

MONTHLY LUNCHTIME SEMINAR SERIES

63rd Session:

**"YOU'VE BEEN HACKED!
NOW WHAT?"**

*Judge Lynn M. Egan (Ret.)
Mr. Trent Walton*

April 24, 2018



FACULTY BIOS

April 24, 2018

JUDGE LYNN M. EGAN (Ret.)

Judge Lynn M. Egan became a Cook County Circuit Court judge in 1995 and served in the Law Division for nearly 22 years. She presided over high volume motion calls, an Individual Commercial Calendar, an Individual General Calendar and bench and jury trials. For several years before her retirement in 2017, she was the only Cook County judge assigned to a General Individual Calendar in the Law Division, which includes every type of case filed in the Division, specifically including personal injury actions such as medical & dental malpractice, product liability, infliction of emotional distress, defamation/slander, premises liability, construction & motor vehicle accidents, as well as commercial disputes such as breach of contract, fraud, conspiracy, breach of fiduciary duty, wrongful termination, employment discrimination and legal & accounting malpractice. She managed these cases from time of filing until final disposition, including all motion practice, case management, settlement conferences and trials. Additionally, Judge Egan was committed to assisting parties with the voluntary resolution of cases. As a result, hundreds of cases pending on other judges' calls in the Law & Chancery Divisions & the Municipal Districts were transferred to Judge Egan each year for settlement conferences and she helped facilitate settlements totaling over 275 million dollars.

Judge Egan also served as a member of several Illinois Supreme Court Committees, including the Executive Committee, Discovery Procedures Committee, Civil Justice Committee and Education Committee. She was also a faculty member at dozens of judicial seminars throughout the state, including the annual New Judges' Seminar, regional conferences and the mandatory Education Conference. She authored numerous articles on subjects such as discovery, requests to admit, restrictive covenants, Day-In-The-Life films, directed verdicts, jury selection & instructions, Dead Man's Act, Supreme Court Rule 213, expert witnesses, reconstruction testimony, court-ordered medical exams, attorney-client/work product privileges, sanctions, special interrogatories, examination of experts and damages. She also served as a mentor for new judges and the Illinois Courts Commission, a seven-member panel responsible for rendering final decisions on matters of judicial discipline.

Judge Egan has served on Bar Association committees and Boards of Directors and has been a frequent speaker at Bar Association seminars. She has taught law school classes and judged trial & appellate advocacy competitions. In 2012, she became a registered CLE provider through the Illinois MCLE Board and provides free CLE seminars for attorneys and judges every month. Since her monthly seminar series began in August 2012, Judge Egan has awarded over 13,000 hours of free CLE credit to Illinois attorneys.



Prior to joining the bench, Judge Egan was an equity partner at Hinshaw & Culbertson, where she focused her practice on medical negligence cases. In addition to trial work, she argued before the Illinois Supreme Court on a matter of first impression in the country in *Cisarik v. Palos Community Hospital*. Similarly, during her earlier career in the Cook County State's Attorney's Office, she worked in the criminal and juvenile divisions and argued before the Illinois Appellate and Supreme Courts on matters of first impression in Illinois. She currently works as a senior mediator at ADR Systems in Chicago.

TRENT WALTON

Trent Walton has 16 years of expertise in cyber security, computer forensics, eDiscovery and software development specialized for the legal industry. He has created two cutting-edge legal software products that are currently being used by customers in the Am Law 100, Fortune 500 and U.S. government. Trent has also provided consulting services on complicated technical matters for law firms of all sizes, major corporations and insurance carriers. He is an accomplished speaker who has given more than 300 continuing education seminars for both attorneys and insurance claims professionals.

Trent most recently served as chief technology officer and national director of legal technology at U.S. Legal Support, Inc., one of the leading providers of litigation services, after it acquired his small business specializing in computer forensics and eDiscovery services. During his final year at U.S. Legal Support, the company was ranked No. 1 in both eDiscovery and Court Reporting Services by the National Law Journal.

Trent has founded three small businesses in the technical legal services and software spaces, all of which were acquired by larger companies who prized their intellectual property and strong operations.

Trent holds a Bachelor's of Science in Computer Information Sciences and a Bachelor's of Business Administration in Entrepreneurial Management from Texas Christian University.

KRIS MERRITT

Kris's broad and deep experience in and around cyber security have led to an understanding that the right people doing the right kind of work, with the right tooling and enablement, is the answer to every hard security problem.

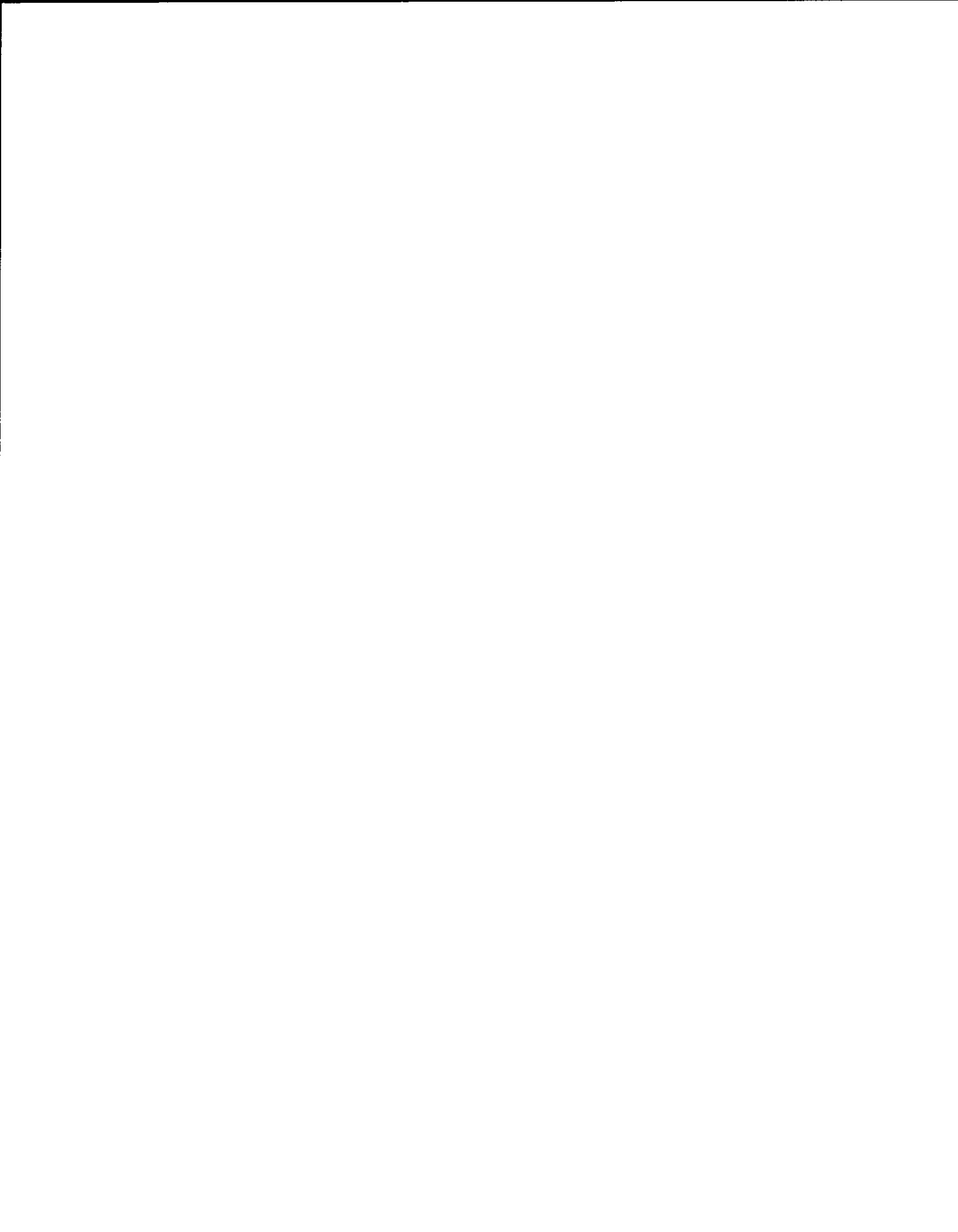
Kris has 14 years of experience in cyber security, network defense, and IT operations, mainly in leadership roles of security operations, incident response, digital forensics, signature development, indicator management, and tactical tool development within very large enterprise networks. Kris has a special interest in

security orchestration, automation, and culture, and has applied related philosophies to build lean-but-powerful security operations teams in the U.S. Air Force ("AFCERT"), General Electric, and CrowdStrike. Most recently, Kris started and led CrowdStrike's Falcon Overwatch hunting service from the ground-up as well as the company's internal hunting program.

Kris holds a Bachelor's of Science in Computer Engineering from the U.S. Air Force Academy and an MBA from the University of Phoenix.

SECTION A

- *Is Cyber Security a Risk to Law Firms?* by Trent Walton, April 2018.



CLE Program: Is Cyber Security a Risk to Law Firms?

Description:

Join a judge and two tech experts for a walk through of the current trends regarding law firm data breaches. The speakers have collectively discovered hundreds of targeted attacks across every industry vertical spanning dozens of countries. They will provide insight into the many motives and tactics used by today's attackers as well as considerations for preparing for tomorrow's attacks.

Topics Covered:

- Ethical obligations in a law firm data breach
- Motives of attackers
- Techniques used by cyber criminals
- Associated costs and consequences
- How a law firm can prepare themselves for a breach

CLE Length: 1 Hour

Program Outline

- Introduction to Speakers (5 Minutes)
- The Statistics (5 Minutes)
 - ABA's 2016 Legal Technology Survey Report, more than one quarter of firms with more than 500 lawyers admitted they experienced some type of breach. Approximately 40 percent of those firms reported significant resulting business downtime and loss of billable hours, and approximately 25 percent recounted hefty fees to correct the problems.
 - 40% of law firms that had their networks assessed had experienced a data breach in 2016 and did not know about it.
 - Nearly 1 million UK law firm passwords are available on the dark web, report says
 - Attached PDF
 - 80% include passwords
 - Cost: \$93,322. Average cost of network intrusion investigation.
 - "Not just money, anxiety and uncertainty."
 - ...
- Ethical obligations (15 Minutes)
 - ABA 1.1 and 1.6
 - Look at Ethical Considerations
 - Breach notification laws, IL

- Law Firm breaches (20 Minutes)
 - Why?
 - Money
 - Access to confidential information
 - ...
 - How?
 - Phishing
 - Website visit
 - Thumb drive
 - Zero day exploit
 - Not-Petya
 - DLA Piper
 - Physical access
 - Raspberry Pi
 - Ransomware
 - Why and How use case:
 - Moses Afonso Ryan \$700K in lost billings from ransomware
 - Moses Afonso Ryan's computers became infected with the ransomware virus last year as a result of a lawyer clicking on an email attachment, the suit says. The virus disabled the firm's computer network, along with all of the documents and information on the network. As a result, lawyers and staffers "were rendered essentially unproductive," according to the suit.
 - <http://www.abajournal.com/news/article/victimized-by-ransomware-law-firm-sues-insurer-for-700k-in-lost-billings>
 - Associated Costs and Consequences
 - Incident response, investigation
 - Lost billables
 - Lost work product, client data
 - Stolen client information
 - Breached attorney/client communication
 - 3rd party litigation
 - Loss of clients
 - Attorneys departure from firm
 - Costs and Consequences Use Case
 - ["Ransomware Attack on DLA Piper Puts Law Firms, Clients on Red Alert"](https://blog.barkly.com/dla-piper-petya-ransomware-attack)
 - <https://blog.barkly.com/dla-piper-petya-ransomware-attack>
 - A full day without phones. Six days without email. Nearly two weeks without complete access to older email and other documents
 - "Consider litigators unable to access motions on a deadline. Trial lawyers preparing for arguments without key documents. Transactional lawyers unable to communicate with clients"

SECTION B

- *“You’ve Been Hacked – Now What?”* by Judge Lynn M. Egan (Ret.), April 24, 2018.



YOU'VE BEEN HACKED – NOW WHAT?

by

Judge Lynn M. Egan (Ret.)

April 24, 2018

Despite the fact that the Illinois Rules of Professional Conduct have long required attorneys to safeguard client information, many attorneys and law firms remain uninformed about the scope of risk or frequency of unauthorized disclosure through cyber breaches. This lack of knowledge raises not only competence issues, particularly given the fact that the FBI issued an advisory warning to law firms on November 1, 2009 that they were being specifically targeted by hackers, but also professional liability exposure and economic losses following a malware attack. See, *Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax is Back*, by Joseph R. Marconi, *ISBA Mutual*.

Significantly, a large percentage of law firms that experience a cyber breach do not have cyber insurance and have no idea whether their general insurance covers cyber liability and losses. This is quite risky, especially for corporate lawyers who are involved in client wire transfer instructions or represent clients in trade secret or patent litigation or mergers and acquisitions, all of which can be attractive targets for hackers.

I. Illinois Rules of Professional Conduct

Although cyber security threats are constantly evolving, our ethical responsibilities remain constant, as defined by the following specific provisions of the Illinois Rules of Professional Conduct:

Rule 1.1 – Competence. Comment 8. “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...”

Rule 1.6 – Confidentiality of Information. (a) “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) or required by paragraph (c).” (e) “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.”

Comment 18: Reasonableness is judged by: sensitivity of the information, likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards and the extent to which safeguards adversely affect the lawyer’s ability to represent clients (e.g., software that is excessively difficult to use).

NOTE: Both Rules 1.1 and 1.6 have been amended in recent years to address the increased reliance on technology, including cloud-based services, in the representation of clients. While cloud-based services are certainly permissible, lawyers who use them must have a sufficient understanding of this technology to “properly assess the risks of unauthorized access and/or disclosures of confidential information.” *Preventing Law Firm Data Breaches*, by John W. Simek & Sharon D. Nelson, *Law Practice Magazine*, Vol. 38, No. 1, 2012.

See also, ISBA Professional Conduct Advisory Opinion No. 16-06 (Lawyer may use cloud-based services when rendering legal services so long as he takes reasonable measures to ensure the information is protected from breaches. This obligation does not end merely because the lawyer selected a reputable provider.) An example of the ongoing obligation is illustrated by the complaint filed in Jason Shore & Coinabul, LLC v. Johnson & Bell, Ltd., 2016, No. 16-cv-4363.

Rule 5.1 Responsibilities of Partners, Managers, and Supervisory Lawyers. (a) “A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.” (b) “A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.”

Rule 5.3 Responsibilities Regarding Nonlawyer Assistance. (b) “A lawyer having direct supervisory authority over the nonlawyer shall

make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."

Comment 2: "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product.

CAUTION: Even if the firm has effective cyber security measures in place, lawyers and nonlawyers employed by the firm must be instructed not to use personal, unprotected routers when working on client matters.

II. Illinois Legislation Impacting Personal Privacy

Although the Illinois legislature passed the **Geolocation Privacy Protection Act** in June 2017, Governor Rauner vetoed it in September 2017. This Act sought to protect data privacy by limiting the collection and disclosure of location data from mobile devices by private entities. Consumers would have received notification that their geolocation data was being collected and used and the state's attorney or attorney general was empowered to sue violators pursuant to the Consumer Fraud and Deceptive Business Practices Act.

Similarly, the **Right to Know Act** (SB 1502), has not yet been passed. This Act requires operators of commercial websites or online services that collect personally identifiable information about customers who use or visit their sites through the Internet to notify them of its information sharing practices and provide means by which customers can request the specific information shared. After being re-referred to the Rules Committee on July 6, 2017, it was approved for consideration on April 3, 2018 and placed on the Calendar, but ultimately postponed for further consideration on the same date.

The **Personal Identification Protection Act** ("PIPA")(815 ILCS 530/1-25) was originally enacted, effective January 1, 2006, but was amended effective January 1, 2017 in ways that significantly broaden its protection. Although the Act always required notification at no charge when a covered data breach occurred, the amendment

broadened the scope of protected information, expanded the notice obligations for breaches involving log-in credentials and limits the “encryption safe harbor” so that notification is now required even for encrypted or redacted personal information if the keys to unencrypt or unredact the information was also acquired in the breach.

Although it is unclear whether law firms are “data collectors” under the Act, lawyers representing the following types of clients should definitely be familiar with the recent amendments:

- Government agencies
- Public and private universities
- Corporations
- Financial institutions
- Retail operators
- Any other entity that handles, collects, disseminates, or otherwise deals with nonpublic personal information.

The failure of a “data collector” to make the required notification can constitute a violation of the Consumer Fraud and Deceptive Business Practices Act.

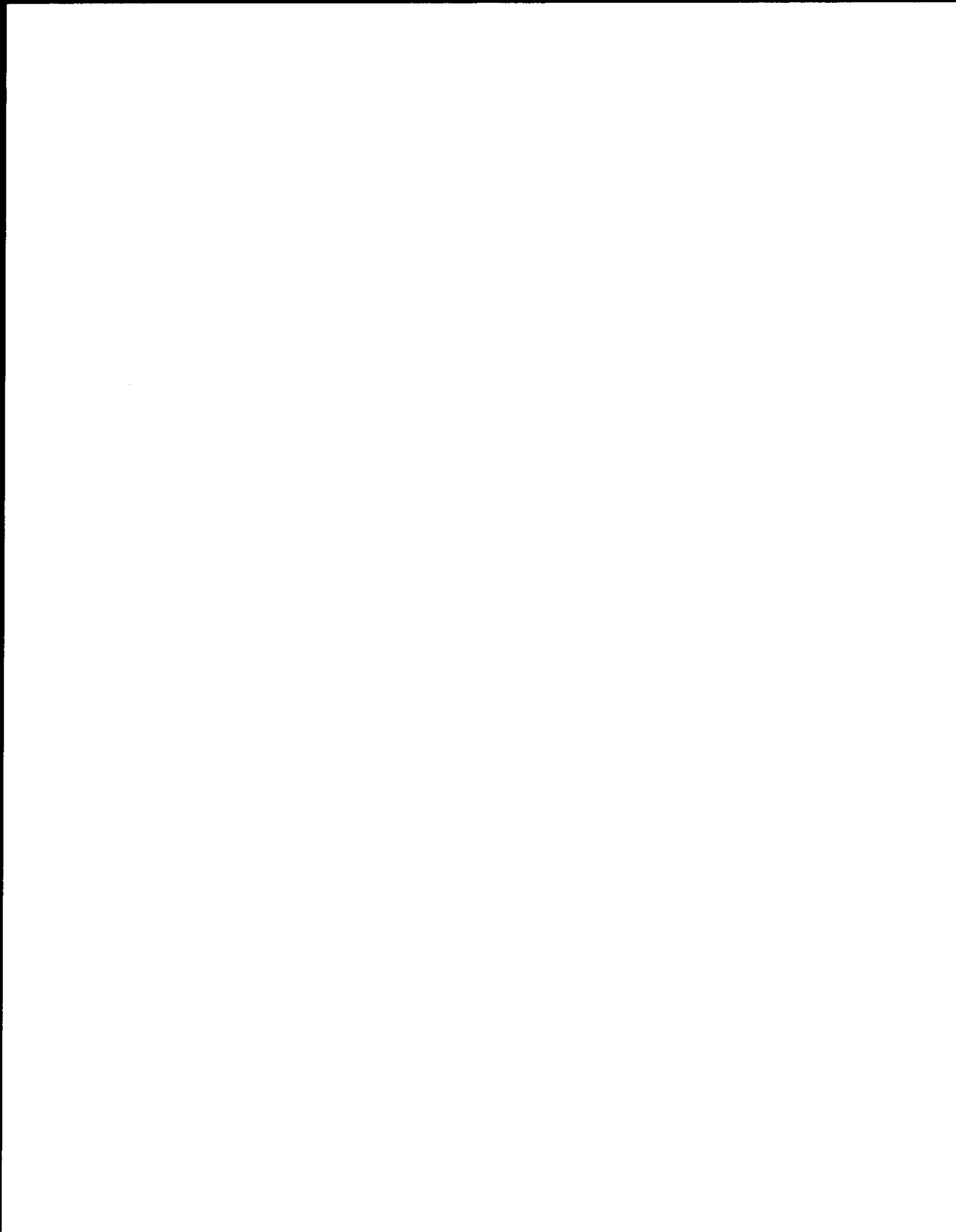
III. Miscellaneous Resources

Whether personal information has been breached in the context of the attorney-client relationship or otherwise, the following federal agencies offer informative guidance about appropriate responses:

- The Federal Trade Commission provides detailed suggestions and resources, including specific discussions about how to protect your identity, the warning signs of identity theft, how to discover identity theft, what to do if you suspect misuse of your social security number or tax-related and medical identity theft. (www.consumer.ftc.gov/topics/privacy-identity-online-security).
- The Federal Deposit Insurance Corporation (FDIC) provides guidance on response programs for data breaches by financial institutions. (www.fdic.gov/news/news/financial/2005/fil2705.html).

SECTION C

- *Personal Information Protection Act, 815 ILCS 530/1-40(West 2017).*



AN ACT concerning business.

**Be it enacted by the People of the State of Illinois,
represented in the General Assembly:**

Section 5. The Personal Information Protection Act is amended by changing Sections 5, 10, and 12 and by adding Section 40 as follows:

(815 ILCS 530/5)

Sec. 5. Definitions. In this Act:

"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or

subject to further unauthorized disclosure.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) Social Security number.

(2) Driver's license number or State identification card number.

(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/10)

Sec. 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope

of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the

breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject

persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(d) Notwithstanding any other subsection in this Section ~~(e)~~, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(Source: P.A. 94-36, eff. 1-1-06; 94-947, eff. 6-27-06.)

(815 ILCS 530/12)

Sec. 12. Notice of breach; State agency.

(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall

include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(a-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the State agency with a written request for the delay. However, the State agency must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(b) For purposes of this Section, notice to residents may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the State agency demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to

be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the State agency has an email address for the subject persons; (ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and (iii) notification to major statewide media.

(c) Notwithstanding subsection (b), a State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/40 new)

Sec. 40. Disposal of materials containing personal information; Attorney General.

(a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.

(b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:

(1) Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.

(2) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.

(c) Any person disposing of materials containing personal information may contract with a third party to dispose of such

materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

(d) Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than \$100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed \$50,000 for each instance of improper disposal of materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

(f) A financial institution under 15 U.S.C. 6801 et. seq. or any person subject to 15 U.S.C. 1681w is exempt from this Section.



Course Evaluation Form

Title of Course: "YOU'VE BEEN HACKED! NOW WHAT?"

Date of Course: April 24, 2018 Location: James R. Thompson Center Assembly Hall Auditorium

Directions: On a scale of 1 to 5, (5 being the highest or best and 1 being the lowest or worst), please rate the program:

Rate how well this course satisfied your personal objectives 5 4 3 2 1

Comments: _____

Rate how well the environment contributed to the learning experience 5 4 3 2 1

Comments: _____

Rate how well the written materials contributed to the learning experience 5 4 3 2 1

Comments: _____

Rate the level of significant intellectual, educational or practical content 5 4 3 2 1

Comments: _____

Please rate the faculty using the same 1 – 5 scale:

Name: JUDGE LYNN M. EGAN (Ret.)

Comments: _____

Name: MR. TRENT WALTON

Comments: _____

Overall Teaching Effectiveness					Effectiveness of Teaching Methods					Significant Current Intellectual or Practical Content				
5	4	3	2	1	5	4	3	2	1	5	4	3	2	1

SUGGESTIONS FOR FUTURE SEMINARS: _____

Monthly Lunchtime Seminar Series

63rd Session:

“You’ve been hacked! Now what?”

Judge Lynn M. Egan (Ret.)

Mr. Trent Walton

April 24, 2018

Contents:

- Faculty Bios
- CyberShield U.S. Company Overview
- CyberShield U.S. Services
- USI Cyber Basic Data Security & Privacy Liability
- USI Cyber Liability How Does Your Policy Compare 2017
- “You’ve been hacked – Now What?” by Judge Lynn M. Egan (Ret.), April 24, 2018
- 2018 BakerHostetler Data Security Incident Response Report
- “Cybersecurity: Risks and Safeguards for the Business Litigator” by Jeffery K. Brandt, Monica Minkel, RPLU, MLIS, Daniel C. Nelson, C|EH, CIPP/US
- Personal Information Protection Act, 815 ILCS 530/1-40 (West 2017).

FACULTY BIOS

April 24, 2018

JUDGE LYNN M. EGAN (Ret.)

Judge Lynn M. Egan became a Cook County Circuit Court judge in 1995 and served in the Law Division for nearly 22 years. She presided over high volume motion calls, an Individual Commercial Calendar, an Individual General Calendar and bench and jury trials. For several years before her retirement in 2017, she was the only Cook County judge assigned to a General Individual Calendar in the Law Division, which includes every type of case filed in the Division, specifically including personal injury actions such as medical & dental malpractice, product liability, infliction of emotional distress, defamation/slander, premises liability, construction & motor vehicle accidents, as well as commercial disputes such as breach of contract, fraud, conspiracy, breach of fiduciary duty, wrongful termination, employment discrimination and legal & accounting malpractice. She managed these cases from time of filing until final disposition, including all motion practice, case management, settlement conferences and trials. Additionally, Judge Egan was committed to assisting parties with the voluntary resolution of cases. As a result, hundreds of cases pending on other judges' calls in the Law & Chancery Divisions & the Municipal Districts were transferred to Judge Egan each year for settlement conferences and she helped facilitate settlements totaling over 275 million dollars.

Judge Egan also served as a member of several Illinois Supreme Court Committees, including the Executive Committee, Discovery Procedures Committee, Civil Justice Committee and Education Committee. She was also a faculty member at dozens of judicial seminars throughout the state, including the annual New Judges' Seminar, regional conferences and the mandatory Education Conference. She authored numerous articles on subjects such as discovery, requests to admit, restrictive covenants, Day-In-The-Life films, directed verdicts, jury selection & instructions, Dead Man's Act, Supreme Court Rule 213, expert witnesses, reconstruction testimony, court-ordered medical exams, attorney-client/work product privileges, sanctions, special interrogatories, examination of experts and damages. She also served as a mentor for new judges and the Illinois Courts Commission, a seven-member panel responsible for rendering final decisions on matters of judicial discipline.

Judge Egan has served on Bar Association committees and Boards of Directors and has been a frequent speaker at Bar Association seminars. She has taught law school classes and judged trial & appellate advocacy competitions. In 2012, she became a registered CLE provider through the Illinois MCLE Board and provides free CLE seminars for attorneys and judges every month. Since her monthly seminar series began in August 2012, Judge Egan has awarded over 13,000 hours of free CLE credit to Illinois attorneys.

Prior to joining the bench, Judge Egan was an equity partner at Hinshaw & Culbertson, where she focused her practice on medical negligence cases. In addition to trial work, she argued before the Illinois Supreme Court on a matter of first impression in the country in *Cisarik v. Palos Community Hospital*. Similarly, during her earlier career in the Cook County State's Attorney's Office, she worked in the criminal and juvenile divisions and argued before the Illinois Appellate and Supreme Courts on matters of first impression in Illinois. She currently works as a senior mediator at ADR Systems in Chicago.

TRENT WALTON

Trent Walton has 16 years of expertise in cyber security, computer forensics, eDiscovery and software development specialized for the legal industry. He has created two cutting-edge legal software products that are currently being used by customers in the Am Law 100, Fortune 500 and U.S. government. Trent has also provided consulting services on complicated technical matters for law firms of all sizes, major corporations and insurance carriers. He is an accomplished speaker who has given more than 300 continuing education seminars for both attorneys and insurance claims professionals.

Trent most recently served as chief technology officer and national director of legal technology at U.S. Legal Support, Inc., one of the leading providers of litigation services, after it acquired his small business specializing in computer forensics and eDiscovery services. During his final year at U.S. Legal Support, the company was ranked No. 1 in both eDiscovery and Court Reporting Services by the National Law Journal.

Trent has founded three small businesses in the technical legal services and software spaces, all of which were acquired by larger companies who prized their intellectual property and strong operations.

Trent holds a Bachelor's of Science in Computer Information Sciences and a Bachelor's of Business Administration in Entrepreneurial Management from Texas Christian University.

KRIS MERRITT

Kris's broad and deep experience in and around cyber security have led to an understanding that the right people doing the right kind of work, with the right tooling and enablement, is the answer to every hard security problem.

Kris has 14 years of experience in cyber security, network defense, and IT operations, mainly in leadership roles of security operations, incident response, digital forensics, signature development, indicator management, and tactical tool development within very large enterprise networks. Kris has a special interest in

security orchestration, automation, and culture, and has applied related philosophies to build lean-but-powerful security operations teams in the U.S. Air Force ("AFCERT"), General Electric, and CrowdStrike. Most recently, Kris started and led CrowdStrike's Falcon Overwatch hunting service from the ground-up as well as the company's internal hunting program.

Kris holds a Bachelor's of Science in Computer Engineering from the U.S. Air Force Academy and an MBA from the University of Phoenix.



CYBERSHIELD U.S.

**A single data breach could paralyze
your practice and compromise your
clients' confidential information**

OVERVIEW

CYBERSHIELD U.S. offers cybersecurity detection, response and consulting services designed specifically for the needs of law firms and the clients they serve. Our team combines world-class expertise in cybersecurity, incident response, threat hunting and forensics with years of experience in litigation services, forensics, eDiscovery and law enforcement.

We understand the vulnerabilities of and threats to law practices and provide customized solutions to protect firm assets, quickly detect compromises, and effectively respond to data breaches, insider threats and malware outbreaks. Whether you want to audit vendor compliance, communicate securely with clients, or protect internal firm networks, CYBERSHIELD U.S. provides cybersecurity services tailored to your goals.

IMPROVE DETECTION

- Many attackers are not found for months, increasing damage and cost to respond
- Existing tools are ineffective: phishing accounts for 34% of incidents, even with modern firewalls and gateways
- Teams are inexperienced at hunting advanced threats
- Firms and their vendors keep huge amounts of secure data, yet may not be prepared to protect it

IMPROVE RESPONSE

- Intrusions are challenging to investigate and often affect highly sensitive, regulated or proprietary information
- Identifying and containing hackers and insider threats is complex
- Malware, including viruses, Trojan horses and ransomware are difficult to eradicate
- Hiring and retaining experienced response personnel is tough

IMPROVE PROTECTION

- Unknown vulnerabilities and threats increase risks to company assets
- Overburdened security staff may be challenged to identify and prevent breaches
- Immature information security programs can lead to gaps in security controls

**Prepare for or suspect a
data breach?**

Call us for a free consultation.

[cybershieldus.com](http://www.cybershieldus.com)

855-

US



CYBERSHIELD U.S.

CYBERSHIELD U.S. offers cybersecurity detection, response and consulting services for law firms and their clients

Compromise Assessment (Threat Hunting)

We can actively identify attackers that evade your defenses. We hunt down cyber intruders already in your systems to eradicate them, protect your critical assets and save money. This service is vital because data breaches are common and expensive; the faster you detect a breach, the less it costs you.

In the event of a data breach, our certified responders use advanced tools to investigate and remediate the incident. An effective incident response team: **(1) reduces the cost of an incident; (2) minimizes stress and confusion; and (3) reduces the chance of reinfection.** Our team also delivers a best-in-class report customized to your technical and legal requirements.

Cybersecurity is a complex discipline; our expert consultants help you save time, money and effort and steer you toward clear improvements and reduced risk. We offer expert assessments, advice and training to help you maximize your investments.

We create custom solutions for your specific needs, including ways to: **(1) enhance your team's skills** through training and staff planning; **(2) improve your processes, policies and documentation** to meet compliance and operational goals; and **(3) refine your technology** through technical assessments, architecture, design and tuning. In addition, we provide the following standard services:

- Training, including continuing legal education (CLE), for your associates, security teams and executives
- Security assessments to find vulnerabilities and recommend actionable solutions
- Vendor assessments to audit the security of your legal service providers and other trusted vendors
- Security program design that provides a risk-based, cost-effective strategy to meet compliance or industry best-practices in information security

Prepare for or suspect a data breach?

Call us for a free consultation.

CYBERSHIELDUS.com

855-

US



Data Security & Privacy Liability

For data to be useful, it must be accessible, yet access creates vulnerabilities.
Will your company have protection when you need it most?

There are hundreds of regulations now in state after state which require companies to take specific actions when data is compromised. How will your company pay the extra expenses associated with complying with your privacy policy? Do you know who to call when a data breach happens to you?

Data Security & Privacy Liability insurance products have come a long way in the last ten years. Coverage is broader than you think and less costly than you might expect. The application process has even gotten easier (for some companies at least). A quality Data Security & Privacy Liability product may cover many different insuring agreements including the following:

Media Liability - Media Liability addresses the various media exposures like pictures posted on your website or copyright infringement on content.

Security & Privacy Liability - Security & Privacy Liability provides for defense costs and legal expenses to deal with a civil or criminal suit arising from a data breach or hacking.

Regulatory Defense and Penalties - State and Federal penalties may be imposed after a breach with the Regulatory Defense Costs will provide you with resources to defend your action (or inaction) and many policies cover fines & penalties imposed.

Breach Response Costs - Many companies find the majority of their expense in the breach notification cost category. This risk includes forensic assistance, public relations costs, notification and credit monitoring.

Reputational Damage and Business Income - Some companies may suffer a loss of income after a breach due to an inability to operate or have significant cost to repair the public trust with their customer base.

Network Asset Protection - Sometimes the goal of a hacker is to damage, destroy, or delete data. Network Asset Protection can help you with the extra expense to recover and restore your data.

Cyber Extortion - Cyber Extortion can happen via e-mail or other communication where a hacker is holding your data hostage for ransom. Many policies provide resources that will help you mitigate damage from an extortion attempt.

Cyber Terrorism - Cyber Terrorism may cause significant loss to an organization.

Cyber Crime/Social Engineering - Confidence fraud has happened since the beginning of time. Today, fraudsters may use e-mail, forged documents and phone calls to manipulate your employees into sending money or other assets to the criminals. There is insurance available to cover these types of events.

USI's Management & Professional Services (MPS) team brings decades of focused, dedicated experience working alongside a wide range of companies. Our analysis and review of your exposures can help develop broad coverage at a competitive price that will meet the needs of your organization.

Data Security & Privacy Liability (Cyber) policies vary, sometimes widely, by carrier. Work with a team that understands the nuances of coverage and that can explain why a different product might be a better fit for your unique exposures.


Contact your USI MPS representative today to learn how to address the exposures in your company.
Call Monica Minkel at 303.831.5103 or e-mail at monica.minkel@usi.biz.



Cyber Liability

How Does Your Policy Compare?

Data Security & Privacy Liability Insurance products have come a long way in the last five years. Coverage is broader than you think and cheaper than you might expect. The application process has even gotten easier (for some companies at least). Are you covered?

		Your Policy
Multimedia Liability <i>(Coverage not limited to Internet)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Security & Privacy Liability <i>(Coverage not limited to Internet)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Regulatory Defense & Penalties <i>(Coverage not subject to cap on damages)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Privacy Breach, Response Costs <i>(Coverage not limited)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Reputational Harm (USI Exclusive BrandGuard)	<input type="checkbox"/>	<input type="checkbox"/>
Network Asset Protection/ Business Income Interruption <i>(Short waiting period)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Cyber Extortion <i>(Including Ransom demand in non-US currency)</i>	<input type="checkbox"/>	<input type="checkbox"/>
Cyber Crime / Social Engineering	<input type="checkbox"/>	<input type="checkbox"/>
PCI Compliance Fines & Penalties	<input type="checkbox"/>	<input type="checkbox"/>

USI's Management & Professional Services (MPS) team brings decades of focused, extensive experience working alongside a wide range of companies. Our analysis and review of your exposures can help develop broad coverage at a competitive price that will meet the needs and budget of your organization.

Data Security & Privacy Liability (Cyber) policies vary, sometimes widely, by carrier. Work with a team that understands the nuances of coverage and that can explain why a different product might be a better fit for your unique exposures.

Contact your USI representative today to learn how to address the exposures in your company. Email Monica Minkel at monica.minkel@usi.com or call 303.831.5103.

YOU'VE BEEN HACKED – NOW WHAT?

by

Judge Lynn M. Egan (Ret.)

April 24, 2018

Despite the fact that the Illinois Rules of Professional Conduct have long required attorneys to safeguard client information, many attorneys and law firms remain uninformed about the scope of risk or frequency of unauthorized disclosure through cyber breaches. This lack of knowledge raises not only competence issues, particularly given the fact that the FBI issued an advisory warning to law firms on November 1, 2009 that they were being specifically targeted by hackers, but also professional liability exposure and economic losses following a malware attack. See, *Don't Let Cybersecurity Breaches Lead to Legal Malpractice: The Fax is Back*, by Joseph R. Marconi, *ISBA Mutual*.

Significantly, a large percentage of law firms that experience a cyber breach do not have cyber insurance and have no idea whether their general insurance covers cyber liability and losses. This is quite risky, especially for corporate lawyers who are involved in client wire transfer instructions or represent clients in trade secret or patent litigation or mergers and acquisitions, all of which can be attractive targets for hackers.

I. Illinois Rules of Professional Conduct

Although cyber security threats are constantly evolving, our ethical responsibilities remain constant, as defined by the following specific provisions of the Illinois Rules of Professional Conduct:

Rule 1.1 – Competence. Comment 8. “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...”

Rule 1.6 – Confidentiality of Information. (a) “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) or required by paragraph (c).” (e) “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.”

Comment 18: Reasonableness is judged by: sensitivity of the information, likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards and the extent to which safeguards adversely affect the lawyer’s ability to represent clients (e.g., software that is excessively difficult to use).

NOTE: Both Rules 1.1 and 1.6 have been amended in recent years to address the increased reliance on technology, including cloud-based services, in the representation of clients. While cloud-based services are certainly permissible, lawyers who use them must have a sufficient understanding of this technology to “properly assess the risks of unauthorized access and/or disclosures of confidential information.” Preventing Law Firm Data Breaches, by John W. Simek & Sharon D. Nelson, *Law Practice Magazine*, Vol. 38, No. 1, 2012.

See also, ISBA Professional Conduct Advisory Opinion No. 16-06 (Lawyer may use cloud-based services when rendering legal services so long as he takes reasonable measures to ensure the information is protected from breaches. This obligation does not end merely because the lawyer selected a reputable provider.) An example of the ongoing obligation is illustrated by the complaint filed in Jason Shore & Coinabul, LLC v. Johnson & Bell, Ltd., 2016, No. 16-cv-4363.

Rule 5.1 Responsibilities of Partners, Managers, and Supervisory Lawyers. (a) “A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.” (b) “A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.”

Rule 5.3 Responsibilities Regarding Nonlawyer Assistance. (b) “A lawyer having direct supervisory authority over the nonlawyer shall

make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."

Comment 2: "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product.

CAUTION: Even if the firm has effective cyber security measures in place, lawyers and nonlawyers employed by the firm must be instructed not to use personal, unprotected routers when working on client matters.

II. Illinois Legislation Impacting Personal Privacy

Although the Illinois legislature passed the **Geolocation Privacy Protection Act** in June 2017, Governor Rauner vetoed it in September 2017. This Act sought to protect data privacy by limiting the collection and disclosure of location data from mobile devices by private entities. Consumers would have received notification that their geolocation data was being collected and used and the state's attorney or attorney general was empowered to sue violators pursuant to the Consumer Fraud and Deceptive Business Practices Act.

Similarly, the **Right to Know Act** (SB 1502), has not yet been passed. This Act requires operators of commercial websites or online services that collect personally identifiable information about customers who use or visit their sites through the Internet to notify them of its information sharing practices and provide means by which customers can request the specific information shared. After being referred to the Rules Committee on July 6, 2017, it was approved for consideration on April 3, 2018 and placed on the Calendar, but ultimately postponed for further consideration on the same date.

The **Personal Identification Protection Act** ("PIPA") (815 ILCS 530/1-25) was originally enacted, effective January 1, 2006, but was amended effective January 1, 2017 in ways that significantly broaden its protection. Although the Act always required notification at no charge when a covered data breach occurred, the amendment

broadened the scope of protected information, expanded the notice obligations for breaches involving log-in credentials and limits the “encryption safe harbor” so that notification is now required even for encrypted or redacted personal information if the keys to unencrypt or unredact the information was also acquired in the breach.

Although it is unclear whether law firms are “data collectors” under the Act, lawyers representing the following types of clients should definitely be familiar with the recent amendments:

- Government agencies
- Public and private universities
- Corporations
- Financial institutions
- Retail operators
- Any other entity that handles, collects, disseminates, or otherwise deals with nonpublic personal information.

The failure of a “data collector” to make the required notification can constitute a violation of the Consumer Fraud and Deceptive Business Practices Act.

III. Miscellaneous Resources

Whether personal information has been breached in the context of the attorney-client relationship or otherwise, the following federal agencies offer informative guidance about appropriate responses:

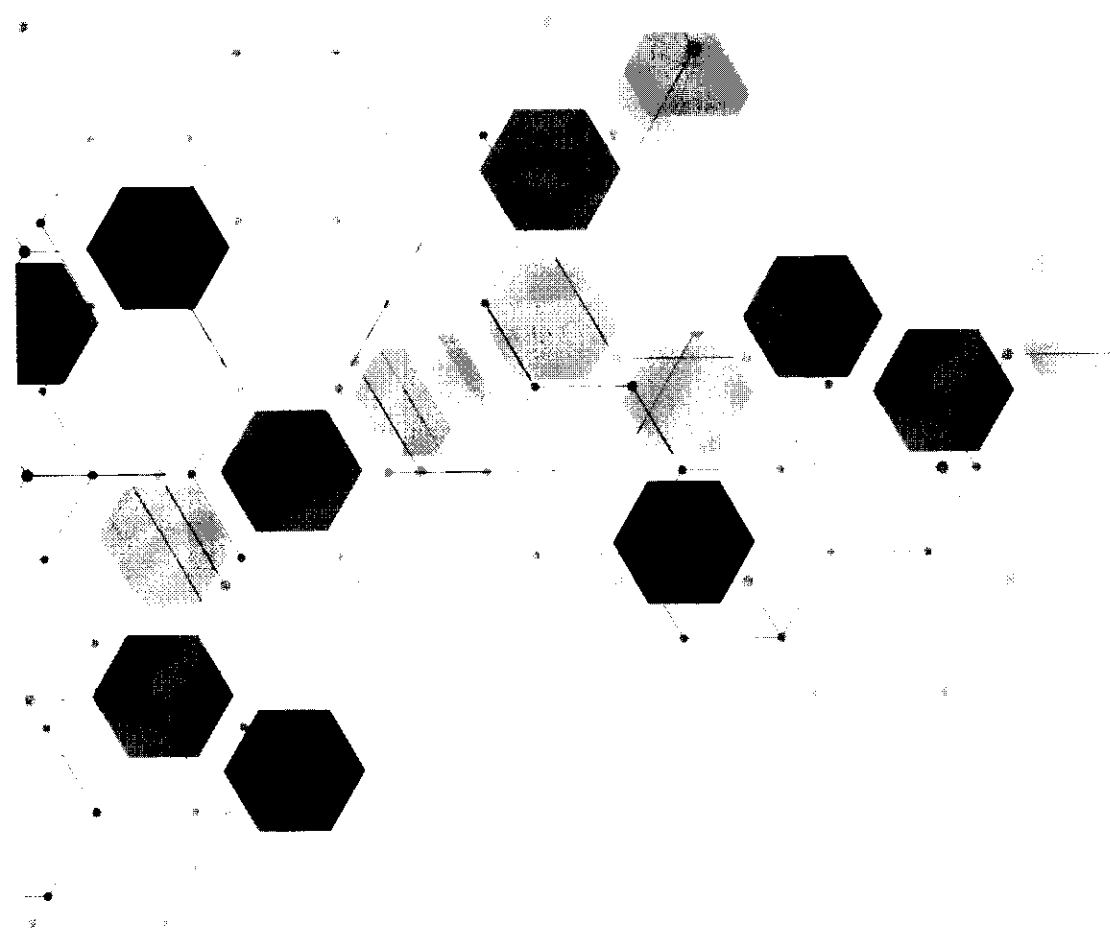
- The Federal Trade Commission provides detailed suggestions and resources, including specific discussions about how to protect your identity, the warning signs of identity theft, how to discover identity theft, what to do if you suspect misuse of your social security number or tax-related and medical identity theft. (www.consumer.ftc.gov/topics/privacy-identity-online-security).
- The Federal Deposit Insurance Corporation (FDIC) provides guidance on response programs for data breaches by financial institutions. (www.fdic.gov/news/news/financial/2005/fil2705.html).

BakerHostetler

2018 DATA SECURITY INCIDENT RESPONSE REPORT

Building Cyber Resilience

Compromise Response Intelligence in Action



Key Findings



Much like encryption of external devices several years ago, multifactor authentication (MFA) has become an essential security measure and is increasingly becoming a regulatory expectation. However, MFA is not infallible, and not all MFA solutions are equally secure.



With incidents on the rise and the stakes higher than ever, senior management, boards, and external auditors are becoming involved in data breach prevention and response.



As entities migrate to the cloud, most security issues are not caused by the cloud service provider, but by how the entity or its service provider configures access to the cloud.



Any entity, of any size, may become the victim of a cyber-attack. Hackers are happy to hit “singles” and take advantage of the lax security practices of small and medium-sized entities, and attacker techniques and tools simplify the process of finding even obscure targets of opportunity.



Recent high-profile incidents have rekindled regulatory interest. And large multistate settlements have given state attorneys general the funds to hire experts and more aggressively investigate breaches.



With the May 25, 2018 effective date looming, entities have been racing the clock to get their privacy, data security and incident response practices in order. Expect adjustments to continue as the regulation is implemented.



Entities still are not executing on the basics. Endpoint monitoring agents, security information and event management (SIEM) solutions, and privileged account management tools have become more common, but good hygiene could have prevented many incidents.



The line determining cognizable damages continues to blur. In addition, recent cases show that privilege may not apply to all incident-related communications, and that some entities choose to waive privilege.

CONTENTS

- 02 Incident Response Trends
- 04 Why Incidents Occur
- 06 Timeline Provides Context for Response Expectations
- 08 Forensics Drive Key Decisions
- 10 Regulators More Involved
- 12 Prepare for Privilege Challenges
- 14 Use Compromise Response Intelligence to Minimize Risk

This is our fourth Report addressing the issues entities care about most when it comes to incident response. The Report's focus remains consistent with that of prior years, although this year we emphasize the importance of using Compromise Response Intelligence in addition to the measures necessary to be Compromise Ready.

2017 was another record-setting year for data security incidents. Attack groups continued to exploit vulnerabilities to gain access to valuable data, phishing remained prevalent and successful, and employees and their vendors made common mistakes that placed sensitive information at risk. But despite attackers' old tactics continuing to work, we saw them also develop new and innovative attacks, including those against supply chains and Internet of Things (IoT) devices. As regulator scrutiny increases and new international breach notification laws take effect, more entities will struggle with these issues globally.

While all incidents cannot be prevented, there are measures entities can take to minimize their attack surface and reduce the frequency and severity of incidents. Equally important, given the increase in attacks intended to disrupt operations, is a focus on building cyber resilience for an agile response. It can be hard to know where to begin, especially in an environment of constant change – but taking steps to proactively address these issues is what we call being Compromise Ready.

Our goal in publishing this Report is to offer practical steps you can take to reduce your risk profile, build resilience, and be better prepared to respond when an incident occurs. The data and experience behind the recommendations come from our work on more than 560 incidents in 2017 and more than 2,000 others in years past. Just as security teams use threat intelligence to prevent attacks, we hope you will use the Compromise Response Intelligence from this Report to prioritize and gain executive support for security spending, educate key stakeholders, fine-tune incident response plans, work more efficiently with forensic firms, assess and reduce risk, build scenarios for tabletop exercises, and determine cyber liability insurance needs.

Please continue to reach out and let us know what information you would find most useful in future reports.

Sincerely,



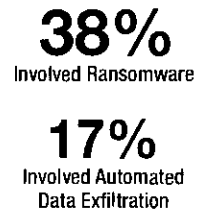
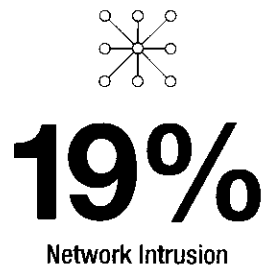
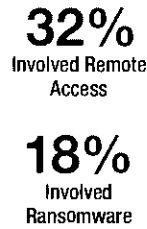
Ted Kobus
Leader, Privacy and Data Protection Team

560+

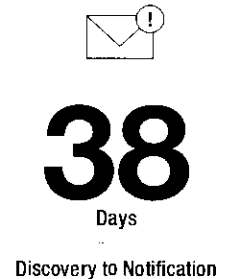
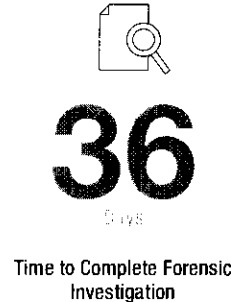
Incidents in 2017

Incident Response Trends

Top 5 Causes



Incident Response Timeline



OCCURRENCE

DISCOVERY

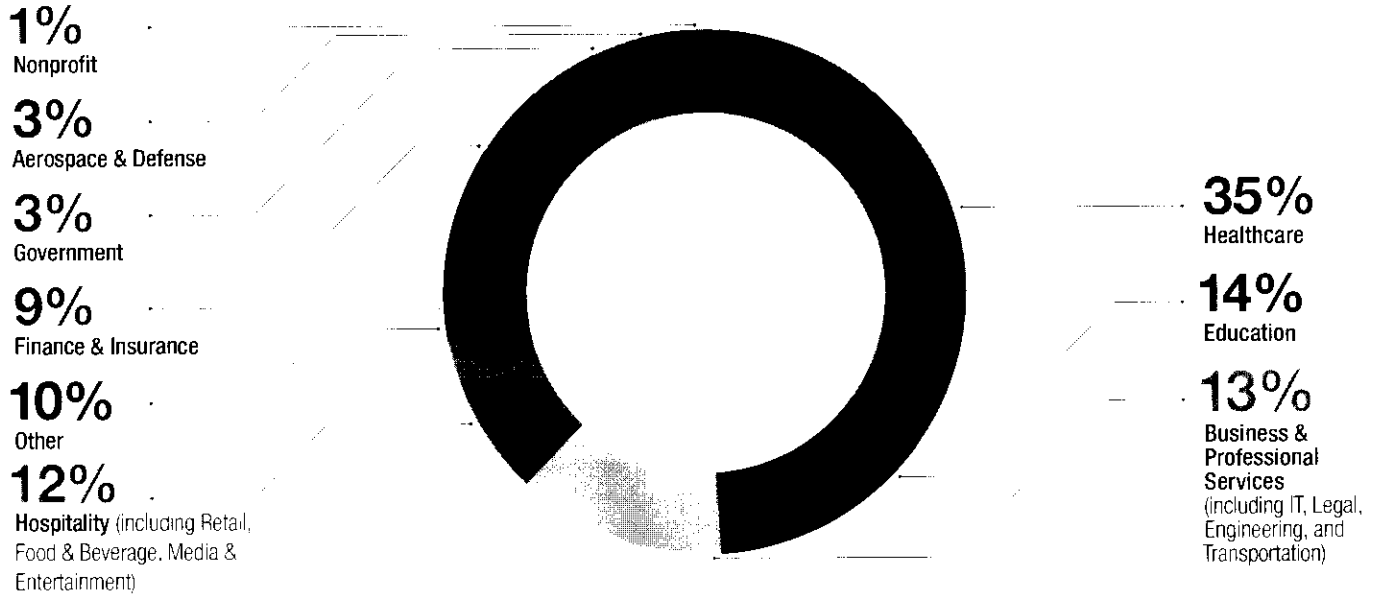
NOTIFICATION



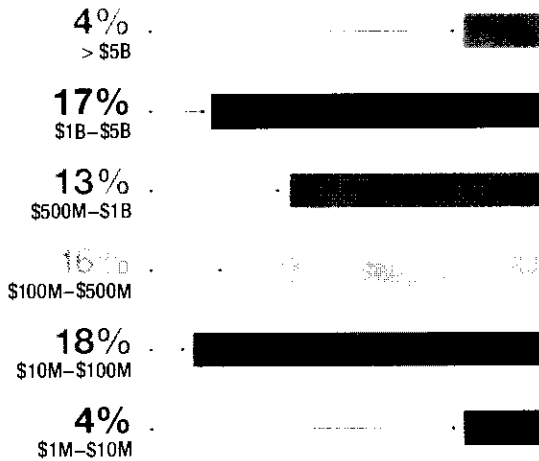
CONTAINMENT

FORENSIC INVESTIGATION COMPLETE

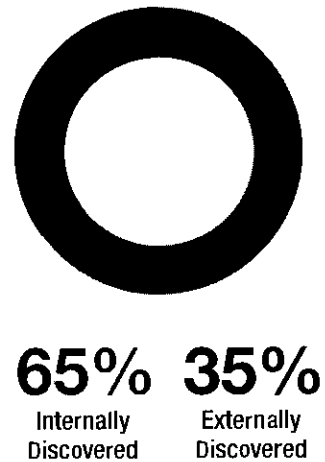
Industries Affected



Entity Size by Revenue



Breach Discovery



Average Forensic Investigation Costs

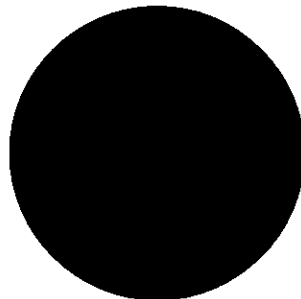


\$84,417
All Incidents

\$436,938
20 Largest Investigations

100%
Increase Over Last Year

Notifications vs. Lawsuits Filed



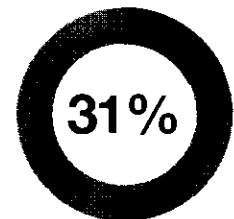
350

Notifications

10

Lawsuits Filed

AG Inquiries Following Notification



31%

Non-AG Inquiries

Year	Count
2016	29
2017	43

Why Incidents Occur

Phishing and Exploitation of Vulnerable Systems Top the List

Over one-third (34%) of the incidents we responded to began when an employee was phished – tricked by an email message into providing access credentials to an unauthorized party, visiting a phony website, downloading an infected document, or clicking on a link that installed malware. Both sophisticated and unsophisticated hackers use phishing to obtain direct network access, convince employees to wire money, enable remote access with compromised credentials, or deploy malware and ransomware. These incidents can be costly and difficult to investigate.

Exploitation of vulnerable systems to gain network access was the second-most frequent tactic used by attackers to obtain initial access, accounting for 19% of the total. After gaining access, deployment of ransomware was the most likely next occurrence.

Ransomware Attacks Continue

Ransomware attacks continued to grab the spotlight with their frequency, occasionally dramatic demands for payment, and headline-ready names like WannaCry. Increasingly, the more traditional ransomware incidents occurred through poorly configured Remote Desktop Protocol services – which are susceptible to default-password guessing or brute-force attacks – rather than traditional phishing links. The attacker remains undetected while conducting reconnaissance and can launch a more devastating attack by encrypting critical data (and, in some instances, deleting backup files). In many cases, victims successfully restore data without paying a ransom, thanks to increasingly maintaining robust off-site backups.

Cloud Misconfigurations: A Growing Trend

System misconfiguration is a new category we tracked this year to reflect the growing number of incidents where unauthorized individuals gain access to cloud instances and storage devices because permissions are set to “public” instead of “private.” Often the unauthorized persons are “security researchers” who will contact the media regarding what they were able to access. These incidents accounted for 6% of the total.



As the value of bitcoins rose, so did the number of crypto-miner attacks, when hackers install malware that uses the victim entity's computer resources to mine bitcoins or other cryptocurrencies for the attacker.

Phishing for Mail Access

As entities continued moving to cloud-based email systems like Office 365 without enabling MFA, we saw a surge in phishing incidents targeting Office 365 login credentials. Often multiple employees, sometimes 20 or more, were phished at the same time, giving the attacker access to all the compromised accounts. The default log settings for most Office 365 instances are not granular enough to show which emails and data an attacker accessed, complicating notification determinations. To address this concern, several forensics firms have developed custom scripts to extract logs with sufficient detail to support notification determinations. Some entities experienced multiple incidents before enabling MFA.

One tactic used by attackers to avoid detection was so common that it is worth a special note. After compromising a user's mail account and using the target's account to send fraudulent emails (in furtherance of a wire fraud scam, W-2 theft or some other fraud), an attacker will typically add mailbox rules to ensure that replies to the imposter emails are forwarded to the attacker and deleted from the mailbox, preventing the real user from seeing replies to the imposter's emails. Thus, merely changing passwords is not enough to contain an incident. Entities must search for and deactivate unauthorized rules changes immediately upon learning of an incident. **Important: Do not delete these rules – they must be preserved for forensic investigation.**

Take Action: Close the Employee Loophole

The number of phishing incidents, inadvertent disclosures, and cloud misconfigurations shows that employees and third-party vendors continue to cause incidents. Effective training can reduce the frequency and severity of these incidents. Because people are fallible, training is not enough and technological safety nets are needed. For incident prevention, a strong training and technology mix includes:

- ▶ **Phishing training, including test phishing campaigns, to increase awareness.**
- ▶ **Educating employees to not provide login credentials or use the same credentials for multiple sites or services.**
- ▶ **Enabling MFA throughout the entity.**
- ▶ **Deploying endpoint security agents and advanced email threat protection tools.**
- ▶ **Developing effective network segmentation.**

Overall

6%

System Misconfiguration

11%

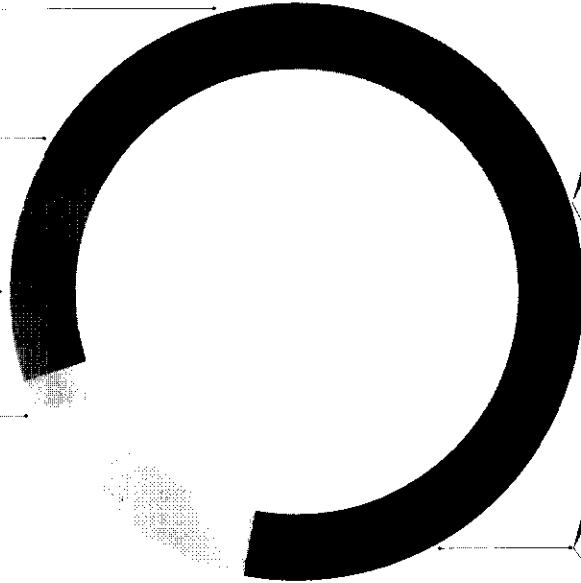
Stolen/Lost Device or Records

13%

Other

17%

Inadvertent Disclosure



Phishing Breakdown

34%

Phishing

32% Remote Access

24% Other

20% W-2 Scam

18% Ransomware

6% Automated Information Exfiltration

Network Intrusion Breakdown

19%

Network Intrusion

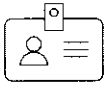
38% Ransomware

29% Other

17% Automated Information Exfiltration

16% Remote Access

Responsible Party



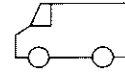
53%

Employees (includes employee error such as mistakenly providing information in a phishing scam)



31%

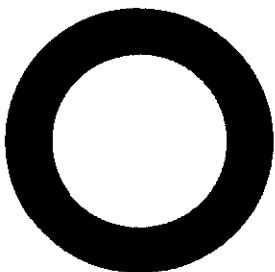
Unrelated Third Parties (e.g., security researchers)



16%

Vendors/Service Providers

Breach Discovery



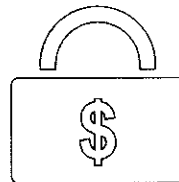
65%

of Breaches Internally Discovered

35%

of Breaches Externally Discovered

Ransomware



\$40,000

Average Payment

100% relied on vendor when payment in bitcoins requested

Timeline Provides Context for Response Expectations

When an incident occurs, entities often want to notify regulators and affected individuals as quickly as possible. However, it is critical to first take the time to contain the attack. The forensic, legal and in-house team will then work to determine who is affected, identify measures to prevent a reoccurrence, and mitigate potential harm. To help you set realistic expectations, we looked at the timing of the incident response life cycle's core elements: detection, containment, analysis, and notification.

Network Intrusion Timeline

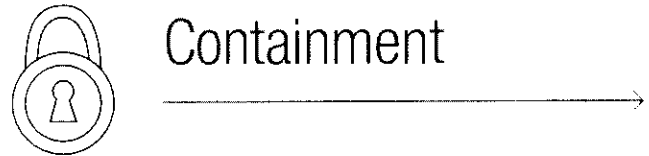
Network intrusions tend to take longer to detect and contain than other types of attacks, because multiple steps are involved. However, the timeline follows the overall pattern of other types of attacks. More than 90% of all network intrusions were detected in less than six months and contained in less than a week. More than half of all forensic investigations were completed within a month, with only 4% taking longer than three months.

Overall Incident Response Time



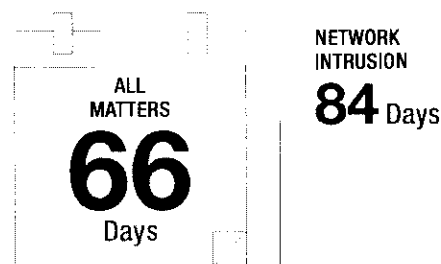
The time from initial occurrence to detection continues to be where entities have the most room to improve. Earlier detection usually means more forensic data is available, which leads to more effective mitigation efforts and more certainty about what occurred. Good logging and visibility are also critical.

Entities are more aware than ever of the importance of constant vigilance. Of the data breaches in this year's survey, 65% were detected internally. Only 8% remained undetected for more than six months, and only 4% for more than a year.

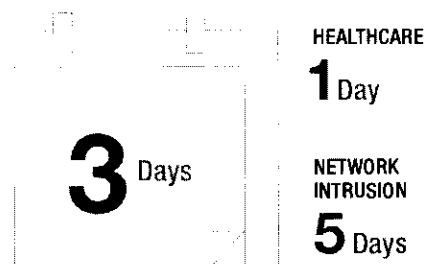


Ending the attack is critical to reducing exposure, and incident response teams continue to find faster containment strategies. Time to containment was less than a week in 97% of incidents; only 2% took more than a month to contain. Key factors in time to containment are as follows: (1) an existing relationship with a forensic firm, (2) quick access to forensic data such as logging and endpoint information, and (3) effective project management to build and execute the containment plan.

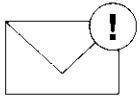
Occurrence to Discovery



Discovery to Containment



Number of Individuals Notified



AVERAGE:

87,952

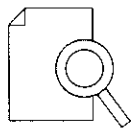
Notifications by Industry

Hospitality (Food/Beverage, Retail)	627,723
Education	46,783
Business & Professional Services	8,284
Healthcare	6,470
Finance & Insurance	3,572
Other	2,729
Nonprofit	957
Government	927
Aerospace & Defense	275

Take Action:

Keys to Shortening the Timeline

- ▶ Increase SIEM log storage to look back at incidents.
- ▶ Identify a forensic firm in advance, and conduct onboarding to speed the process later.
- ▶ Use endpoint security tools to get visibility faster.
- ▶ Be mindful that the pressure to move quickly must be balanced with the need for a complete, thorough investigation and effective containment.



Analysis

Forensic analysis is getting faster and more sophisticated, with new tools and increased personnel. This year's analysis period was shorter than last year's, with 55% of investigations completed in less than one month and 87% in less than two. Only 4% of investigations took more than three months from start to finish. Despite the understandable desire for speed, it is important to let the forensics process run its full course to determine the actual scope of the incident. Entities that rush or skip this important step and simply assume the worst-case scenario run the risk of making a broader notification than is necessary or appropriate.

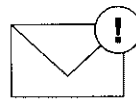
Engagement of Forensics to Completion

36

Days

HEALTHCARE
29 Days

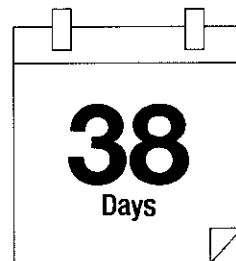
NETWORK
INTRUSION
36 Days



Notification

With local, national, and internet media continuing to make data breaches headline news, entities feel increased pressure to make notifications quickly. In response, notification times dropped in 2017. As in the past, entities are preparing to notify as close in time as possible to when a complete forensic investigation reveals who may have been affected.

Discovery to Notification



HEALTHCARE
43 Days

NETWORK
INTRUSION
45 Days

Forensics Drive Key Decisions

In the first days after an intrusion is discovered, the ability to quickly and efficiently conduct a forensic investigation is critical. A focused forensic investigation can help you answer the essential questions: What happened? How did it happen? How do we contain it? Whom do we need to tell? How can we protect affected individuals? Getting fast, accurate answers is especially important when the compromised data includes personal information that may trigger a reporting requirement.

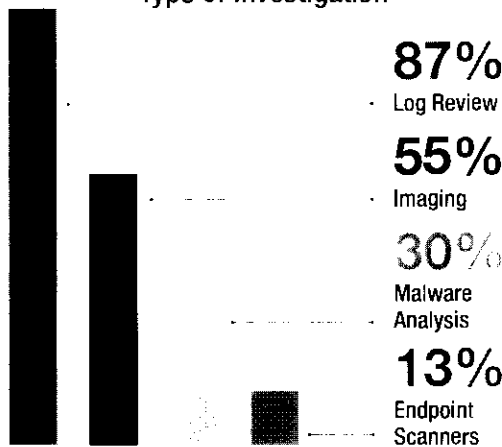
In 2017, forensics were used in 41% of intrusion incidents overall, compared with 34% in 2016, showing that entities are realizing the value of hiring outside investigators with broad experience and resources. Forensics were used in 65% of network intrusion incidents, probably due to the inherent complexity of those investigations.

Forensic investigators use a variety of tools to determine the scope of information affected and the extent of the incident. Depending on the situation, they may analyze information from an entire network, a specific application, or a particular computer, mobile device, or other endpoint. In 2017, the most frequently used tool was log review, which enables the investigator to reconstruct how data was accessed and to determine whether it was exfiltrated. It can tell you who clicked on a phishing link, and how effective your defenses are. Log

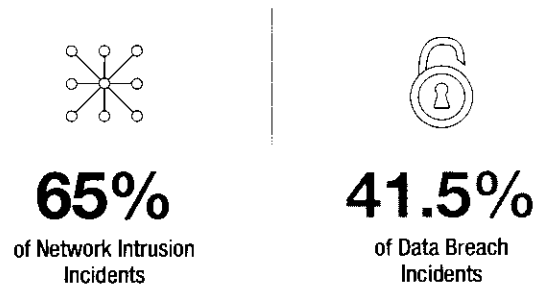
review was used in 87% of forensics investigations this year, probably due to the increase in Office 365 incidents involving attackers gaining access to different accounts. This trend further demonstrates how critical it is for entities to collect and retain robust logs in both on-premises and cloud environments.

Device imaging, used in 55% of investigations in 2017, helps evaluate servers and databases for malware and other forensics artifacts. Malware analysis, used 30% of the time, looks at the specific types of malware – where they came from, how they work, and whom they may impact. And endpoint scanners, which review activity in desktops, laptops, and point-of-sale devices, were used in only 13% of investigations, down from 28% in 2016.

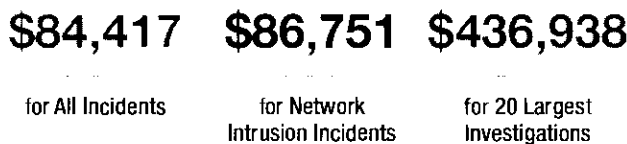
Type of Investigation



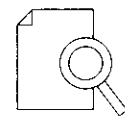
Use of Outside Forensics



Forensic Investigation Costs



Average Completion Time for Forensic Investigation



24%

Evidence of Data Exfiltration in Network Intrusion Incidents

Data at Risk*



46%
Social
Security



39%
Health
Information



26%
Other Confidential
Information
such as student ID
numbers, usernames
and passwords, and
intellectual property



24%
Birthdate



15%
Financial
Data



12%
PCI Data



10%
Driver's
License

* These amounts total more than 100% because many incidents involved multiple types of data.

Latest Trends in Forensics

Forensic investigators have been creative in developing tools that respond to new types of attacks. For example, faced with a huge jump in Office 365 intrusions, some firms have developed tools that can determine which emails were opened and which objects the attacker accessed. This information can significantly limit the scope of review, as well as the number of required notifications.

Investigating in the Cloud

Although forensic techniques and principles are generally the same in cloud investigations, cloud environments raise some special challenges. In a Software as a Service (SaaS) environment, the vendor – not the entity – controls the underlying infrastructure, including logging. Because logs are so often critical to investigations, make sure to understand a vendor's log detail, obligations, and preservation practices well in advance of an incident.

An Infrastructure as a Service (IaaS) arrangement moves some or all of an entire entity's infrastructure into a cloud environment. Forensic investigators typically cannot connect to physical machines to collect images and data. Instead, they must have processes in place to collect and analyze data in cloud environments. Some forensic firms have overcome this challenge by creating their own virtual systems with forensic tools in the cloud, which they use to connect to and analyze client storage devices.

Take Action: Choose the Right Forensic Firm

In considering whether to hire an outside forensic firm or deciding between possible firms, consider the 3Cs:

- **Capability:** What tools does the outside firm use to conduct investigations? Will its tools work in your environment? Can it quickly provide visibility to endpoints, capture network traffic, and search for current indicators of compromise? Or will it want to forensically image all devices and conduct manual analysis?
- **Capacity:** What's their – and your – bandwidth? Will the firm have a competent team available when you call? Do you have enough resources to deploy the tools, support the investigation, and carry out containment and remediation actions while still doing your day job?
- **Credibility:** Will stakeholders (e.g., regulators, customers, board members, shareholders) expect you to have engaged an external firm? And will they have confidence in the forensic firm's findings? Does the firm have experience responding to the types of incidents you are likely to face?

Even if you have preselected a forensic firm, when an incident arises you should take a close look at whether that firm is best-suited for the particular investigation. Some investigations call for a firm that can tell you exactly what attackers did within your environment. Others require specialized knowledge of a particular application or system. Consult with experienced counsel and your cyber carrier to leverage their experience – their Compromise Response Intelligence – with the options you are considering.

Regulators More Involved

In the wake of several recent high-profile incidents, regulators are taking a more aggressive role in investigating data breaches. We are seeing increases in both the number of inquiries and the speed with which the inquiries are made. No longer confined to a few active state attorneys general (AGs), investigations may be opened by any AG whose state's residents are affected. Additionally, although the number of resolution agreements has dropped, the Office for Civil Rights (OCR) continues to heavily investigate HIPAA (Health Insurance Portability and Accountability Act) compliance following breaches affecting more than 500 people, and more quickly than in years past.

Higher Budgets, Higher Stakes

Regulatory investigations are no longer just informal inquiries that seek voluntary cooperation. More and more, we are seeing agencies issue subpoena-like civil investigative demands (CIDs) that require significant effort to respond.

State AGs and other regulators, well-funded by large multistate settlements, are combining their power to compel testimony and documents with more experts to help them dive deeper into your operations than ever before. CIDs and informal letters now request not only your entity's information security plan and remediation steps, but also more burdensome technical requests, including details about your environment and its physical, technical, and administrative controls. OCR in particular has added instructions to its data requests that may change existing assumptions about how long and in what format an entity must hold and preserve data.

Outcomes of these inquiries often go well beyond the incident itself. While settlement proposals often contain a monitoring component and a corrective action plan, regulators are also beginning to issue closing letters. These letters do not support enforcement action, but contain certain findings and require the entity to acknowledge that it must comply with all statutory obligations. OCR can use this acknowledgment against the entity in a future incident. Similarly, after a complaint investigation or compliance review, OCR may negotiate a resolution agreement requiring an entity to take corrective action to comply with HIPAA. These can be far-reaching agreements that call for a systemic change in the way a state operates, or they may cover a single healthcare provider or hospital.

Size Doesn't Matter

AGs are looking beyond the number of affected residents to explore an entity's "systemic issues." Those that are slow to investigate, are slow to notify and experience repeat data incidents may be especially vulnerable.

AG Inquiries Following Notifications	
2016	2017
37	64
Non-AG Inquiries	
2016	2017
29	43
OCR Inquiries Where Notice in a Healthcare Incident Exceeded 500	
2016	2017
13	22

What an AG Wants



Incident Response Plan



Employee Training Manual



Policies and Procedures



Forensic Reports



Information on Specific Data Loss Prevention



Information on Use of MFAs

Technology Helps Protect Payment Cards

Adoption of EMV technology is making it harder to use stolen card data, and point-to-point encryption use is reducing the number of large card-present theft incidents. When they do occur, because Visa and Mastercard raised the operating expense reimbursement rates across all card types, the baseline expectation for the combined network liability assessment (recovery of operating expense and counterfeit fraud) increases. On average, the lowest expectation starts at \$4 per at-risk account. The per card assessment amount can climb to \$20 or more based on the amount of fraud that issuing banks report. Generally, larger incidents will be on the low end of the range because the percentage of cards with attributable fraud will be lower than small incidents where the attacker may be able to sell a larger percentage of the cards on a forum. American Express changed its Data Security Operating Policy (DSOP), so when it decides its DSOP applies the opening demand from American Express will be \$5 per at-risk account.

As experts predicted, EMV adoption has caused attackers to more frequently target e-commerce sites, and we saw a resurgence in these attacks. Even if a site uses tokenization, an attacker with access to the site's administrative console or checkout-page code can bypass tokenization and capture payment card data. Liability assessment programs apply to these incidents now too.

EU Update: Preparing for GDPR Notification Requirements



The EU's General Data Protection Regulation (GDPR), effective May 25, 2018, addresses personal data breach notification in Article 33 (notifying authorities) and Article 34 (notifying individuals). The harm threshold for notifying regulators is lower than the threshold for notifying individuals – notification to authorities should occur within 72 hours after the entity has “become

aware” of a personal data breach that is likely to result in a “risk to the rights and freedoms of natural persons.” By contrast, notification to individual data subjects must occur when the breach is likely to result in a high risk to the rights and freedoms of natural persons. In both cases, the risk analysis must broadly consider the confidentiality, integrity, and availability of data.

Because the GDPR's definitions of “personal data” and “personal data breach” are broader than those in the United States, a notifiable breach may be triggered by different incidents. For example, unauthorized disclosure of a list of names and addresses with religious affiliations and church attendance frequency might be perceived as threatening to the rights and freedoms of EU data subjects, but would not trigger a U.S. notification requirement.

Multinationals must plan to manage incidents that affect multiple jurisdictions, as notification under one regulatory regime could create legal risk in another. For example, providing notice to an EU regulator within the 72-hour window could prompt questions about notification timing in the United States. Incident response plans should designate a single decision-maker or a central team to manage potential conflicts. Our incident response tabletop exercises for global entities help their distributed teams take a collaborative and consistent approach to managing multijurisdictional events.

2017 Per Card Assessment Range for Operating Expense and Fraud

\$4-\$20

Credit Monitoring Offered When Notification Occurred

60%

Average Redemption

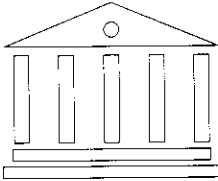
35%

Take Action:

Manage Regulatory Risk

- ▶ **Have a response plan and team in place and practice.**
- ▶ **Investigate incidents expeditiously and notify as soon as possible, ideally within 30 days of discovering the incident.**
- ▶ **Communicate a culture of transparency and compliance when responding to regulatory inquiries.**

Prepare for Privilege Challenges



Motions to dismiss and discovery defendants reduce exposure and limit the scope of discovery. In 2017, courts appeared to favor dismissing specific causes of action while allowing others to proceed. For example, in *In re: Pioneer Health Data Breach Litigation*, an Arizona federal court dismissed a claim of contract breach and implied duty of care claims, but allowed others to move forward.

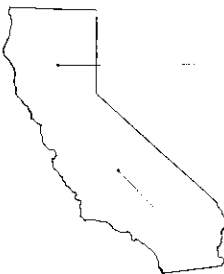
Data breach litigation is surviving motions to dismiss and proceeding to discovery, where plaintiffs seek breach investigation records and challenge defendants' assertions that the investigations are protected by various legal privileges. In 2017, three courts ruled on these challenges, with different results.

California Protects Forensics Documents

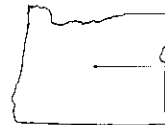
In a case involving a health insurance entity, a federal court in the Northern District of California held that the attorney work-product doctrine protected documents sent by a forensics vendor to its client. The key issue was whether the vendor created the documents in "anticipation of litigation." Although some documents had been created both to assist in litigation and to help the entity respond to the suspected incident, the court held that the "litigation purpose permeate[d] the documents" and warranted protection.

The United States District Court for the Central District of California reached a similar conclusion in a case involving a major consumer credit reporting agency. The plaintiffs argued that the forensic report and related documents were not protected by the attorney work-product doctrine because the company "had independent business duties to investigate data breaches and it hired [forensics vendor] Mandiant to do exactly that ..." But the court found that the company's duty to perform the work did not remove work-product protection. Instead, the court used a Ninth Circuit standard to analyze whether the documents were created "because of" litigation or the threat thereof. In ruling that the privilege applied, the court noted that (1) Mandiant was hired by a law firm to help it provide legal advice in anticipation of litigation; (2) Mandiant provided its report to the law firm, not to the entity; and (3) the form and content of Mandiant's report were largely dictated by the law firm's instructions.

Are Forensic Documents Protected From Discovery?



- **Northern District of California**
Work-product protection exists for documents created in anticipation of litigation, even when they also serve another purpose.
- **Central District of California**
Work-product protection exists for documents created because of litigation or the threat of litigation, despite independent business duty to investigate.



- **District of Oregon**
There is no protection for documents not prepared by or sent to counsel, documents relating to third-party work, or communications with parties not involved in the breach.

Oregon Limits the Privilege

The United States District Court for the District of Oregon reached a different conclusion. That court required the defendant to show that each document it intended to withhold was specifically "legal advice." However, the facts of that case were unique. In October 2014, the entity had proactively engaged Mandiant to conduct a forensic investigation independent of counsel, and the court scrutinized the timing and scope of that engagement in its ruling.

The court focused on the requirement for the business entity to prepare most of the documents in response to the data breach (such as press releases and customer notices) regardless of the litigation. It said the entity's intention to have an attorney review the documents, and the possibility that attorneys advised on the drafting "[do] not make every internal draft and every internal communication relating to those documents privileged and immune from discovery." To maintain the privilege, the entity had to show that the communications were sent to or from counsel seeking or providing legal advice.

Take Action: Build the Paper Trail

- ▶ **Certain work performed during incident investigation and response serves a business purpose and therefore may not be privileged. Consider the timing and language of your vendor engagements and scope of work letters.**
- ▶ **Where vendors will have dual purposes, one of which is to assist counsel in litigation, use additional engagement letters or scope of work agreements to make that purpose clear.**
- ▶ **Assume communications with PR and crisis management firms are not privileged. Act and write accordingly.**
- ▶ **Consult with the litigation team early to develop a privilege strategy for confidential communications.**
- ▶ **Remember that privilege fights happen months or years after a communication is created. Develop a labeling strategy for privileged documents and emails that will streamline litigation review.**

Use Compromise Response Intelligence to Minimize Risk

Any entity, of any size, may find itself the victim of a cyberattack. Criminal organizations and security researchers constantly scan the internet for vulnerabilities and poorly configured systems. If your systems and data are exposed to the internet, it's only a matter of time before an attacker will target you.

While new threats continue to appear, the incident preparation and response landscape has not changed dramatically from prior years. Our recommendations from previous years still hold true, and we have added some new ones to reflect developing threats and updated strategies.

PREVIOUS RECOMMENDATIONS ARE STILL CRITICAL

1 Increase awareness of cybersecurity issues.

In particular, employees must receive training and education on the dangers of phishing emails and what they look like.

2 Identify and implement basic security measures.

- Segregate subnetworks that contain sensitive and valuable data from other parts of the network.
- Disable or harden remote desktop access on internet-facing systems.
- Ensure that patch management procedures are in place and critical patches are installed in a timely manner.
- Remove administrative rights from normal users, and limit the number of privileged accounts.
- Implement a web proxy that can block access to untrusted websites.
- Utilize threat intelligence and endpoint protection tools.
- Deploy endpoint monitoring and an intrusion detection and prevention system.
- Aggregate logs from critical sources into an SIEM tool, and configure properly tuned, real-time alerts.

- Retain logs for at least one year, preferably longer.
- Prohibit access to personal email accounts from the entity's network.

3 Create a forensics plan.

You can't protect what you don't understand. Create and maintain accurate network diagrams, device inventories, and data maps to ensure that the internal IT team knows your entity's environment. The plan should also address internal procedures and tools for collecting and preserving forensic evidence, and identify pre-vetted forensic firms and those for which a master service agreement is in place.

4 Build business continuity into your incident response plan.

With ever-growing ransomware and distributed denial of service (DDoS) attacks, business continuity should be built into your incident response plan and tested.

5 Manage your vendors.

Vendor incidents are still occurring. It is critical to know your vendors and how they operate. You must understand what data is being shared, how it is being secured, and what happens if the vendor has an incident. Explore what logs your vendor maintains, what level of detail they provide, how long they are retained, and your ability to access those logs to investigate an incident.

6 Combat ransomware.

The best defense against a ransomware demand is a full and complete backup that is readily available. Creating a Bitcoin wallet in advance and prefunding it can minimize impact if backups are unavailable; however, there are other considerations that need to be addressed before creating a wallet. Most entities engage a forensic firm with a funded Bitcoin wallet.

7 Purchase the right cyber insurance policy.

Look for risk management services and guidance from your carrier in addition to a solid policy, appropriate limits, and claims experience.

NEW RECOMMENDATIONS KEEP YOUR RISK POSTURE CURRENT

8 Implement a strong, top-down risk management program.

- Your entity's information security posture starts at the top. Unfortunately, senior executives are often the most vocal opponents of enhanced security measures. It is imperative for executives at the highest level to be "all in" and constantly project the importance of information security.
- Conduct a comprehensive risk assessment as the basis for your risk management program. This will help you identify and reduce legal risk in your information security practices, respond to regulatory and legal challenges, and focus information security resources on the most critical risk scenarios.
- Entities in every industry should look at the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies. Even if your entity is not covered by this regulation, experts believe it may be the model for future state or federal cybersecurity regulations.

9 Adopt updated password guidance, and implement MFA or other risk-based authentication controls.

Authentication by username and password alone can no longer protect sensitive information or secure remote access to network resources and third-party providers. This is true for several reasons. First, outdated guidance on password complexity and rotation (now updated) has inadvertently trained users to create bad passwords and share them across sites and services. Second, attackers have preached so many large stores of username and password combinations

that billions of breached password records are now in the public domain. Third, attackers use simple tools to automate so-called credential-stuffing attacks, in which attackers use these stolen password databases to brute-force their way into poorly protected services and sites.

As with any good security solution, this problem calls for a layered approach tailored to your entity's risk scenarios and tolerance:

• Adopt updated password guidance.

Consider updated password policies to match recent guidance published by the National Institute for Standards and Technology (NIST) and Microsoft, which eliminates complex, hard-to-remember passwords and arbitrary password-rotation rules in favor of rules that (1) encourage longer, easier-to-remember "memorized secrets"; (2) check proposed passwords against the corpuses of known breached passwords; (3) implement protections (like rate limiting) that mitigate brute-force attacks; and (4) rotate passwords only if there's a good reason to do so (e.g., password database stolen, password phished).

• Use strong MFA or other risk-based authentication controls.

To mitigate phishing, credential-stuffing attacks and password reuse scenarios, implement strong MFA controls using software- or hardware-based tokens. Entities concerned about the business impact of full MFA can consider risk-based controls that require additional authentication steps only when suspicious activity is detected. Besides being a good security practice, MFA and other advanced authentication methods are on regulatory agencies' radars.

Consider implementing these controls in any scenario involving (1) remote access to email (on-premises or in the cloud); (2) remote access to network resources through VPN; (3) remote

access to cloud resources, including third-party SaaS providers that handle sensitive information like HR or payroll data; and (4) login pages to customer-facing web applications containing sensitive data or processes.

10 Keep data secure in the cloud.

Migrating to the cloud is a great step to increase your entity's data security, but it doesn't mean you can let up on other security measures. Data in the cloud is more secure in some respects, but it is still vulnerable if the entity's overall security posture is weak. When considering a cloud solution, work with your risk management team to ensure that its security model works with your program.

Understand the shared-responsibility model, and ensure that you are doing your part to secure and monitor your data in the cloud. Different uses of the cloud – IaaS, SaaS or PaaS – carry different security obligations. All cloud deployments should be approved by management after being screened for security implications, and secured by personnel with the training and experience to secure data in cloud environments.

11 Prepare for more regulatory inquiries.

- Because of recent settlements between regulators and entities, regulators have more funds to investigate entities that suffer data breaches. As a result, expect more regulatory inquiries, including formal inquiries in the form of CIDs, and more extensive requests for information.
- Because of greater regulatory scrutiny as well as the potential for litigation, think strategically about the timing and language in investigation vendor engagements and scope of work

letters/documentation, especially when engaging existing vendors to assist with an incident investigation. Attorney-client and work-product privileges may not protect all communications.

- Focus on complete and timely remediation following an incident. Regulators want to know you have taken significant steps to prevent another incident from occurring.

12 If you are a publicly traded entity, update your Item 1A Risk Factors regarding privacy and security.

Based on the Securities and Exchange Commission's guidance on cyber risk factors, entities generally disclose three categories of risks: (1) operations/business resiliency – the entity relies heavily on technology to run the business, and if the technology fails, then there may be impact; (2) a data breach risk – what cyber risks the entity may face on a going-forward basis, and what material cyber incidents have already occurred; and (3) privacy/security regulatory compliance – the ability to adapt and comply with new laws as they are enacted and modified globally. Review your risk factors and ensure that these areas are covered.

Risk Assessments: An Essential Guide

Risk assessments are a critical foundation for any information security program. They help satisfy regulatory requirements, demonstrate a commitment to cybersecurity and suggest where to invest limited security resources. In fact, risk assessments have proven so valuable that many standards and regulatory frameworks now require them (HIPAA's Security Rule, the Payment Card Industry Data Security Standard [PCI DSS], NIST, and the New York Department of Financial Services Cybersecurity Requirements, to name a few).

Many entities, however, still do not incorporate true risk assessments into their information security planning, often because of confusion about what a risk assessment is – and is not.

- **A risk assessment identifies threats, vulnerabilities, likelihood and impact.** Risk assessments are often confused with other risk-management tools, such as vulnerability assessments, penetration tests and red-team exercises, compromise assessments, gap analyses, and compliance audits. These are valuable tools, but they do not accomplish the purposes of a true risk assessment. Indeed, they may be rejected by regulators evaluating an entity's compliance with risk assessment requirements.
- **A risk assessment prioritizes and tailors recommendations to a particular entity.** To be useful, a risk assessment must do more than merely catalog an entity's vulnerabilities. Nor can it base its recommendations on generic risk ratings that ignore environment, culture, and risk appetite. Rather, the assessment must tie known vulnerabilities to the threats and attack scenarios most likely to affect the entity.
- **A risk assessment is an ongoing process.** Entities often err by treating a risk assessment as a point-in-time compliance exercise. In fact, it's a continuous process of reflection and improvement. As part of its risk assessment program, an entity should establish a committee or group to meet regularly to evaluate emerging threats and vulnerabilities.
- **A risk assessment focuses on the entire entity, not just information technology.** True risk assessments evaluate all aspects of security management programs, including vendor-management policies and procedures, security awareness training programs, staffing and competence of security engineers and compliance officers, incident response programs, and the management structure of security teams.

About BakerHostetler

To receive an electronic version of this report, please visit bakerlaw.com/DSIR

BakerHostetler has more than 940 lawyers in 14 offices, and is widely regarded as having one of the leading data privacy and cybersecurity practices. Our attorneys have managed more than 2,500 data security incidents for some of the world's most recognized brands. Our Privacy and Data Protection team's work extends beyond incident response and is one of the largest of its kind. In addition to privacy and data breach issues, we handle regulatory compliance, GDPR and other cross-border issues, marketing and advertising, eDiscovery, regulatory, and class action defense.

To learn more about how to prevent, prepare for, or manage a data breach, contact BakerHostetler.

Editor in Chief **Craig Hoffman**

Chicago
T +1 312 593 0391
choffman@bakerlaw.com

Janine Anthony Bowen

Atlanta
T +1 404 919 9910
jbowan@bakerlaw.com

David A. Carney

Cleveland
T +1 216 891 3530
dcarney@bakerlaw.com

Teresa C. Chow

Los Angeles
T +1 310 919 3438
tchow@bakerlaw.com

Casie D. Collignon

Denver
T +1 303 751 4007
ccollignon@bakerlaw.com

William R. Daugherty

Houston
T +1 713 646 1321
wdaugherty@bakerlaw.com

Gerald J. Ferguson

New York
T +1 212 685 4196
gferguson@bakerlaw.com

Amy E. Fouts

Atlanta
T +1 404 919 8411
afouts@bakerlaw.com

Alan L. Friel

Los Angeles
T +1 310 412 6863
afriel@bakerlaw.com

Randal L. Gainer

Seattle
T +1 206 461 1811
rgainer@bakerlaw.com

Lisa M. Ghannoum

Cleveland
T +1 216 891 3430
lghannoum@bakerlaw.com

Linda A. Goldstein

New York
T +1 212 685 4006
lgoldstein@bakerlaw.com

Patrick H. Haggerty

Chicago
T +1 312 489 4117
phaggerty@bakerlaw.com

John P. Hutchins

Atlanta
T +1 404 919 9919
jhutchins@bakerlaw.com

Edward Jacobs

New York
T +1 212 685 4610
ejacobs@bakerlaw.com

Laura E. Jehl

Washington, D.C.
T +1 202 691 1588
ljehl@bakerlaw.com

Andreas T. Kaltounis

Seattle
T +1 206 461 1080
akaltounis@bakerlaw.com

Paul G. Karlsgodt

Denver
T +1 303 761 3611
pkarlsgodt@bakerlaw.com

David E. Kitchen

Cleveland
T +1 216 891 3330
dkitchen@bakerlaw.com

Theodore J. Kobus III

New York
T +1 212 671 1064
tkobus@bakerlaw.com

M. Scott Koller

Los Angeles
T +1 310 919 8437
mskoller@bakerlaw.com

Aaron R. Lancaster

Washington, D.C.
T +1 202 361 1501
alancaster@bakerlaw.com

Melinda L. McLellan

New York
T +1 212 685 4610
mclellan@bakerlaw.com

Holly A. Melton

New York
T +1 212 685 4006
hmelton@bakerlaw.com

Eric A. Packel

Philadelphia
T +1 215 361 1001
epackel@bakerlaw.com

Lynn Sessions

Houston
T +1 713 646 1337
lsessions@bakerlaw.com

James A. Sherer

New York
T +1 212 685 4270
jsherer@bakerlaw.com

James A. Slater

Cleveland
T +1 216 891 3430
jslater@bakerlaw.com

Paulette M. Thomas

Chicago
T +1 312 691 3380
pmtomas@bakerlaw.com

Daniel R. Warren

Cleveland
T +1 216 891 3415
dwarren@bakerlaw.com

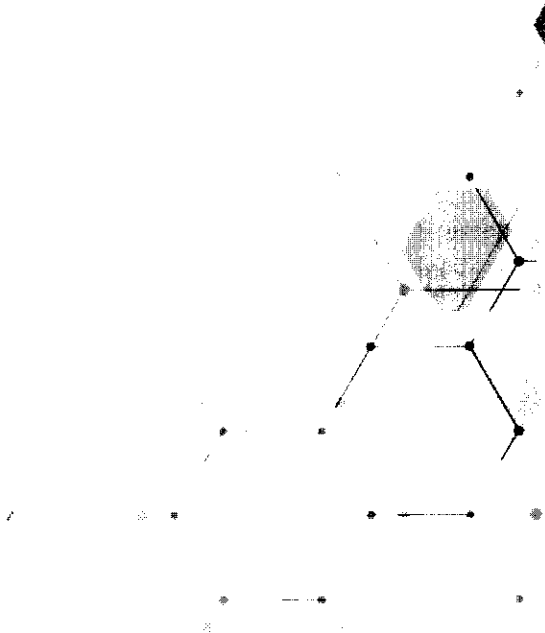
Christopher A. Wiech

Atlanta
T +1 404 919 9414
cwiech@bakerlaw.com

BakerHostetler

bakerlaw.com

To receive an electronic version of this report,
please visit **bakerlaw.com/DSIR**



Cybersecurity: Risks and Safeguards for the Business Litigator

Jeffery K. Brandt

Jackson Kelly PLLC

Monica Minkel, RPLU, MLIS

USI Mountain

Daniel C. Nelson, C|EH, CIPP/US

Armstrong Teasdale, LLP

CONTENTS

A Glossary	1
Common Types of Attacks	3
Drive by download	3
Malware	3
Phishing	3
Ransomware	3
Social Engineering	3
Spearphishing	4
Trojan horse	4
Virus	4
Zero-Day Vulnerability	4
Overview of Security Principles	5
The CIA Principle	5
Multi-Layered Security	6
Prevention	6
Detection	6
Containment	6
Remediation	6
Overview of Security Control Types	7
Administrative	7
Technical	7
Physical	7
Cyber Insurance Overview	8
Why bother?	8
What's the risk?	8
Who offers cyber insurance?	8
What types of coverage are available?	8
Components of cyber insurance	9
Cybersecurity Basics Checklist	10
Top 10 Things to Ask Your IT Department	11

A Glossary

The IT team has many terms that, to the uninitiated, can sound confusing. But, a basic understanding of these terms greatly assists in productively working with IT.

A **computer network or data network** is a group of interconnected computers. The primary components of a network are “Clients” and “Servers.” The computers are connected using either wired (today, often fiber) or wireless connections. Interestingly, the internet is in fact just a giant network.

A **client** is generally considered to be a device that allows everyday users to work with within a network. A laptop or desktop connected to a network is a “client,” as is your cellphone when interacting in a network. In security discussions, clients are often referred to as “endpoints.”

Cloud computing, is essentially to process of taking pieces of the network out of a company’s server room, and putting them into a data center where they are managed and controlled by others. Thus, instead of your laptop communicating over an internal network with a server in your server room, your laptop is communicating over the internet with a server in a data center someplace else. From a security perspective, Cloud Computing is not necessarily more secure than traditional on-premise networks, but rather presents a different set of security challenges.

Data loss prevention (DLP) software is designed to detect unauthorized movement of your data. DLP monitors data while it is being used, while it is being transmitted, and where it is stored. DLP systems can alert the company to unauthorized movement of data, can block that unauthorized movement, and log who, when and where data is being viewed or taken.

A **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. **Network firewalls** are generally software running on a dedicated computer that protects a network or part of a network. **Host-based firewalls** are software that controls traffic in or out of a single machine.

The **Internet of Things** (IoT) is the network of physical objects – devices, vehicles, buildings and other items – embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

An **intrusion detection system** (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations. IDS is an important security

component because it is a given that intruders will breach your outer walls (such as firewalls). Being able to detect the presence of hackers inside your network assists in containing, eradicating and remediating the damage. Given that the average time a hacker spends inside a network prior to detection (what the industry calls “dwell time”) is over 200 days, it is critical that successful intrusions are swiftly located and the damage is correspondingly limited.

The **National Institute of Standards and Technology (NIST)** is a non-regulatory agency of the United States Department of Commerce. NIST provides a comprehensive library of cyber security protocols, programs and directives which are increasingly becoming the norm for both government and private industry.

A **penetration test**, informally called a pen test, is an intentional probing of a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data. Typically, a penetration test is requested by the owner of the computer system to determine potential security vulnerabilities. Penetration tests can include attempts to breach the physical security of a building or office.

Risk assessments are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. Risk assessments generally identify the following elements: threats that could harm and adversely affect critical operations and assets; vulnerabilities that these threats can exploit, and potential resulting impacts to an organization if the threat exploits the vulnerability. Risk assessments can also include developing an action plan based on the identified risks. A “risk assessment” is not the same process as a “penetration test” or an audit or gap analysis all of which are designed to find potential weaknesses in your security program. Thus, a good security plan includes performing both a risk assessment and pen tests, audits and other security assessments.

A **router** is a networking device that forwards data, contained in data packets, between computer networks. Routers perform the “traffic directing” functions on the Internet. A router is connected to two or more data lines from different networks (as opposed to a network switch, which connects data lines from one single network).

A **server** is really just a central computer that functions in the background to provide services to clients. The email server, for example, is a computer that coordinates the sending, receipt and storage of email among clients. Increasingly, traditional on-premises servers are being replaced by “The Cloud.” But, “The Cloud” is really just a server that is maintained by someone else to provide the functionality that used to reside in a company’s on-premises servers. Typical servers are database servers, file servers, mail servers, print servers, web servers, game servers, and application servers.

“**Virtual machine**” or “**Virtualization**” refers to a “computer” which is created within another computer using special software. As an example, a normal laptop computer can be equipped with software which creates many distinct “virtual computers” which all exist within the physical confines of the single laptop. These virtual machines can each act as a separate computer, and would appear, to those interacting with the virtual machine, generally

indistinguishable from a separate physical computer. Much of modern computing, and cloud computing in particular, is built on the use of virtual machines.

Common Types of Attacks

Drive by download

The automatic loading of malware on a user's computer when they visit an infected website. While the risk of a drive by download is highest when visiting some of the shadier or more off-color parts of the internet, hackers have managed to compromise prominent websites and use them to infect visitors with drive by attacks.

Malware

Short for malicious software, malware is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malware generally propagates by attaching itself to an existing program or other executable content. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency.

Phishing

Phishing is a common form of social engineering where the hacker attempts to get something from the victim by means of a false communication. Common examples would include a forged email from a bank asking the user to "log on" and provide account usernames and passwords. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by using spoofed emails or through instant messaging, and it often directs users to enter details at a fake website whose look and feel are virtually identical to the legitimate one.

Ransomware

Ransomware restricts access to the infected computer system in some way, and demands that the user pay a ransom to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive. Once encrypted, these files are generally impossible to decrypt without paying the ransom for the encryption key. Ransomware typically infects a computer by disguising itself as, or hiding within, a legitimate file, such as an email attachment.

Social Engineering

The process of convincing humans to take some action the hacker desires. Examples include convincing the front desk receptionist to allow the hacker access to non-public office areas, or convincing the company's HR director to send a file containing employee social security numbers to a fake "payroll" company. Phishing and Spearphishing are two of the most common forms of social engineering. As technical controls have improved, social engineering is

becoming increasingly common as a core part of attacks. Put simply: security technology becomes smarter every day; users do not. Humans are by far the weakest link in the security chain.

Spearphishing

A subset of phishing attacks, where the phishing attack is directed at specific individuals or companies. The attackers use more personal information in their attack to convince the victim that the message is legitimate.

Trojan horse

A "Trojan" is any malicious computer program which generally acts as a backdoor, allowing hackers to remotely access a computer as if they were physically at the keyboard. A Trojan is one of the worst forms of malware that can infect a computer.

Virus

A virus is a small program that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an email note or in a downloaded file, or be present on a flash drive or data storage device. The immediate source of the email note, downloaded file, or storage device you've received is usually unaware that it contains a virus. Some viruses wreak their havoc as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer.

Zero-Day Vulnerability

Also known as "zero-hour" or "0-day," a Zero-Day is a disclosed computer-software vulnerability that hackers can exploit to adversely affect computer programs, data, additional computers or a network. It is known as a "zero-day" because once the flaw becomes known, the software's author has zero days in which to plan and advise any mitigation against its exploitation (for example, by advising workarounds or by issuing patches).

Overview of Security Principles

The CIA Principle

Many people think of "Security" as synonymous with "Confidentiality." Focusing on confidentiality alone will leave one vulnerable to many other harmful threats. Security pros use the "CIA Triad": Confidentiality, Integrity and Availability.

Confidentiality

Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" (ISO27000). It is roughly equivalent to privacy and is a set of rules that limit access to information. Cryptography and encryption methods are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

Integrity

Integrity is the property of maintaining and assuring the accuracy and completeness of the information. This includes ensuring that the information cannot be modified in an unauthorized or undetected manner. An example of an attack on information integrity would be to intercept the data during transmission and modify it before it reaches the intended recipient.

Availability

Availability is the property of allowing authorized users access to the information. Information must be available to authorized users when they want access to it. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. Examples of attacks on the availability of information include ransomware and denial of service attacks.

Multi-Layered Security

Many people think of security as being about “prevention,” or “keep them out.” Unfortunately, cybersecurity is about much more than just higher or thicker walls. The simple fact is that “they” are going to get in. Good security doesn’t stop at the perimeter, but instead is comprised of four equally-important elements:

Prevention

Prevention includes the “walls,” which may be physical or logical. It also includes planning and understanding: where is the data, what are the risks, and what are the security priorities. Awareness and training are just as important as the other barriers employed.

Detection

Average attack “dwell time” – the time “they” are inside a network before discovery – is over 200 days. That’s a lot of time to do a lot of damage. Using technology and vigilant users to detect intrusions more quickly is a key security component.

Containment

“Inside the network” doesn’t have to mean “inside the entire network.” Good system architecture, the use of containment technology, and good planning can keep a small intrusion from becoming a major disaster.

Remediation

Even with fire codes, sprinkler systems, and fire retardant materials, the fire department is still busy. Stuff happens, and responding quickly and appropriately, with the right assets, can be the difference between a stove top incident and burned-down house. Planning, practice, and the right tools to respond and to fix (including risk sharing tools like insurance and indemnification) are a core part of a good security posture.

Overview of Security Control Types

Solid cyber security requires the implementation of three different types of protection (most often referred to as “controls”): administrative, technical, and physical controls.

Administrative

Administrative controls are the policies, processes and procedures required to promote security. They tend to be things that employees may do, or must always do, or cannot do. Examples of administrative controls include password requirements, the escalation procedure to be used in the event of a break-in (i.e., who is notified first, second, and other steps taken) and the list of steps to be followed when a key employee is terminated (i.e., disable their account and change the server password). Administrative controls are vitally important, but frequently the most overlooked component of cyber security.

Technical

Technical controls are those controls implemented through technology. Examples of technical controls include firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). For many organizations, their technical controls may be stronger than their administrative and physical controls, reflecting the misunderstanding that cybersecurity is only a function of purchasing security equipment.

Physical

Physical controls prevent physical access to locations, such as non-public office areas. Physical controls can also include physical access to critical systems, such as generators or electrical substations. Examples of physical controls range from physical keys, key cards, and retinal recognition systems, to security gates, walls, and man traps.

Cyber Insurance Overview

Why bother?

As cyber incidents continue to explode, the insurance industry has repeatedly been stuck with expensive, unplanned-for claims under various types of insurance (CGL, Property & Casualty, etc.). The industry's response has been to exclude coverage for cyber-related incidents from most traditional policy forms, and instead sell separately-underwritten cyber insurance. Thus, it is increasingly likely that, absent a cyber policy, your loss will not be covered by insurance.

What's the risk?

While there is some variation in the data, the most authoritative estimates for the cost of lost personal data are over \$200 per lost record. So, a loss of 5,000 records (which many would call a "minor" breach) could be a \$1,000,000 problem. Moreover, these costs do not scale linearly: smaller breaches are significantly more expensive on a per-record basis than larger incidents.

Even incidents which don't involve data theft are becoming increasingly costly. In our increasingly-networked world, loss of access to information, or factory downtime when computer-controlled machines go silent, can quickly result in significant business interruption damages.

Who offers cyber insurance?

Almost all of the major liability carriers offer cyber insurance policies. But, there is no "standard" policy, and coverages, exclusions, and definitions vary considerably and materially between carriers. It is imperative that you work with a broker who has specific and demonstrable experience and expertise in cyber insurance, as there are many brokers who have sold the wrong coverage simply because they don't truly understand the risks or the product.

What types of coverage are available?

Generally, **first party** and **third party** coverages.

First party coverage generally compensates for costs, damages and losses suffered "internally" by the organization. Examples include forensic costs to investigate a possible incident, and data breach response costs to notify and protect your customers. Business interruption coverage is an often-overlooked, but potentially important, first party coverage. With the rise in ransomware, extortion coverage is an increasingly valuable first party coverage.

Third party coverage generally compensates for losses incurred with respect to third party claims. Examples would include defense costs in data breach litigation, and regulatory penalties.

Components of cyber insurance

While different carriers define coverages in different ways, it is often helpful to think of coverage components in terms of **Errors & Omissions, Network Security, Media** and **Privacy**.

Errors & Omissions coverage generally applies when your cyber product or service fails to perform, and causes damage to a third party.

Network Security coverage may provide first and/or third party coverage for network security failures (other than data breaches).

Media coverage generally provides third party coverage for intellectual property infringement and defamation.

Privacy coverage provides first and/or third party coverage for data breach incidents.

Cybersecurity Basics Checklist

Know the Types of Data You Possess and Where it is Stored

- Understand the types of data you possess, including who owns it, why it is in your possession, and how long you need to keep it
- Understand what information is confidential, sensitive, or subject to legal requirements
- Understand how and where information is being stored

Conduct a Risk Assessment

- Understand the relative likelihood and impact of various risks to your data

Routinely Assess Physical and Technical Safeguards

Awareness, Awareness, Awareness (and a little bit of Training)

Prepare a Breach Response Plan

- Create a detailed playbook for responding to incidents of varying severity
- Identify an incident response team and assigns clearly a defined role to each team member
- Identify a breach coach (with emergency contact information)
- Identify contractors/third parties (with emergency contact information) who will be a part of the incident response team

Conduct Table Top/Mock Event Exercises

- Ensure team members understand the plan and their roles before an incident occurs

Develop a Culture that Values Security

- Train employees and contractors about the importance of security
- Reward compliant behavior
- Follow up on mistakes with targeted training

Top 10 Things to Ask Your IT Department

Do we have a data map?

Most organizations don't truly know where all their information is: who is touching it, where it is stored, and how it travels. If your organization has not undertaken a formal survey to "map" the organization's information, it is very likely that there are information stores, and information uses, which security has not identified. And if security doesn't know they exist, they can't be secured.

When was our last information risk assessment?

There is simply not enough time or money to completely secure against every possible risk. Absent a risk assessment, decisions on allocation of time and funds will not efficiently correlate with those risks most likely to impact the organization.

Have we adopted a cybersecurity framework?

A good cybersecurity framework provides the overall structure for the implementation of various security plans. Absent a framework, the organization likely lacks a cybersecurity program, but instead pursues a number of potentially un-coordinated projects.

When was our last penetration test?

Every cybersecurity program needs to be *regularly* pressure tested to find potential holes.

Do we have somebody in a dedicated security role?

Even if it's only a part-time position, somebody needs to take specific day-to-day responsibility for security. The bad guys work 24/7; your security needs to be just as constant.

Do you perceive that anyone outside the IT Department is regularly involved in security activities?

Most of your cybersecurity incidents will arise from outside of IT's domain. Good security starts with direct and meaningful senior management sponsorship, and includes HR, operations, legal, and other "non-IT" personnel as essential players.

Do we have a designated Cyber Incident Response Team?

An organization without a designated Cyber Incident Response Team is like a city without a fire department.

Do we have a defined process to determine when, and to whom, security incidents should be reported?

Your organization will face thousands of potential incidents each year. The vast majority do not require senior management involvement (or even knowledge). But, how does IT know when you need to know?

Have we practiced incident response?

No fire department, army, or doctor would ever think of operating in a crisis environment without first practicing. Your incident response team should prepare for crisis the same way.

What policies would you like to see implemented to enhance security?

Password, information use, and similar policies – we call them “administrative controls” – are one leg of the three-legged security stool. Have you ever tried to sit on a one-legged stool?

AN ACT concerning business.

**Be it enacted by the People of the State of Illinois,
represented in the General Assembly:**

Section 5. The Personal Information Protection Act is amended by changing Sections 5, 10, and 12 and by adding Section 40 as follows:

(815 ILCS 530/5)

Sec. 5. Definitions. In this Act:

"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or

subject to further unauthorized disclosure.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) Social Security number.

(2) Driver's license number or State identification card number.

(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(Source: P.A. 94-36, eff. 1-1-06.)

(815 ILCS 530/10)

Sec. 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope

of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the

breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject

persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(d) Notwithstanding any other subsection in this Section ~~(e)~~, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(Source: P.A. 94-36, eff. 1-1-06; 94-947, eff. 6-27-06.)

(815 ILCS 530/12)

Sec. 12. Notice of breach; State agency.

(a) Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall

include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(a-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the State agency with a written request for the delay. However, the State agency must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(b) For purposes of this Section, notice to residents may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the State agency demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to

be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the State agency has an email address for the subject persons; (ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and (iii) notification to major statewide media.

(c) Notwithstanding subsection (b), a State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.

(d) If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

(Source: P.A. 94-947, eff. 6-27-06.)

(815 ILCS 530/40 new)

Sec. 40. Disposal of materials containing personal information; Attorney General.

(a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.

(b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:

(1) Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.

(2) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.

(c) Any person disposing of materials containing personal information may contract with a third party to dispose of such

materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

(d) Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than \$100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed \$50,000 for each instance of improper disposal of materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

(f) A financial institution under 15 U.S.C. 6801 et. seq. or any person subject to 15 U.S.C. 1681w is exempt from this Section.

You've been hacked! Now what?

Presented by:
Judge Lynn M. Egan (Ret.)
Trent Walton CCE, ACE

BREAKING NEWS
HACKED!



Judge Lynn M. Egan

- Cook County Circuit Court Judge, 19 Years
- Member of Illinois Supreme Court Committees
 - Civil Justice Committee
 - Education Committee
 - (Former Member): Executive Committee, oversees all Illinois Supreme Court committees
 - (Former Member): Discovery Procedures Committee, now Civil Justice Committee
- Authored articles on
 - Discovery, requests to admit, restrictive covenants, Day-In-The-Life films, directed verdicts, jury selection and instructions, Dead Man's Act, Supreme Court Rule 213, expert witnesses, reconstruction testimony, court-ordered medical exams, attorney-client/work product privileges, sanctions and damages
- Bar Association committees and Boards of Directors
- Registered CLE provider through the Illinois MCLE Board
 - Awarded over 10,000 hours of CLE credit to Illinois attorneys
- Prior to joining bench
 - Argued before the Illinois Supreme Court: Cisarik v. Palos Community Hospital



Trent Walton CCE, ACE

- Sedona Conference – Member
 - Working Group on Electronic Document Retention and Production (WG1)
 - Brainstorming Group on Information Governance
- Computer Cybersecurity, Forensics & eDiscovery
 - Certified Computer Examiner (CCE)® #684
 - Certified AccessData Examiner (ACE)®
 - Licensed Private Investigator #PI1.0000371
 - Certified in Windows Forensics by AccessData
 - Certified Electronic Discovery Specialist
 - Certified in eDiscovery Software Products ranging from ECA through Review
 - Served as Expert in issues ranging from Computer Forensics to Complex eDiscovery Matters
- Software Development
 - Created E.L. Native Review™ for Concordance, Rated 4.6 out of 5 by TechnoLawyer Publication
 - Acquired by Wave Software, 2010
 - Created eCloudCollect™, now DataCollectPro™
 - Acquired by ZApproved 2014

CYBERSHIELD U.S.

855-CYBERUS



“Give me an example of how a hacker can access an attorney’s email account.”

FORTUNE

May 18, 2016

LinkedIn Lost 167 Million Account Credentials in Data Breach

A Russian hacker, who goes by "Peace," is selling 117 million email and password combinations on a dark web marketplace, Vice Motherboard reports. The going rate for the loot is five Bitcoins, or about \$2,300.

CYBERSHIELD U.S.

855-CYBERUS



Example of Email Exploit Workflow

Download Credentials Database

Filter Emails by Domain

Locate Email Server

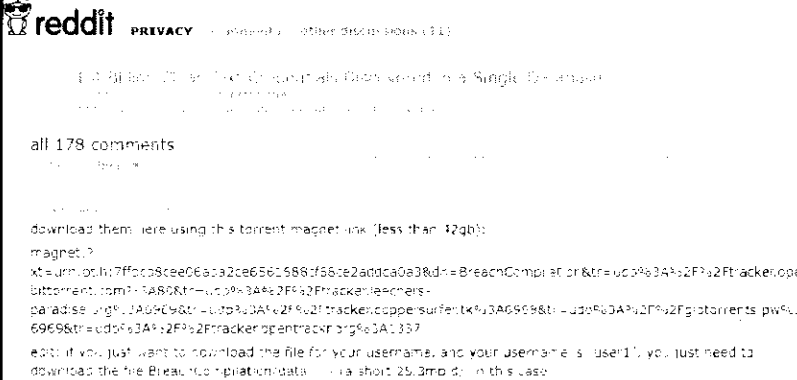
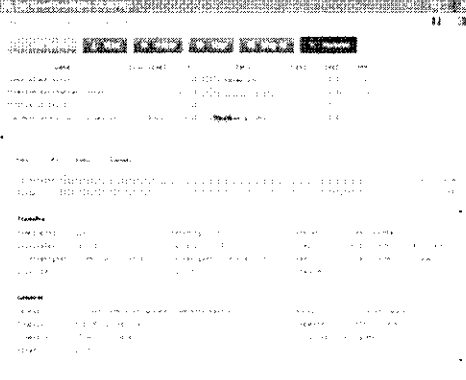
Attempt Logins

Successful Login

CYBERSHIELD U.S.

855-CYBERUS

Step 1: Get Credentials List

Download
Credentials
Database

Filter Emails
by Domain

Attempt
Logins

Exploit
Account

CYBERSHIELD U.S. 855-CYBERUS

Step 2: Filter by Law Firm Domains

law.com

birkland.com

bakermckenzie.com

skadden.com

dlapiper.com

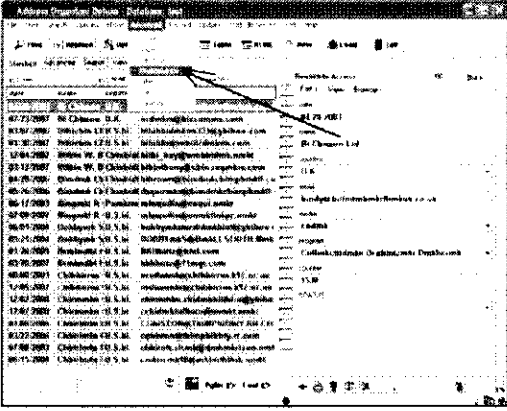
jacobson.com

sidlay.com

hoganlovells.com

morganlewis.com

nortonrosefahbright.com



Download
Credentials
Database

Filter Emails
by Domain

Attempt
Logins

Exploit
Account

CYBERSHIELD U.S. 855-CYBERUS



Step 3: Locate Email Server

Pref	Hostname	IP Address
5	mail.woon.com	192.171.1.100 B&W TDM - Communications Group LLC - 4819018
5	mail.woon.com	192.171.1.100 B&W TDM - Communications Group LLC - 4819018
5	mail.woon.com	192.171.1.100 AT&T Services, Inc. - 481118
5	mail.woon.com	192.171.1.100 Dajem Communications - 48174

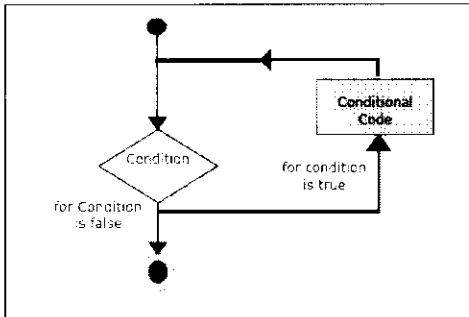


CYBERSHIELD U.S.

855-CYBERUS



Step 4: Attempt Logins

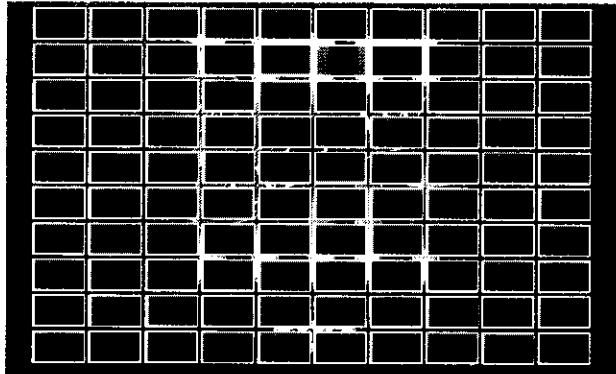


CYBERSHIELD U.S.

855-CYBERUS



Compromised Email Study



- AMLaw 100 email focus
 - 100 emails per firm
- Find credentials from past breaches
 - Use law firm email
- 96% of firms had ≥ 1 compromised account
- 48.5% of accounts had associated passwords
 - Of 96 firms with >1 compromised accounts

CYBERSHIELD U.S.

855-CYBERUS



What Can a Hacker Do With Email Access?

- Wire fraud
- Phishing co-workers and clients using trusted email
- Access to confidential information
- Insider trading
- Intellectual property
- Extortion
- Case insight
- Damage reputation

CYBERSHIELD U.S.

855-CYBERUS



Illinois Rules of Professional Conduct

- **Rule 1.1 – Competence.** *Comment 8.* “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...”



Illinois Rules of Professional Conduct

- **Rule 1.6 – Confidentiality of Information.** (a) “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) or required by paragraph (c).” (e) “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.”
- *Comment 18:* Reasonableness is judged by: sensitivity of the information, likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards and the extent to which safeguards adversely affect the lawyer’s ability to represent clients (e.g., software that is excessively difficult to use).



Illinois Rules of Professional Conduct

- **Rule 5.1 Responsibilities of Partners, Managers, and Supervisory Lawyers.** (a) "A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." (b) "A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct."





Illinois Rules of Professional Conduct

- **Rule 5.3 Responsibilities Regarding Nonlawyer Assistance.** (b) "A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."
- Comment 2: "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."



Law Firm Data Breaches

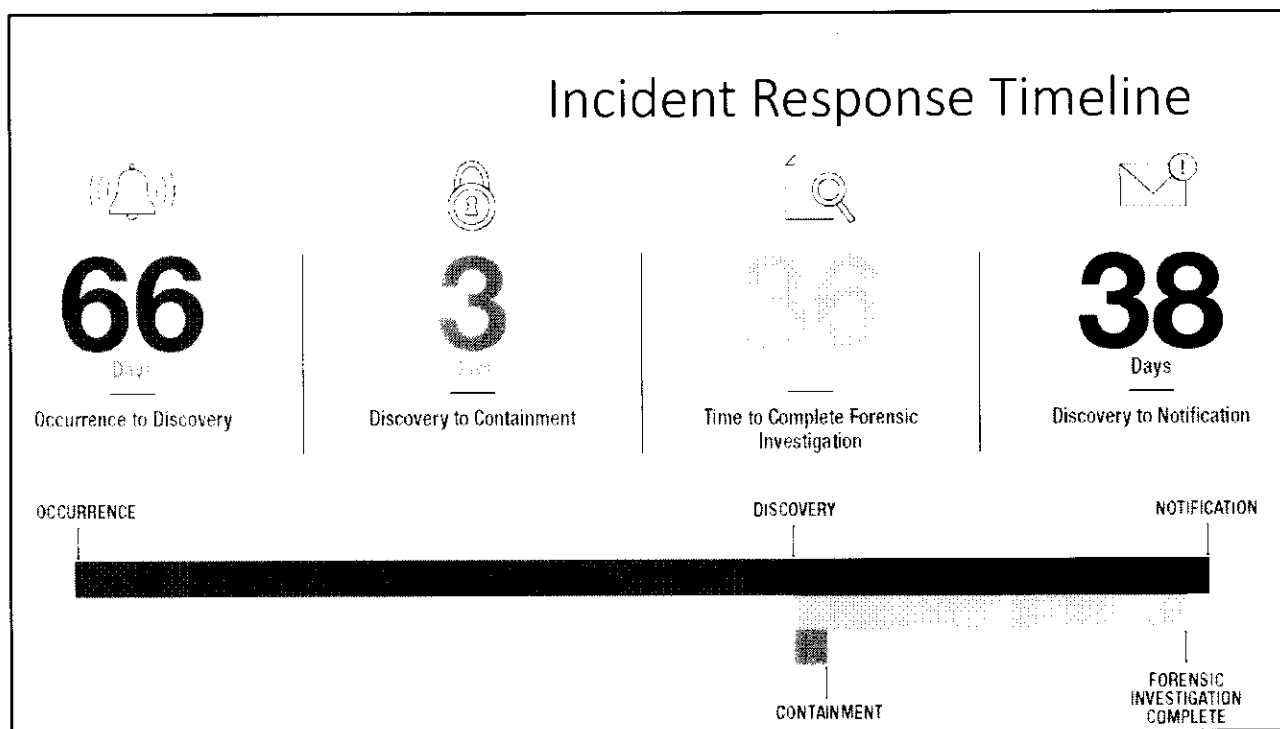
CYBERSHIELD U.S. 855-CYBERUS



Law Firm Vulnerability

- 2016 Compromise Assessment found 40% of firms had a data breach and didn't know
- 2017: ABA's 2017 *Legal Technology Survey Report*, firms that reported experiencing a breach:
 - 2-9 Lawyers: 27%
 - 10-49 Lawyers: 35%
 - > 500 Lawyers: 25%
- 2018: Nearly 1 million UK law firm associated email passwords available on the dark web – 80% includes passwords

CYBERSHIELD U.S. 855-CYBERUS



Why? Motives

- Wire-Fraud, closing funds
- Access to confidential information
- Insider trading
- Money, extortion
- Intellectual property
- Case insight
- Access to clients
- Access to additional data

855-CYBERUS

CYBERSHIELD U.S.

How? Techniques Used

SOCIAL ENGINEERING

CYBERSHIELD U.S. 855 CYBERUS

M|R
MOSES RYAN
ATTORNEYS

160 Westminster Street, Suite 400, Providence, RI 02903
tel: 401.453.3600 fax: 401.453.3904

**Ransomware:
Moses Ryan**

- 10-Attorney Law Firm in RI, 2016
- Attorney clicked on email attachment
- Down for three months
- Paid ransom twice totaling \$25k
- Lost \$700k in billable revenue over three months.
- Insurance paid \$20k, policy limit

WE GET THE JOB DONE

ME...TORY CONTACT

*Fram: The Office of The State Attorney
<com_department@outlook.com>
Date: Wed, Feb 14, 2018 at 10:37 AM
Subject: The Office of The State Attorney Complaint
To: Bar Member*

Dear Bar Member:

A complaint has been filed against your Business.

Enclosed is a copy of the complaint which requires your response. You have 10 days to file a rebuttal if you so desire.

You may view the complaint at the link below.

complaint889417.pdf

Rebuttals should not exceed 15 pages and may refer to any additional documents or exhibits that are available on request.

The Office of The State Attorney cannot render legal advice nor can The Office of The State Attorney represent individuals or intervene on their behalf in any civil or criminal matter.

Please review the enclosed complaint. If filing a rebuttal please do so during the specified time frame.

Sincerely,

The Office of The State Attorney

Theorizing how
it could of
happened?
Phishing Exploit
Example

855-CYBERUS



Case Study: Targeted Law Firm Attack

- Targeted firms representing major banks and Fortune 500
- “[Targeted] email accounts of law firm partners working on mergers and acquisitions”
- “.. Using a law firm employee’s credentials, the defendants installed malware on the firm’s servers to access emails...”
- Over 94 days hackers reconnected downloading different data
- Hackers made > \$4M with insider trading

**WEIL
GOTSHAL**



Cravath, Swaine & Moore LLP

Cravath

CYBERSHIELD U.S.

855-CYBERUS



DocuSign

Secure | <https://ssymarecords.com/inputs/16e/DC/0/g/lead/>

DocuSign

Em

Hello.

Please click on View Document to electronically view your document in your email.

Make sure to read all pages of the document.

If you wish to contact us, please call us at [REDACTED].

We appreciate your business.

Sincerely,

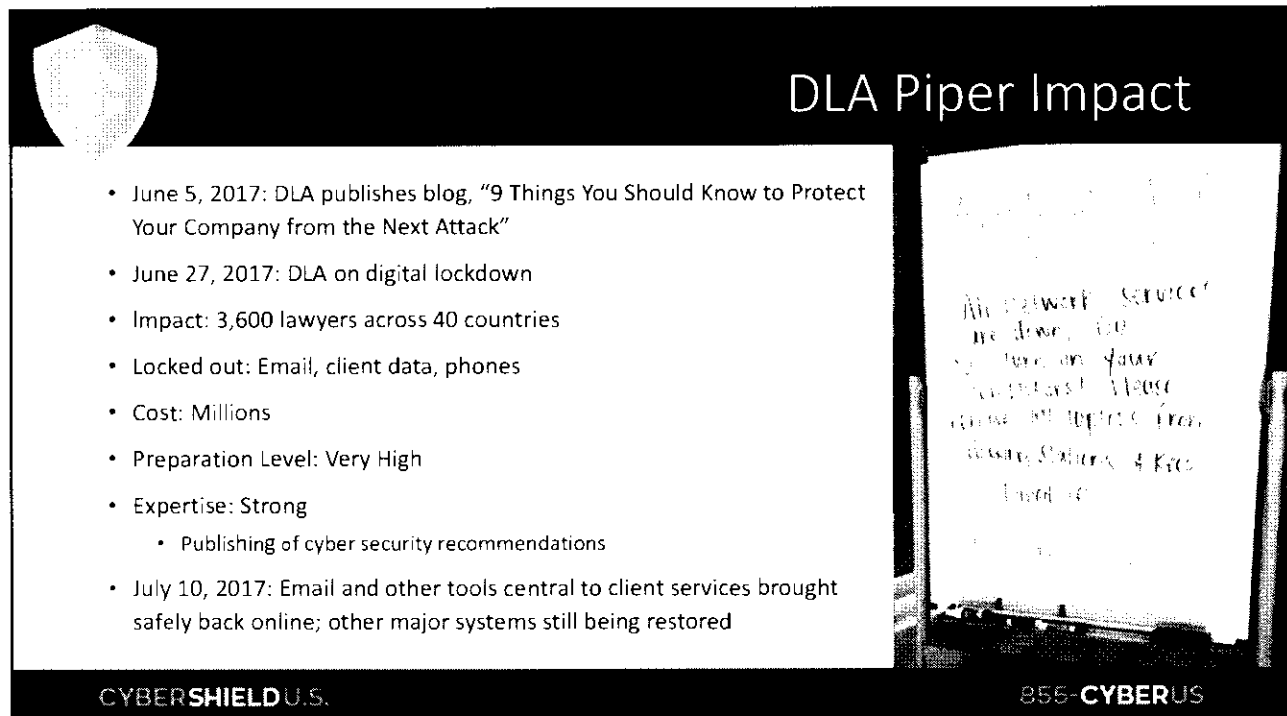
[REDACTED] - Attorney at [REDACTED]

PASSWORD: [REDACTED]

Powered by DocuSign

ACCESS ENCRYPTED FILE(S) WITH YOUR EMAIL

- Microsoft Account
- Office365
- AOL
- Yahoo!
- GoDaddy
- Google



DLA Piper Impact

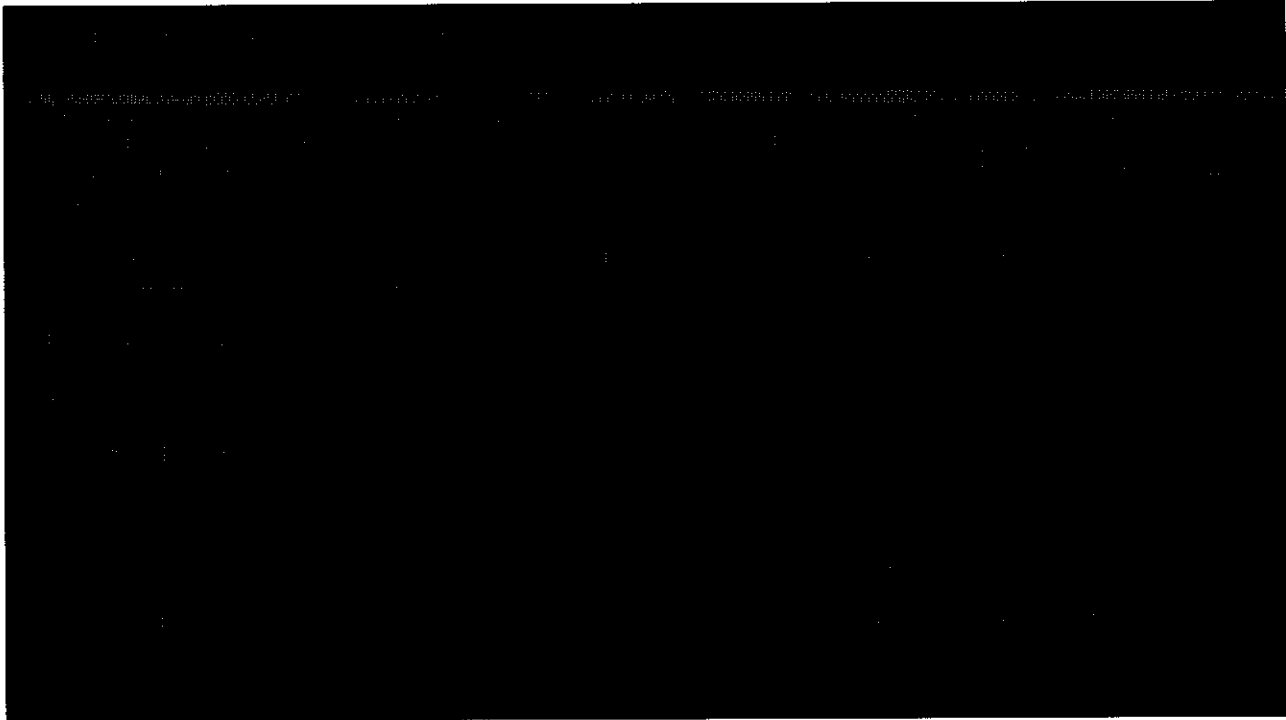
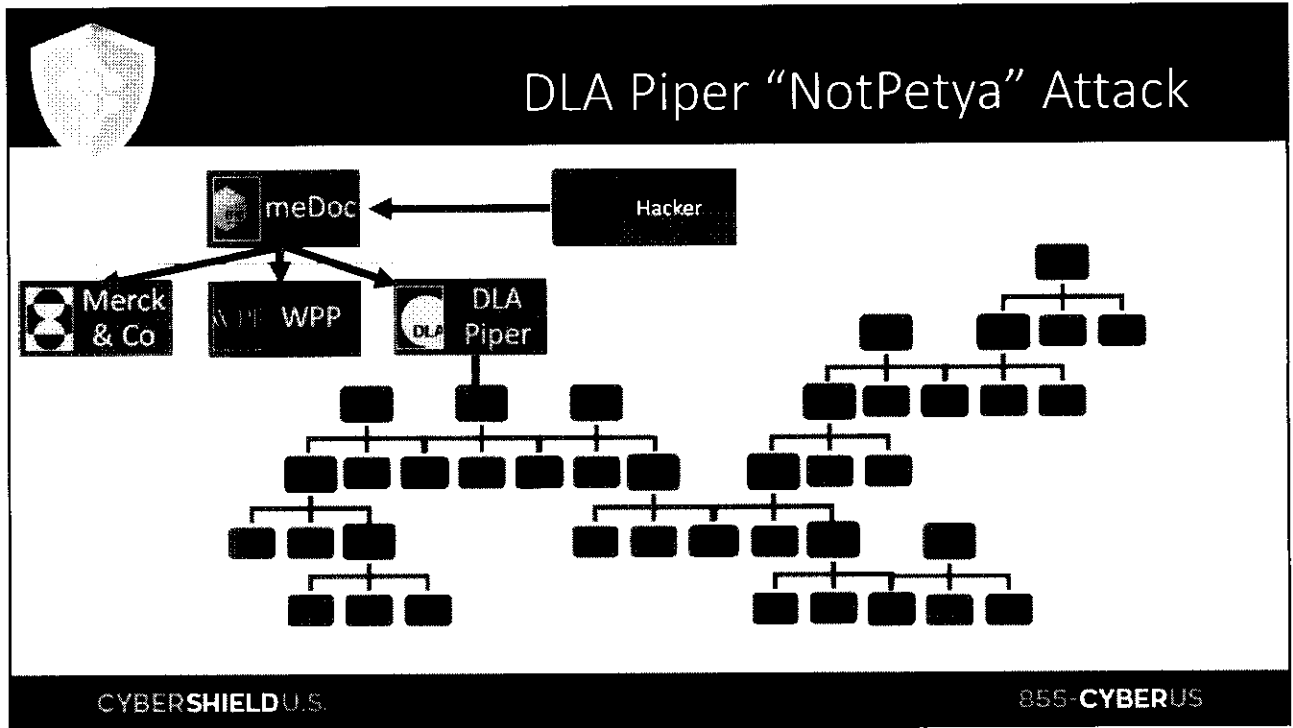
- June 5, 2017: DLA publishes blog, "9 Things You Should Know to Protect Your Company from the Next Attack"
- June 27, 2017: DLA on digital lockdown
- Impact: 3,600 lawyers across 40 countries
- Locked out: Email, client data, phones
- Cost: Millions
- Preparation Level: Very High
- Expertise: Strong
 - Publishing of cyber security recommendations
- July 10, 2017: Email and other tools central to client services brought safely back online; other major systems still being restored

Handwritten notes on whiteboard:

All network services are down. Do not turn on your computers. Please remove all laptops from network. Station 4 Key Level 10

CYBERSHIELD U.S.

855-CYBERUS





Data Breach Costs

- Incident response, investigation
- Lost billables
- Lost work product, client data
- Stolen client information
- Breached attorney/client communication
- Third party litigation
- Loss of clients
- Attorneys depart from firm

CYBERSHIELD U.S.

855-CYBERUS

Cyber Attack Operational Preparation

- Early stage fact finding
- Red-flag review
- Gap analysis
- Development of incident response plan
- Implementation
- Technology support
- Training
- Incident response
- Insurance





Cyber Attack Technical Preparation

- Secure SMB and RDP
- Patch all possible machines, identify and isolate the ones you can't
- Protect endpoints
- 3-2-1 backup strategy
- Compromise assessment
- Security assessment
- MFA: Multi-Factor Authentication
- Network/Systems Logging (Faster Investigation)
- Vet your vendors

CYBERSHIELD U.S.

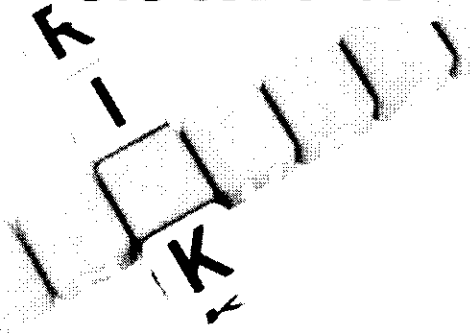
855-CYBERUS



Cyber Liability Insurance

Monica Minkel

303-831-5103



- Media Liability
- Security & Privacy Liability
- Regulatory Defense and Penalties
- Breach Response Costs
- Reputational Damage and Business Income
- Network Asset Protection
- Cyber Extortion
- Cyber Terrorism
- Cyber Crime/Social Engineering

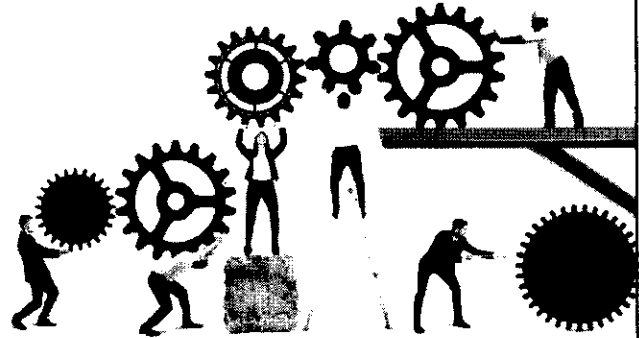
CYBERSHIELD U.S.

855-CYBERUS



Cyber Attack Response

- Contact internal and external counsel
- Notify insurance provider
- Contact a cybersecurity firm
 - Best to have pre-arranged
- Contact law enforcement
- Report to regulator if required
- Communicate to employees
- Disclose to clients
 - Different notification laws per state



CYBERSHIELD U.S.

855-CYBERUS



Tips for Personal Data Security

- Unique passwords
 - LastPass
- Multi-factor
 - Google Authenticator
- Use anti-virus
 - Avast, Windows Defender
- Backup Data
 - Dropbox, Google Drive
- Keep software up-to-date
- Stay away from free wifi
- Avoid phishing attacks



CYBERSHIELD U.S.

855-CYBERUS

You've been hacked! Now what?

Presented by:

Judge Lynn M. Egan (Ret.)

Trent Walton CCE, ACE



SHIELD



Compromise Assessment (Threat Hunting)

Trent Walton
720-878-3913

twalton@cybershieldus.com