handle **informing employees** about the incident? How will you ensure that the law firm speaks with one voice and that employees do not spread information about the breach in person or online? How will your social media cover the breach, if at all?
- If you have a **data breach notification law** in your state (and almost all do), put it right in the plan along with compliance guidelines. You may be required to contact your state Attorney General. These laws vary widely so be familiar with your own state law. Also, determine whether other states' breach notice laws may apply – residences of employees or clients, location of remote offices, etc. Make sure that the relevant data breach regulations are referenced in the plan and attached to it.
- Identify any **impacted data that is covered by other legal obligations** like HIPAA or client contractual requirements and comply with notice requirements.
- Conduct **training on the plan**. Make sure that everyone understands the plan and their role under it.
- **Test the plan**. This can range from a quick walk through of hypothetical incidents to a full tabletop exercise. Include contacts with external resources to make sure that everything is up to date. This will help to make everyone familiar with the plan and to identify areas that should be revised.
- Does the breach require that IT and **information security controls and policies** be updated or changed? Does what you learned from the breach require that the IRP itself be revised? The IRP should mandate at least an annual review even without an incident.

Prepare now! The new mantra in security is that businesses (including law firms) should prepare for <u>when</u> they will suffer a data breach, not for <u>if</u> they may suffer a breach. This requires security programs that include detection, response and recovery, along with identification and protection of data and information assets.

Successful response requires an effective Incident Response Plan. Attorneys who are prepared for a breach are more likely to survive and limit damage. Those who are unprepared are likely to spend more money, lose more time, and suffer more client and public relations problems.

New Developments

The Legal Services Information Sharing and Analysis Organization (LS-ISAO) Services was launched in 2015 with the help of the financial services industry whose 15-year-old Financial Services Information Sharing and Analysis Center (FS-ISAC) is considered one of the most mature ISAC/ISAO groups today.

Applications to become members of the group were sent to about 200 law firms (mostly large firms) - membership is $8000 per year. This is obviously a work in progress, and unlikely to help solo, small and midsize law firms.

ISACs and ISAOs provide an official mechanism for sharing information about the latest cyberattacks and threats spotted targeting specific industries, for instance, and include databases of the threats and vulnerabilities for their members, as well as provide conferences and other ways for members to interact and share their experiences to better collaborate in fighting cybercrime and cyber espionage actors. Among the industries with ISACs and ISAOs are the aviation, the defense industrial base, emergency services, IT, maritime, nuclear energy, real estate, public transportation, retail, and water utilities.

Initially, the LS-ISAO will offer members access to intel-sharing list servers with threat information and advisories from vendors and government agencies as well as member-to-member threat sharing and other resources. Ultimately, it will evolve to offer portal services for members to securely and anonymously share threat intelligence, as well as the Holy Grail of intel-sharing - automating the use of the information into the member's internal security tools and networks.

Just as were writing these materials, the U.S. House and the U.S. Senate approved controversial cybersecurity legislation buried within a $1.1 trillion government spending agreement that was needed to prevent a government shutdown. In fact, apparently all kinds of legislation is buried in that bill. Seems to happen way too often.

The bill passed the House on December 18th with a vote of 316-113, and was quickly approved by the Senate with a 65-33 vote the same day. The Cybersecurity Information Sharing Act (CISA) has been contentious since the beginning of its life . . .

“Chief information officers are not excited about this,” Matthew Green, a cryptographer and professor at Johns Hopkins University told *SCMagazine.com*. “They are saying, we don't want anything to do with this.”

While CISA includes providing liability relief for companies sharing data with government agencies, many multinational corporations are concerned about reputational risk, especially as they try to navigate international issues such as Safe Harbor, which was ruled invalid by the European Commission in October.

“How that is all going to be resolved?” asked Green. “I have no idea, but it is the last thing that tech firms want to deal with right now.”

The act creates a voluntary cybersecurity sharing process allowing the public and private sectors to share information on cyber threats and attacks with the federal Department of Homeland Security without legal liability issues and while protecting private information. Companies would be required to review and remove any personally identifiable information unrelated to cyber threats before sharing information with the government.

Some industry groups, such as banking, have groups for sharing information about online threats, but the bill seeks to increase sharing, especially with government agencies, said David Ries, a member at Clark Hill PLC.

The key, he said, is “striking a balance between information the federal government really needs for a coordinating role and security, and not giving them too much that identifies unnecessary private details or business information.” Many readers will recognize Dave as a frequent source of RTL stories - and our regular co-author.

The bill is “dangerous” for giving intelligence agencies too much authority, and it does not go far enough to address existing problems such as unencrypted files, out-of-date software and user errors, said the Electronic Frontier Foundation, a San Francisco nonprofit that advocates for Internet privacy.

“CISA — and its amendments — do not even begin to address these serious problems,” the foundation said in a statement. “Instead, they mandate information sharing with the intelligence community, creating even more cyberspying.”

Does CISA balance privacy with the need for cybersecurity? We shall see.

What Will You Do When Your Law Firm Is Breached?

by Sharon D. Nelson, Esq. and John W. Simek

© 2016 Sensei Enterprises, Inc.

Note that we did NOT title this article, "What Will You Do If Your Law Firm is Breached?" The reason is simple – experiencing a data breach is not an "if" – it is a "when." Just ask the IRS and the Office of Personnel Management. Mind you, their approach to information security was sloppy. Lawyers cannot afford, ethically, to have slipshod security when protecting confidential data.

Incident Response Plans

We have often written about steps to secure your data but this time we are stressing that it is imperative that you are ready for a data breach. This means you need a plan, which tends to be called an Incident Response Plan (IRP), often focused on data breaches but "incidents" can refer to responding to ransomware, fighting attempted hacks or an insider accessing data without authorization.

Most large firms now have these plans in place, but many smaller firms do not. More and more, we are seeing clients and insurance companies asking to see your Incident Response Plan. In the face of ever-escalating data breaches, now is a good time to come up with a plan. After all, football teams don't get the playbook on game day!

The problem with all plans is that they don't survive first contact with the enemy. That's ok. Far worse is having no plan at all and reacting in panic with no structure to guide your actions. We see that all the time – the first hour you spend with a client after they know they've been breached is often called "the upchuck hour." It is not a happy time.

Don't go in search a template IRP. No two law firms are set up exactly the same and all have different business processes, network infrastructures and types of data. You need a plan customized to fit your firm – the smaller you are, the shorter the plan is likely to be. While a book could be written about IRPs, we are going to give you a condensed and, we hope, digestible overview.

The Elements of an IRP

- Name the position titles which will be responsible for the functions listed in the IRP. Don't use names since people come and go. You need a broad-based team if you are a firm of any size – management, IT, information security, human resources, compliance, marketing, etc. Have a conference call bridge line identified in case a breach happens at night or on the weekends and include home/cell phone numbers and personal as well as work e-mail addresses. This list will need to be updated regularly as people join or leave the firm.
- Identify the contact information for a good data breach lawyer – many large firms now have whole departments working with data breaches. Don't think you can handle this without an attorney who specializes in data breaches. Your data breach lawyer (if you selected a good one) will be an invaluable quarterback for your IRP team – and he or she may be able to preserve under attorney/client privilege much of the information related to the breach.
- Identify the location of your insurance policy (which darn well better cover data breaches). You need to make sure you are covered before you start and list the insurer's contact information because you are going to need to call your insurer as soon as you are aware of a possible breach.
- Identify the contact information for law enforcement – perhaps your local FBI office – often the first folks called in.
- Identify the contact information for the digital forensics company you would want to investigate and remediate the cause of the breach. Generally, you will have been breached for six months or more before you discover the breach – it will take time to unravel what went on. You'll want to know if all data that should have been encrypted was indeed encrypted in transmission and in storage. If it was, this may lessen your notification burden. Identify any PII (Personally Identifiable Information) that may have been compromised.
- If you have intrusion detection or data loss prevention software, those logs should be provided to your investigators immediately and preserved. If you don't, you may want to think about implementing such software.

- Identify the contact information for your bank in case your banking credentials have been compromised.
- (Optional but often useful) Identify the contact information for a good public relations firm. If you are not required to make the breach public, you may not need one, but if it does go public, you may need to do some quick damage control. Your insurance coverage may provide for this, in which case the insurance company will put you in contact with the appropriate firm.
- How will you handle any contact with clients and third parties, remembering that you may wish not to "reveal all" and yet need to achieve some level of transparency? Be forewarned that this is a difficult balance. You will feel like the victim of a data breach, but your clients will feel as though you have breached their trust in you. A data breach that becomes public can cause a mass exodus of clients so work through your notification planning with great care. Be wary of speaking too fast before facts are fully vetted – this is a common mistake, trying to limit the damage and actually increasing it as the scope of the breach turns out to be far greater than first known.
- How will you handle informing employees about the incident? How will you ensure that the law firm speaks with one voice and that employees do not spread information about the breach in person or online? How will your social media cover the breach, if at all?
- If you have a data breach notification law in your state (and almost all do), put it right in the plan along with compliance guidelines. You may be required to contact your state Attorney General. These laws vary widely so be familiar with your own state law.
- If you have HIPAA, HITECH or other regulated data that may be impacted, make sure the relevant data breach regulations are referenced in the plan and attached to it.
- Does the breach require that IT and information security policies be changed? Does what you learned from the breach require that the IRP itself be revised? The IRP should mandate an annual review even without an incident.

Dress rehearsals

Yes, you do want to rehearse for a data breach. Add and subtract factors. Add a terrorist threat, subtract key personnel who are on a cruise, yada, yada. This is most often done as a tabletop exercise, one that should take place at least annually.

You will find that your needs and responses to a breach may evolve over time. For instance, as ransomware saw a 4000% increase in 2014, it became apparent that many back-up systems needed to be re-engineered so that they wouldn't be impacted by Cryptolocker, CryptoWall and their many variants. The threats will no doubt morph over time – as will the defenses.

Employee training

Make no mistake about it. The most successful attack against law firms is spear phishing - a targeted attack where the attacker has done some reconnaissance. They may know what cases you're involved in, who the opposing counsel is, the nickname of a senior partner, etc. This makes it easy to send what looks like a "genuine" e-mail, which in reality contains a malicious hyperlink or an attachment.

Training employees to be skeptical and to refrain from being click happy and to think about the e-mail they see in their Inbox is invaluable. We've seen firms which have successfully avoided a breach simply because an employee had enough sense to question whether a very well-done phishing e-mail was real.

If you question the monies spent on training or the loss of billable time, stack those costs up against the financial damage of a data breach and you'll see the absolute need for annual training. According to Verizon's 2015 Data Breach Investigations Report, almost 30% of data security incidents were due to human error. Persuaded yet?

Vendor Management

This could be the subject of an entire article, but just take our word for it. The security of third party vendors that have "hooks" into your network is critical for you to understand. Just ask Target which got compromised because an HVAC contractor was breached and the contractor had administrator access to Target's network. Make sure you understand a vendor's information security and don't permit vendors to have access to any data they don't need. A vendor

management policy is now a key law firm policy – we only started seeing these in the last year or two. If you don't have one, this too should be high on your priority list.

Final words

We recently read a white paper which was entitled, "Breach Preparation: Plan for the Inevitability of Compromise." It occurred to us that lawyers are very resistant to that idea, sometimes worried about cost or maybe just burying their heads in the sand and hoping that no bad guys zero in on them. While a data breach is indeed a nightmare, you are far more likely to survive it if you have a plan. This is not the time to be sanguine that you can survive hacking attempts when so many mighty entities have fallen victim.

Complacency and inaction are not your friends. Lawyers love risk management. The surest pathway to data breach risk management is to be prepared.

The authors are the President and Vice President at Sensei Enterprises, Inc., a digital forensics, information security and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) sensei@senseient.com, http://www.senseient.com