ALFA Cyberattack Simulation:

Lessons for Data Breach Preparedness and Response

ALFA Business Litigation Section
May 18, 2017

Carl N. Kunz, III (Chuck), CIPP/US
Morris James LLP

Devin J. Chwastyk, CIPP/US
McNees Wallace & Nurick LLC

The New Reality

Why Should We Be Concerned About Data Privacy and Cybersecurity?

- Data Loss
- Exposure to Identity Theft
- Exposure to Financial Loss
- Exposure to Reputational Damage
- Business Interruption

Increasing Client/Customer Demands

- **Demanding Protection**
- **Want to know information is safe**
- **Want indemnity agreements**

- **Want to see vendor agreements**
- **Want to review insurance policies**
- **Want to know you have a plan**
  - Doc retention, breach response

Costs Of Data Loss and Breaches

- **IBM & Ponemon Institute: *2016 Cost of Data Breach Study: Global Analysis*:**
- **The average cost paid for each lost or stolen record:**
  - **Globally $158**
  - **US Avg. $221**
  - **Healthcare $355**
  - **Education $246**
  - **Financial $221**
  - **Retail $172**
  - **Industrial $156**
  - **Transportation $129**
- **Avg. Total Cost of Breach for the 383 survey participants:**
  - $4 million

Welcome to Bullz-Eye Corporation!

Bullz-Eye is a (wholly-fictional) manufacturer of darts, dart boards, lawn darts, pool tables, shuffleboard courts and other games and merchandise focused on customer-to-target interaction.

Bullz-Eye has a manufacturing plant in Exeter, Pennsylvania, and subsidiaries that operate retail locations throughout the U.S. and overseas.

Meet Bullz-Eye's CEO

Today the audience steps into the shoes of the Chief Executive Officer of Bullz-Eye, Dorothy Spot.

On this Thursday morning, Dot Spot enjoyed a relaxing breakfast with her husband, Mark.

She and their son, Fletcher, had time for a quick game of Pin-The-Tail-On-The-Donkey before Fletcher met his school bus.

That Dreaded Phone Call

The Spot family's tranquil morning is interrupted by an urgent call from Dot's assistant, who tells Dot that she has been unable to login to her work computer.

Dot rushes to Bullz-Eye's offices, only to find that every employee arriving at work has been greeted by the following message on their computer screens:

What Dot sees on her screen:

Discussion Topics

- What has happened to Bullz-Eye's computer systems?
- Has Bullz-Eye been "hacked" or suffered a "data breach"?
- What should Dot do first?

What has happened to Bullz-Eye's computer systems?

- **Ransomware**
  - Malware that limits access to the affected computer system until a ransom is paid to the "hackers"
  - Delivered by "malware" – email attachments or corrupt internet links
  - Ransomware encrypts the files using an algorithm that is difficult or impossible to crack

Has Bullz-Eye been "hacked" or suffered a "data breach"?

Types of potential data exposure events:

Electronic intrusions:

- Hacking (unauthorized access to a network)
  - Malware
    - Phishing/Spear Phishing (spoofing of a trusted site/sender
  - Ransomware
- Skimming (POS attacks)

Physical loss of control:

- Theft or loss
  - Unencrypted hardware
    - Laptops, hard drives, backup tapes, mobile devices
  - Paper records
- Employee error/negligence
  - User name/password on a Post-It note
  - Email sent to the wrong recipient
  - Insecure shredding or disposal
- Vendor error/negligence

What should Dot do first? What options come to mind?

- **Pay the ransom?**
  - Relies upon “honor among thieves”
  - Frustrates law enforcement; encourages more crime
  - Typically, modest Bitcoin ransom demands
    - Criminals make payment an attractive option
- **Contact law enforcement?**
  - FBI and other agencies may have seen the virus before and could help

What should Dot do first?

Does Bullz-Eye Corporation have a Data Breach Response Plan?

What should Dot do first?

- Data Breach Response Plans
  - Designate key decision makers, including board of directors, key employees, inside legal, outside counsel, IT staff, and IT forensic consultants
    - Identify and include outside counsel and IT consultants in advance to preserve privilege throughout any incident response
  - Provide a decision tree addressing: contacting outside counsel; investigating and remediating the breach; determining notification obligations; documenting response steps; contacting law enforcement; addressing public relations

- Data Breach Response Plans
  - Five Stages For Data Breach Response
  1. **Verification of the breach**
     - Forensic investigator to conduct forensic investigation
  2. **Containment and mitigation**
  3. **Investigation and analysis**
     - Qualified security assessment
  4. **Notification of required parties**
     - State data breach notification laws
     - Coordinate with FBI, Secret Service, and local police
  5. **Post-response review to improve processes**

Dot refers to Bullz-Eye's breach response plan:

- **Dot immediately calls a meeting of Bullz-Eye's breach response team:**
  - CEO, General Counsel, Director of Information Technology, Outside Counsel
- **The IT Director informs her they have been unable to determine the full effect of the malware program**
  - Outside counsel retains the pre-selected IT forensics consultant to diagnose the malware

The Good News:

- **Bullz-Eye's IT consultant quickly recognizes this ransomware program as a common variant**
  - The consultant images the affected computers for investigation (internal and by law enforcement)
- **Bullz-Eye reports this incident to the FBI**
  - The FBI is able to provide the consultant with additional information about this ransomware variant
  - The encryption key is publicly available

The Good News:

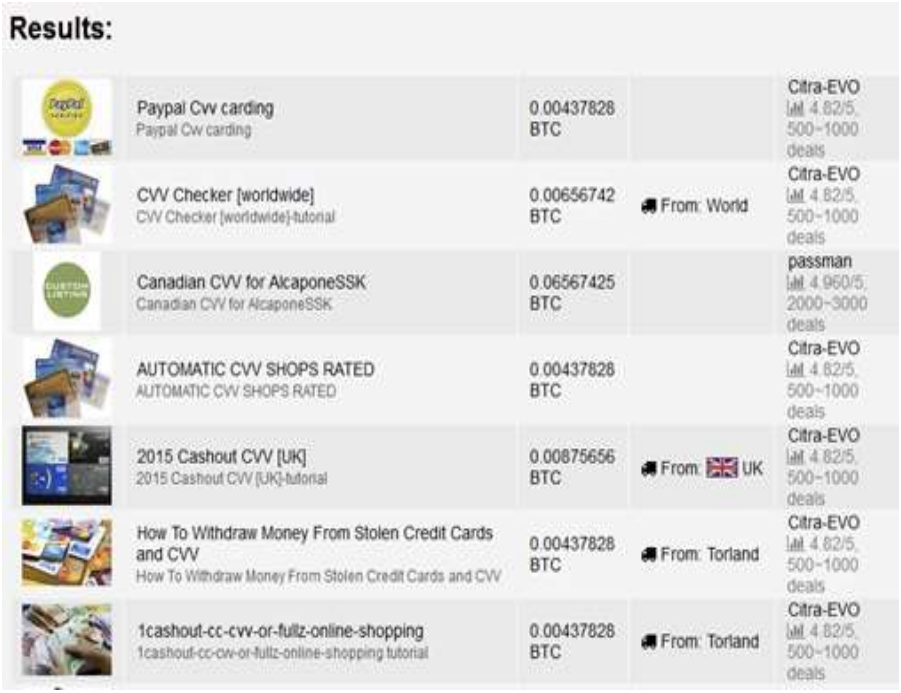
After a business interruption of only a few hours, Bullz-Eye is able to resume regular operations without paying the ransom.

The Bad News:

- The IT consultant reports that, in addition to the ransomware element, the malware contained a rootkit, which allowed the hackers administrator access to the network
- The hackers viewed some of Bullz-Eye's files, and it appears they may have transferred data to an IP address in Kazakhstan

Why would hackers want to steal this information?

- **A list of products/services offered in the principal black markets:**
  - Credit card information
    - CVV (name and address, card number, expiration date, and CVV2): less than $10
    - Dumps: magnetic stripe information: $20-80
  - Fullz
    - Name, address, credit card information, social security number, date of birth, and more: $100
  - Paypal/Ebay account records: $2 and up



- Source: InfoSec Institute

What should Dot do after finding out data may have been taken off Bullz-Eye's system?

- **Containment and mitigation**
  - Ensure that the outflow of information has been stopped and any holes in the company's data security have been plugged
- **Investigation and analysis**
  - Determine what files may have been accessed/viewed/stolen
  - And determine what types of information are contained in those files
- **Notification of required parties**

What should Dot do after finding out data may have been taken off Bullz-Eye's system?

- **Bullz-Eye's in-house IT staff and IT forensic consultants are able to determine that the hackers accessed and stole:**
  - Personnel files, containing names and Social Security numbers used to issue tax forms to Bullz-Eye's employees
  - Customer files, containing names and email addresses for individual customers
    - Including email addresses collected by Bullz-Eye's European subsidiary and transferred to the main office in the U.S.

What should Dot do after finding out data may have been taken off Bullz-Eye's system?

- **Additionally, it is determined that the hackers gained access to the network through the fire protection system in Bullz-Eye's warehouse**
  - The vendor who runs that system failed to install the latest software patch, leaving Bullz-Eye's network unsecure
  - Further, additional malware files are discovered laying dormant, many of which were attached to emails opened by Bullz-Eye's own employees

Was the stolen information protected by law?

- **In the U.S., Personally Identifiable Information ("PII") is generally defined as:**
  - First name, or first initial, and last name of an individual in combination with:
  1. SSN;
  2. Driver's license number or state ID number;
  3. or, financial account, debit, or credit card number in combination with security code or password

- **Outside the U.S., "Personal Information" is defined more broadly:**
  - Any information relating to an identified or identifiable natural person
    - "Direct" or "indirect" identification, *i.e.*, Bob Smith, or the lawyer who lives in the 100 block of Pine Street
    - Broadly drawn to encompass website cookies, IP addresses, factors specific to physical, physiological, mental, economic, cultural or social identity
  - "Sensitive personal data" afforded extra protection:
    - Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life

Is Bullz-Eye going to be prosecuted or sued for failing to protect customer and employee information?

- **Dot meets with her lawyers, and asks:**
  - What obligations do we have to notify our employees and customers that their information may have been stolen by hackers?
  - Could we be sued?
  - What legal liability might Bullz-Eye face because of this data breach?
    - **And, might we be indemnified for any such liability?**

What privacy laws might apply to Bullz-Eye's breach?

1. **State data breach notification laws**
2. **State data security requirements**
3. **Federal Trade Commission – unfair trade practices**
4. **Federal laws (industry specific)**
   a. HIPAA/HITECH Act (health care providers/insurers)
   b. Privacy Act and Federal Information Security Management Act (public sector)
   c. Family Educational Rights and Privacy Act (educational institutions)
   d. Gramm-Leach-Bliley Act (financial institutions)
5. **Payment Card Industry Data Security Standard (PCI-DSS)**
6. **Approximately 109 foreign data privacy laws and regulations**
   a. Examples:
      1. GDPR and Privacy Shield (EU)
      2. Data protection regulations (European states)
      3. PIPEDA (Canada)
7. **Contractual liability**

Does Bullz-Eye have to notify its customers that their information was exposed?

- **State data breach notification laws**
  - No generally applicable federal data security laws
  - 47 states, plus D.C. and Puerto Rico, have laws requiring an entity that maintains, stores or manages computerized data to provide notice of any breach of the security of the system to any resident of the state whose unencrypted and unredacted personal information was accessed and/or acquired or is reasonably believed to have been accessed and/or acquired by an unauthorized person.

- **State data breach notification laws**
  - Notable variances between state laws require careful examination of law in each state of residence of affected persons
  - When is notice required? Reasonable belief of breach or harm-based requirement?
  - How long does the entity have to provide notice?
  - Must AG's office be notified?
  - What information must be included in the notice?

Could Bullz-Eye have broken any other state laws?

- **Beyond notification laws, some states impose affirmative data security requirements on entities collecting personally-identifiable information of their residents**
  - At least 12 states—Arkansas, California, Connecticut, Florida, Indiana, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas and Utah—have imposed broader data security requirements
  - Many impose obligations to dispose of physical and electronic records when no longer needed for business purposes by burning, shredding, erasing
  - Some states impose general requirements that organizations implement "reasonable safeguards" (e.g., California)
  - Massachusetts requires organizations implement a WISP (written information security program)
    - Plan must address 10 specific topics including with regard to use of vendors and employee discipline
    - Imposes specific technical requirements, including access controls, firewalls, encryption, and training
  - New York Department of Financial Services in October issued new regulations applicable to banks, insurers, and vendors who contract with those entities

Was any credit card information accessed or stolen?

- PCI-DSS (Payment Card Industry Data Security Standards)
- Industry regulation (VISA, MasterCard, Discover, AmEx, JCB)
  - Requires organizations that handle credit/debit cards to conform to security standards and follow testing/reporting requirements
  - Applies to merchants, payment processors, POS vendors, financial institutions
  - Entities that fail to comply face fines ($5,000 - $25,000), increases in transaction fees, and revocation of authorization to accept credit/debit transactions

- PCI-DSS Requirements:
  - Build and maintain a secure network
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

What about Bullz-Eye's European customers?

- GDPR requires notice and valid consent for all data collected (opt-in only; consent may be withdrawn)
  - In case of a data breach:
    - EU data authorities must be notified "immediately" of a breach;
    - Individuals must be notified if an "adverse impact" is determined;
    - No *de minimis* exception
- Sanctions from warning to fines up to the greater of $20m EUR or 4% of annual global gross income
  - GDPR provides for extraterritorial enforcement; jurisdictional questions are certain to arise

Can Bullz-Eye be sued for this breach?

- Any publicized data breach is a target for plaintiffs' lawyers and class action litigation
  - Claims for negligence, breach of implied contracts, violations of state privacy laws, misrepresentation
  - Offer of credit monitoring will not avoid lawsuits
- The key issue is standing: have the class members suffered some cognizable harm?
  - Mere fear of future harm? Or real financial impact?

- U.S. Supreme Court decisions:
  - **Clapper v. Amnesty International USA: 2013 ruling by U.S. Supreme Court regarding challenge to government wiretapping**
    - Plaintiff's contention that communications likely would be intercepted in the future was not sufficient to establish standing
    - Alleged injury was hypothetical, future harm vs. injury-in-fact
  - **Spokeo Inc. vs. Robins: 2016 decision regarding FCRA claim with no consequential harm, only statutory violation**
    - An "injury-in-fact" must be both concrete and particularized

Can Bullz-Eye be sued for this breach?

- Post-*Spokeo,* courts have struggled to interpret "injury-in-fact"
  - Some courts have found that alleged "imminent threat of identity theft" is insufficient to sue
  - Other courts have found harm not speculative where data has been stolen by criminals even where no actual misuse has happened
  - Allegations of "tangible harm" (fraudulent charges, fees, costs of identity monitoring) have been more successful
  - *Spokeo* not a "magic bullet" for defendants: in 3 months post-*Spokeo*, 32 decisions addressed standing and 22 allowed the case to proceed
- A finding of standing in a class action can result in significant liability
  - *In re: Target Data Breach Litigation*: court found consumers had standing; Target quickly settled out for $10 million with consumer class and more than $50 million with Visa/MasterCard issuing banks
  - Estimated that Target spent $300 million on breach response and litigation costs
- Widening federal circuit split (6th, 7th, and 9th Circuits recognize future identity theft as an injury; 1st, 3rd, and 4th Circuits have rejected mere allegations of future harm
- U.S. Supreme Court may be forced to revisit the issue in upcoming terms

Could the government come after Bullz-Eye for failing to protect personal information?

- **FTC v. Wyndham: (August 2015)**
  - Repeated hacking of Wyndham Hotels' system had exposed the personally identifiable information (including payment card information) of more than 619,000 consumers, resulting in more than $10.6 million in fraud
  - FTC alleged this failure amounts to an "unfair or deceptive act or practice" under FTC Act
  - Wyndham argued it was mere negligence
- **Third Circuit holding:**
  - A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.
  - Upheld FTC standing to bring enforcement actions
  - New standard: 20-year duration consent orders with FTC monitoring of data security and privacy practices

Did Bullz-Eye have a privacy policy or other agreement to protect the data?

- By agreement, a party can obligate another to safeguard information provided in the course of their contractual relationship
  - Parties can also contractually place limitations on liability for a data breach
  - In commercial contracts, assignments and limitations of liability can conform to cyber insurance coverage
- For consumers, a company's outward-facing privacy policy governs the company's collection, storage, and use of consumer data
  - Lawsuits (including class actions) have alleged the failure to protect data deprives the customer of the "benefit of the bargain," entitling the customer to a partial refund of price/fees paid for goods/services
    - Such claims do not require the customer to show actual harm resulting from the exposure of their data

Post-incident Review

Dot calls her breach response team back together to ask: "How can Bullz-Eye Corporation limit the chances of suffering a data breach in the future?"

How could Bullz-Eye have protected itself from this type of incident?

- Businesses should seek to be "compromise ready"
  - Assessment: proactive risk & security monitoring
  - Protection: security policies
    - Training for Staff
  - Response Planning
    - Pre-selected Outside Counsel and IT forensics consultant
  - Risk Transfer
    - Cyber insurance policies
    - Vendor contracts
      - Limitations of liability
      - Indemnification
- Risk & Security Assessments
  - What data exists? Where? Who has access? What safeguards? What laws are applicable?
  - Penetration testing & compromise assessments
    - Assess security of the resources, susceptibility to attacks in any number of areas
    - Penetration testing – attempting to gain access to your own systems through unapproved means
    - Vulnerability testing – identifying areas that may be vulnerable to an attack

What policies should Bullz-Eye have had in place?

- Data Security Policies
  - Designate a senior-level person responsible for coordinating data security efforts
  - Policy elements to address compliance with all applicable laws
    - Regulate the handling, storage, and protection of PII and confidential business information
      - Limit access to records to employees
      - Incorporation of other policies/procedures
        - Electronic Resources policies, BYOD policies, document retention policies, etc.
        - Integration with the Data Breach Response Plan
- Procedures for IT staff support
  - Proactive security: anti-virus, anti-spyware, firewalls, monitoring, patching, encryption
  - Backup and disaster recovery plans
  - Review of vendors and use of cloud technology
  - Limit use of unencrypted information and portable devices/storage media
  - Continue and upgrade regular training modules

What policies should Bullz-Eye have had in place?

- Data Security Policies
  - Employee Training and Discipline
    - Require training and impose disciplinary steps
      - Start simple: explain the ramifications of a data breach; start with the basics (password policies, risks of opening emails)
        - Signed acknowledgment of responsibility
        - Do your employment agreements need to be updated?
    - Impose controls (technical and policy-based) on access of employees to different categories of documents based on the sensitivity of those documents

How else could Bullz-Eye have protected itself?

- Risk Transfer
  - Vendor Contracts
    - Vendor Security Warranties
    - Indemnification
    - Limitations on liability
    - 35% of security violations involve contracted third parties (call centers, IT consultants)
    - Any potential liability pursuant to contract should be matched with cyber insurance coverage
  - Include protections in contracts before permitting access to physical office spaces, computer systems, or stored information, and attempt to negotiate indemnification for any negligence (or intentional acts) that expose data
  - Company Network Access Policies

How else could Bullz-Eye have protected itself?

- Risk Transfer
  - Cyber Insurance
    - Traditional insurance coverage is inadequate: insurance industry denies coverage claims related to cyber attacks under traditional insurance policies
    - Cyber liability policies will cover the costs of forensic analysis, repair of systems, data breach notifications, offers of credit monitoring and, if necessary, legal defense of claims arising from a breach
  - Application process is critical
  - Insurers increasingly evaluate privacy and data security policy and practices before insuring an applicant
  - Aimed at assessing an applicant's cyber-related exposures and IT security practices
  - Claims will be denied if inaccurate or fraudulent data is supplied on application

Cybersecurity Threats to Lawyers: In the News

Cravath, Weil, Other BigLaw Firms Hacked

By Y. Peter Kang

Share us on:

Law360, Los Angeles (March 29, 2016, 10:59 PM EDT) -- The computer networks of Cravath Swaine & Moore LLP, Weil Gotshal & Manges LLP and other major law firms were penetrated by unknown hackers possibly looking to profit from confidential or insider information for publicly traded companies, according to a Tuesday news report.

The FBI and federal prosecutors with the Southern District of New York have opened an investigation to determine if any confidential information was stolen by hackers and used for insider trading, according to the Wall Street Journal, which cited anonymous sources. The report said other prominent firms had their networks breached and that hackers are threatening further attacks.

Cybersecurity Threats to Lawyers: In the News

BRIEF

Report: China linked to 2015 hack of prominent US law firms

AUTHOR
Justine Brown

PUBLISHED
Dec. 8, 2016

Dive Brief:

- Security breaches which occurred at a number of law firms last year have now been linked to a group with connections to the Chinese government, according to Fortune.
- At one firm, hackers stole about around seven gigabytes of data, according to information obtained by Fortune, which could amount to tens of thousands of emails. Hackers reportedly gained access through the email accounts of partners and then relayed data to outside servers.
- For one of the firms, the attacks began in March 2015 and lasted for a period of 94 days, according to the report.

Dive Insight:

Law firms could be particularly appealing target for hackers because they often possess a wide range of sensitive information about their clients. Such information could result in insider trading, which has the potential to be

Cybersecurity Threats to Lawyers: In the News

BigLaw In Crosshairs As Firm Plans Data Breach Litigation

By **Aebra Coe** Share us on:

Law360, New York (March 31, 2016, 12:35 PM EDT) -- Following reports that Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP suffered data breaches at the hands of hackers, a plaintiffs law firm said Thursday that it plans to bring class action legal malpractice litigation against legal industry players over the exposure of client information.

Law firms have a professional duty to protect the privacy of client information, but most of them are not doing a good job when it comes to protecting that information from hackers, according to Jay Edelson, founder and CEO of privacy class action law firm Edelson PC, which nearly a year ago began investigating class action litigation against as-of-yet unnamed law firms over client data breaches.

Cybersecurity Threats to Lawyers: In the News

What are the Panama Papers? A guide to history's biggest data leak

Luke Harding

The Guardian, April 5, 2016

The Panama Papers are an unprecedented leak of 11.5m files from the database of the world's fourth biggest offshore law firm, Mossack Fonseca. The records were obtained from an anonymous source by the German newspaper Süddeutsche Zeitung, which shared them with the International Consortium of Investigative Journalists (ICIJ). The ICIJ then shared them with a large network of international partners, including the Guardian and the BBC.

The documents show the myriad ways in which the rich can exploit secretive offshore tax regimes. Twelve national leaders are among 143 politicians, their families and close associates from around the world known to have been using offshore tax havens.

The Rules of Professional Conduct Require Attorneys To Address Data Security

- **Model Rule 1.1, Competence:**
  - "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
  - Attorneys are required by Rule 1.1 to stay abreast of the "risks associated with relevant technology" in order to competently represent their clients (pursuant to the comment 8 to Rule 1.1).
- **Model Rule 1.6, Confidentiality of Information:**
  - "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent [and] 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."

45

The Rules of Professional Conduct Require Attorneys To Address Data Security

- **Model Rule 1.9, Duties to Former Clients:**
  - ""A lawyer who has formerly represented a client … shall not thereafter … reveal information related to the representation except as these Rule would permit or require with respect to a client."
- **Model Rule 1.15, Record Safekeeping:**
  - "A lawyer shall hold property of clients separate from the lawyer's own property. Funds shall be kept in a separate account … Other property shall be identified as such and appropriately safeguarded ..."
  - Several state ethics decisions make clear that client files, and therefore data provided by clients to their lawyer, are encompassed in the definition of "client property."

46

The Rules of Professional Conduct Require Attorneys To Address Data Security

- **Model Rule 5, Duty of Supervision:**
  - Rule 5.1(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(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."
    - This Rule extends the duty to keep secure electronically-stored client information to law firm employees and staff.

- **ABA Resolution 109:**
  - Recognizes that "[l]awyers and law offices have a responsibility to protect confidential records from unauthorized access and disclosure, whether malicious or unintentional, by both insiders and hackers."
  - Calls upon law firms and other organizations to "develop, implement, and maintain an appropriate cybersecurity program" addressing security controls and requiring regular testing and assessments."
  - Sets forth examples of technical standards to be used by law firms as guidance for their security protocols

47

Practical Tips for Lawyers and Law Firms

- Apply software updates monthly
  - Common software applications (*e.g.*, Adobe) have vulnerabilities that need to be patched
  - Install antivirus programs, malware protection, and firewalls
- Backup data and transfer it off-site every month
  - Use a reputable cloud service
- Encrypt your hard drives, WiFi networks, USB drives, and mobile devices with password protection
  - Utilize email encryption when warranted
  - Windows and Macintosh OS allow for encryption as do many email clients; alternatively, buy a file encryption tool
- Beware of spoofed emails and phishing attempts
  - Do not click on links or open attachments in emails from unconfirmed/unverified senders
- Utilize complex, unique, and long passwords
  - 8-character common word: 52 seconds
  - 8 random characters with numbers: 11 minutes
  - 8 random characters with mixed case, symbols, and numbers: 20 days
  - 10 random characters with mixed case, symbols, and numbers: 5 years
  - 12 characters: 17,134 years
- Connect to your office using a VPN
  - Do not travel with unencrypted files stored on laptops or storage devices
- Control access to confidential client data by staff
- Test your security systems annually – penetration/vulnerability testing by a qualified IT security consultant

48


questions