Remote Working in a Time of COVID-19: Cybersecurity Issues You Need to Know

Presented by the American Bar Association Cybersecurity Legal Task Force, Standing Committee on Law and National Security, Health Law Section and ABACLE
Submit a Question

Visit

to submit a question on the content of this course to program faculty. We’ll route your question to a faculty member or qualified commentator in 2 business days.

The materials contained herein represent the opinions of the authors and editors and should not be construed to be the action of the American Bar Association Cybersecurity Legal Task Force, Standing Committee on Law and National Security, Health Law Section or ABACLE unless adopted pursuant to the bylaws of the Association.

Nothing contained in this book is to be considered as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. This book and any forms and agreements herein are intended for educational and informational purposes only.

© 2020 American Bar Association. All rights reserved.

TABLE OF CONTENTS

1. Presentation Slides

2. COVID-19: Scientific and Medical Considerations (Additional Presentation Slides)
   Aileen M. Marty

3. Understanding Cybersecurity Risks (Chapter 2 of the ABA Cybersecurity Handbook)
   Lucy L. Thomson

4. Get SMART on Data Protection: Training and How to Create a Culture of Awareness (Chapter 13 of the ABA Cybersecurity Handbook)
   Ruth Hill Bro and Jill D. Rhodes

5. Additional Resources
Remote Working in a Time of COVID-19: Cybersecurity Issues You Need to Know

Thursday, March 19, 2020 | 12:00 PM Eastern
Sponsored by the American Bar Association, the ABA Cybersecurity Legal Task Force, the ABA Standing Committee on Law and National Security, and the ABA Health Law Section
Our Panel

• **Ruth Hill Bro (Moderator),** Privacy and Cybersecurity Attorney; Co-Chair, ABA Cybersecurity Legal Task Force; Chicago, IL

• **Christine Lyon,** Partner, Morrison & Foerster LLP; Member of the firm’s Coronavirus Task Force; Palo Alto, CA

• **Dr. Aileen Marty,** Director, Florida International University Health Travel Medicine Program; Vaccine Clinic Commander, Emergency Response Team Development; Professor, Infectious Diseases, Transitional Medicine at FIU; Miami, FL

• **Jill D. Rhodes,** Vice President and Chief Information Security Officer, Option Care Health; Winner of the 2019 Chicago-Area Chief Information Security Officer of the Year Award; Chicago, IL
Topics

• **Cybersecurity 101**: an overview of obligations to protect data, client confidential information, etc. and what’s at stake (Ruth)

• Truth is stranger than fiction: a not so hypothetical **hypothetical** and the issues it raises:
  - COVID-19 Scientific and Medical Considerations (Aileen)
  - Employment and privacy issues (Chris)
  - Cybersecurity issues you hadn’t thought of (Jill)

• **Key Considerations** – extra detail on points in the hypo

• Takeaways and Resources

• Q&A
Cybersecurity 101
Cybersecurity Is a Moving Target

- Cost is escalating
- Risks are multiplying, with everything connected (mobile, remote working, social media, IoT, the cloud, data-driven world)
- Volume/sophistication of cyber attacks are growing
- Targets are increasing and high-stakes
- Legal requirements are increasing
- Clients are demanding
- We must move with change…
Moving with Change

• As Robert F. Kennedy once observed, "Just because we cannot see clearly the end of the road, that is no reason for not setting out on the essential journey. On the contrary, great change predominates the world, and unless we move with change we will become its victims."

• Buckle your seatbelts....
COVID-19 Cyber Threats Are Already on the Rise

- “How hackers are exploiting the coronavirus—and how to protect yourself,” *Fortune*, 3/18/20.
- “HHS cyberattack highlights how hackers are exploiting the pandemic. Here are 4 strategies to mitigate the risks,” *FierceHealthcare*, 3/17/20.
COVID-19 CYBER INSECURITY

- Hackers targeting VPN vulnerabilities
- Phishing – COVID-19 in subject line, pretending to be boss/coworker using personal account
- Ransomware – “home doesn’t mean safe”
- Malware – fake COVID-19 tracker maps, CDC
- Social media pleas related to COVID-19
- Social engineering – someone you trust
- Need for speed … but haste makes waste
- Unvetted personal devices, behind in patches
- Public WiFi networks
- Lack of training – esp. newbie remote workers
Data Security/Cybersecurity

• Protect digital assets: systems, media, and data
• Goals to be achieved (CIA)
  • Ensure confidentiality, integrity, and availability
• Harms to be avoided
  • Unauthorized access, use, disclosure/transfer, disruption, modification/alteration
  • Accidental or intentional loss or destruction
• Categories of security measures/controls (PTA)
  • Physical, technical, and administrative security controls
All Businesses Have
Two Basic Data Security Legal Obligations

• **Duty to protect**
  - Provide “reasonable” or “appropriate” security for systems, media, and data – relative concept
    - To prevent breaches
    - To detect breaches
    - To respond to breaches

• **Duty to disclose**
  - Disclose breaches (to affected parties and regulators)
  - Warn affected parties

• **Source of obligations**: patchwork of statutes and regulations, common law, rules of evidence, rules of professional responsibility (for lawyers), contractual, self-imposed, etc.
“What” Does the Law Require a Business to Protect?

- Data
  - Personal information: employees, customers/clients, prospects
  - Business/client financial information
  - Tax information
  - Trade secrets & other confidential information
  - Transaction information
  - Info. of clients and others received in confidence
- Media containing such data – e.g., flash drives, laptops, CDs, DVDs, mobile phones, etc.
- Computer systems, networks, etc. (in-house, cloud, etc.)
- Communication of such data (email, web-based, etc.)
Hypo: Truth Is Stranger Than Fiction

- Mid-sized law firm with 200 attorneys in 7 states across the country.
- COVID-19 is here. Each of those states has declared a state of emergency. In three states, the Governor has shut down all restaurants and pubs. No sporting events or any external social events.
- President Trump says no more than 10 people should congregate at one place at one time.
- All schools are closed for at least two weeks, and likely more. 70% of your workforce has school-aged children.
- Clients are demanding to know how their confidential data will be protected.
- A senior partner comes to you and names you the head of COVID-19 response. She tells you to set up a plan for the company; remote workforce; emergency management; client relations.
- OUR PANEL WEIGHS IN....
Key Considerations

Extra detail on points in the hypo

COVID-19 Scientific and Medical Considerations

From Dr. Aileen Marty

(see more details in course materials)
Current data for SARS-CoV1 indicates an ID$_{50}$ of 100-150 viral plaque forming units. Current data about the ID for SARS-CoV2 is unknown, however it is clearly more infectious than SARS-CoV1 and thus the ID$_{50}$ is likely to be at least 100 – 150 plaque forming units, or more likely LESS.
SARS-CoV2:

- **Serial interval** (time between successive cases) is 4 - 4.6 days
  - This is *far shorter* than the 7 day serial interval for SARS-CoV1
- **Incubation period** *generally* 2 - 12.5 days (most 5.5 to 6.5 days)
  - *(Exceptional cases at 1 day, or as long as 19 – 27 days)*

This introduces **two key contributors to the rapid spread:**

1. **Asymptomatic transmitters**
2. **Rapid case generations** *(which *challenges* standard contact tracing systems)*


Aileen M Marty MD
Even without antivirals or a vaccine, our actions can make a significant impact on COVID-19.

- Detect, test, treat, isolate, trace, and mobilize our people in the response.
- That is how you CAN detect clusters and how you can prevent clusters from becoming community transmissions.
\[ R_0 = \frac{\text{Opportunity (Contact Rate)}}{\text{Transmission Probability}} \]

**Opportunity (Contact Rate)**
- How close you get & how long you are near infected host, if infected host projects viral droplets on you, if you touch your face after touching a contaminated surface (or hand)

**Transmission Probability**
- For SARS-CoV2 = 2-4
- Probability of viral transmission from infected host

**Susceptibility Probability**
- GOAL is to: < 1
- Probability of infection given exposure

- Limit size of mass gatherings
- Limit TIME near infectious persons
- Hand Hygiene, Proper use of PPE, Room Hygiene (Decontamination)
- Negative Pressure rooms
- Animal-control methods

- Limit ability of SARS-CoV2 to cause new infections via Contact tracing & Isolation, Quarantine, Social Distancing, e.g. Elbow-bump, Burial Methods
- Immune enhancement methods: Healthy Living (exercise, proper sleep, proper nutrition)
- Treat co-morbidities
- Pre-exposure vaccine (not available)
- Avoid things that hamper the immune system (decrease stress, stop smoking, etc.)

**Limit Infectious Period:**
- Antiviral Rx (experimental)
- Post-exposure Vaccines (Not available for SARS-CoV2)

**Recognition:**
- Limit ability of SARS-CoV2 to cause new infections via Contact tracing & Isolation, Quarantine, Social Distancing, e.g. Elbow-bump, Burial Methods
- Immune enhancement methods: Healthy Living (exercise, proper sleep, proper nutrition)
- Treat co-morbidities
- Pre-exposure vaccine (not available)
- Avoid things that hamper the immune system (decrease stress, stop smoking, etc.)

**< 1 (outbreak will extinguish)***
Epidemic Curve of the Confirmed Cases of Coronavirus Disease 2019 (COVID-19)

Wu Z, McGoogan JM. JAMA 24 Feb 2020

Aileen M Marty MD
Key Considerations

Extra detail on points in the hypo
Employment and privacy issues
From Christine Lyon
What are the Privacy Concerns?

Legal restrictions on health-related inquiries or exams by employers

- ADA and state medical confidentiality laws (e.g., CMIA)
- HIPAA, where acting as a covered entity for group health plans
- Common-law privacy claims

Other HR considerations

- Protecting confidentiality to encourage other employees to self-report
- Communicating with workforce to maintain trust and promote health and safety
- Preventing discrimination or harassment

Risk of future backlash/claims if employer seems in hindsight to have failed to protect employee privacy
Who Pays for Leave?

• Voluntary Leaves

• Mandatory Leaves
  • FLSA (or state equivalent)—Exempt Employees
    • To maintain exempt status, employee must receive full salary for any week in which employee works, regardless of number of days or hours worked.
    • Various factors for determining whether an employer can deduct exempt employee’s salary
  • FLSA (or state equivalent)—Non-Exempt Employees
    • Only paid for hours worked.
    • “Reporting Time” requirements require partial pay in some states
  • Employers may permit employees to use vacation/PTO.
• State income supplementation programs
Employers may encourage employees to work from home to control infection but should consider the following issues:
Best Practices

- Encourage sick employees to stay home.
- Employers may also wish to:
  - Prohibit or restrict business travel to or from high-risk areas
  - Limit non-essential travel
  - Postpone large gatherings, use telecommunications as an alternative
  - Reduce non-essential contact with business partners and clients
  - Educate employees about risks and precautions, as recommended by public officials
  - Recommend, or require, that employees with elevated risks of exposure work remotely
  - Permit other sick and high-risk individuals, such as those with other medical conditions, to work remotely, take time off, or work flexible hours as reasonably necessary
  - Regularly clean commonly used surfaces
  - Provide employees with sanitation resources, such as tissues, surface wipes, and trash receptacles

- Several companies have publicly announced policy changes which others may look to as potential industry specific best practices
Key Considerations
Extra detail on points in the hypo
Cybersecurity Issues
From Jill D. Rhodes
How’s the Security?

Must use a layered approach both in the office and remote
How Do We Start?

- Prioritize workforce
- Determine critical apps that remote workforce must access
- Determine how data and systems will be secured while access is provided
  - Depending upon the state, you may need to provide devices to your employees
- Determine if there is data that cannot leave the office – what is it and how is it being managed?
- Look at the rainbow with your IT/InfoSec team and determine what security there is at each level for remote employees
Layered Approach More Difficult with Remote Employees

- Compare Remote workforce
  - Working on own devices
  - Working on company devices
- How are they connecting into your network?
  - VPN
    - CISA on VPN Access (https://www.us-cert.gov/ncas/alerts/aa20-073a)
  - CITRIX – portal for securing information so they can access on personal devices
  - VDI – although this is more of a long term solution
- Is Multifactor Authentication Enabled?
Security Risks and Solutions (Cloud)

Cloud

- MS O365 – Microsoft has several tools that can be leveraged
  - Leverage **Teams** across your environment
    - Storing files
    - Chat feature
    - Conference features
  - **Ensure that employees working on home devices cannot**
    - Print locally
    - Download sensitive proprietary documents onto their personal devices
- Other cloud apps (Workday, Salesforce, etc.)
  - Confirm who has access and that this is limited to what they absolutely need
  - Again, need to ensure they cannot download something to personal computer – may only be able to manage this via policy/contract (work closely with HR on this too!)
Education and Training Are Key!

COVID-19 leads to increase in phishing

Malicious Website: corona-virus-map [dot] com
Emergency Response/Business Continuity

• Build an emergency response plan if you don’t have one
• Determine who is responsible for what – address all key issues that may come up while workers are remote
• Ensure you are ready to escalate if necessary – right now, we are focused on remote employees; be prepared if your employees are sick – how will you manage your work load with a temporary loss of 10% of your employees? 20%?
Don’ts

• Let personal devices directly enter your network unless there are proper mechanisms set up to protect that information
• Don’t forget that security is part and parcel to ensuring successful work from home
• Don’t assume that IT understands your needs, become a partner to ensure that access is granted and that applications are effectively reached
Do’s - People

• Make sure full team (InfoSec, IT, HR, etc.) is engaged to determine who needs remote access and how quickly; prioritize staff
• Establish a remote workforce policy
• Develop standards for your team members; set expectations
• Have your employees work in a separate area of their home where others don’t have as much access
• Limit printing or if they must print, confirm a shredder is also available for use
• Educate your employees about risks and expectations
• Over-communicate with your employees, the more information the better
Do’s - Technology

- Take a Risk-Based Approach
- Use Multifactor Authentication for access into the environment
- Use a tunnel to connect into the network – NO Direct Connections
- If working on phones (corporate or personal), make sure there is a mobile device management tool to support
- Confirm that you have adequate licenses (and IP addresses) to manage your remote workforce
- Make sure your remote tools are patched and updated
- Always understand how your sensitive data is being accessed!
Takeaways and Resources
Moving with Change

• As Robert F. Kennedy once observed, "Just because we cannot see clearly the end of the road, that is no reason for not setting out on the essential journey. On the contrary, great change predominates the world, and unless we move with change we will become its victims.”

• Get moving….stay on top of cyber issues and continually take the steps you need to take. The business you save may be your own.
Key sources of public guidance include:

1. The Centers for Disease Control (CDC)
2. The Occupational Safety and Health Administration (OSHA)
3. The Equal Employment Opportunity Commissions (EEOC)
4. The World Health Organization (WHO)
5. State and Local Authorities
6. The Department of Labor (DOL)
Resources:
ABA Cybersecurity Legal Task Force

The Task Force focuses and coordinates the ABA’s cybersecurity legal and policy analyses/assessments and identifies, compiles, and creates cybersecurity resources from a cross-disciplinary perspective.

Established in 2012. Over 25 ABA entities represented on Task Force.

ambar.org/cyber

Sample initiatives:
• Spearheads cybersecurity working groups/projects (e.g., information-sharing of cybersecurity threats, solo/small firm approaches, vendor checklist, etc.);
• Sponsors ABA Resolutions/Reports (under Policy tab at website), including 2/20 Resolution 118 on cyber/elections
• Spotlights the cybersecurity initiatives of over 25 ABA entities; and
• Undertakes array of publishing, programming, and outreach initiatives…. 
ABA Cybersecurity Resolutions/Reports

- **118 (February 2020):** Urges Congress to protect integrity and security of US federal elections by enacting legislation authorizing and funding NIST.
- **109 (August 2014):** Encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.
- **118 (August 2013):** Condemns unauthorized/illegal intrusions (including by foreign governments) into computer systems and networks used by lawyers and law firms and urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions.
- **116 (August 2015):** Urges the federal, state, local, territorial, and tribal legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.

See other ABA Cybersecurity Resolutions/Reports at the ABA Cybersecurity Legal Task Force site at ambar.org/cyber (Policy tab). (The Reports provide helpful info. on cyber threats, how to address threats, etc.)
Task Force Resources: Articles

- *Digital Dangers*: A joint yearlong exploration of cybersecurity and the law by the *ABA Journal* and the ABA Cybersecurity Legal Task Force
- “Any piece of technology that stores information could be compromised” (11/1/18 article)
- “How clients are pushing their outside counsels to adopt stricter cybersecurity standards and protections” (8/1/18 article)
- Articles (FREE) at abajournal.com/magazine/cyber
Task Force Resources: Handbook

- Winner of 2018 ACLEA Best Publication Award.
- 2 chapters from book included in today’s materials.
- Inspired 5-part webinar series: “Cybersecurity Wake-Up Call: The Business You Save May Be Your Own” (get free e-copy of book when you register for all 5)....
Task Force Resources: Webinars

5-Part Webinar Series (2018, recorded)
“Cybersecurity Wake-Up Call: The Business You Save May Be Your Own”
ambar.org/cyberwakeup

• Darkest Hour? Shining a Light on Cyber Ethical Obligations
• Bumps in the Night: Cybersecurity Legal Requirements, Government Enforcement, and Litigation
• While You Were Sleeping: Ever-Changing Cybersecurity Threats and What You Need to Know Now
• Cybersecurity Is Not One Size Fits All: Addressing Night and Day Differences for Solos/Small Firms, Megafirms, Companies, Government, and Nonprofits
• What Clients Want: Cybersecurity Requirements You Never Dreamed Of
Thank You

- Christine Lyon: clyon@mofo.com
- Aileen Marty: amarty@fiu.edu
- Jill D. Rhodes: Jill.Rhodes@optioncare.com
- Ruth Hill Bro: ruth.hill.bro@gmail.com
Questions?

All attendees can submit questions via the Q&A feature on the webinar interface.
COVID 19
Scientific and Medical Considerations

Aileen M. Marty M.D., FCAP
Professor, Infectious Diseases
Herbert Wertheim College of Medicine, Florida International University
Aileen.Marty@FIU.edu
The Panel

- **Prof Doctor Aileen Marty**, FIU, HW-COM
- Commander, Infectious Disease, FIU-FAST Team
- Senior advisor for the World Health Organization on Mass Gatherings, Outbreak response, and the Health- Security - Interphase
- Physician, scientist, professor of medicine, with more than 40 years of clinical experience.
- Served 25 years in the US Navy, where she became expert at coordinated health care for massive campaigns and field Med-Ready activities. She has served in numerous advisory capacities for Federal, State, and local government.
COVID19 is currently not under control, The sooner we act the less damage that it will cause.

China used its considerable resources and technical competence, to flatten its epidemic curve, however containment of the COVID19 virus requires a coordinated international response.

Managing the outbreak requires international cooperation using traditional public health strategies that ultimately succeeded with SARS, Ebola, and many other threats.
- Intensive contact investigations
- Development of medical countermeasures
- Mobilize supply chains to meet human needs for food, water, and medicine.

Key international efforts must include
- WHO leadership, assist with surveillance, contact investigations, testing, and treatment; foster public trust and cooperation; transparently share scientific information; and incentivizing academia and industry to develop vaccines and antiviral medications.
**Coronaviruses** family of high genetic diversity, all are

- enveloped positive-sense, single-stranded RNA viruses
- Host specificity is based on the spike protein

- SARS-CoV2 is a betacoronavirus shares ~82% of sequence identity with SARS-CoV1

**Source:** CDC/ Hannah A Bullock, Azaibi Tamin

https://phil.cdc.gov/Details.aspx?pid=2335
• Infectious Dose
• Lethal Dose

• \( ID_{10}, ID_{20}, ID_{50}, ID_{80}, ID_{100} \)
• \( LD_{10}, LD_{20}, LD_{50}, LD_{80}, LD_{100} \)

Current data for SARS-CoV1 indicates an \( ID_{50} \) of 100-150 viral plaque forming units
Current data about the ID for SARS-CoV2 is unknown, however it is clearly more infectious than SARS-CoV1 and thus the \( ID_{50} \) is likely to be at least 100 – 150 plaque forming units, or more likely LESS.
SARS-CoV2:

- **Serial interval** (time between successive cases) is 4 - 4.6 days
  - This is *far shorter* than the 7 day serial interval for SARS-CoV1
- **Incubation period** *generally* 2 - 12.5 days (most 5.5 to 6.5 days)
  - *(Exceptional cases at 1 day, or as long as 19 – 27 days)*

This introduces **two key contributors to the rapid spread:**

1. Asymptomatic transmitters
2. Rapid case generations *(which challenges standard contact tracing systems)*

Even without antivirals or a vaccine, our actions can make a significant impact on COVID19

- Detect, test, treat, isolate, trace, and mobilize our people in the response.
- That is how you CAN detect clusters and how you can prevent clusters from becoming community transmissions.
\[ R_0 = \frac{\text{Transmission Probability}}{\text{Opportunity (Contact Rate)}} \]

**Duration of Infectious Period**
- \( R_0 \) = Number of people or surfaces you come in contact with
- \( D \) = How close you get & how long you are near infected host, if infected host projects viral droplets on you, if you touch your face after touching a contaminated surface (or hand)
- \( \beta \) = Opportunity (Contact Rate)
- \( k \) = Transmission Probability
- \( S \) = Susceptibility Probability

**For SARS-CoV2**
- \( R_0 = 2-4 \)
- Goal is to: \(< 1 \) (outbreak will extinguish)

**Limit Infectious Period**: Antiviral Rx (experimental), Post-exposure, Vaccines (not available for SARS-CoV2)

**Limit size of mass gatherings**

**Limit ability of SARS-CoV2 to cause new infections via Contact tracing & Isolation, Quarantine, Social Distancing, e.g. Elbow-bump, Burial Methods**

**Immune enhancement methods**: Healthy Living (exercise, proper sleep, proper nutrition), Treat co-morbidities, Pre-exposure vaccine (not available), Avoid things that hamper the immune system (decrease stress, stop smoking, etc.)

**Limit Infectious Period**
- Antiviral Rx (experimental)
- Post-exposure
- Vaccines (not available for SARS-CoV2)

**Limit Time near infectious persons**
- Hand Hygiene
- Proper use PPE
- Room Hygiene (Decontamination)
- Negative Pressure rooms
- Animal-control methods

**Limit ability of SARS-CoV2 to cause new infections**
- Contact tracing & Isolation
- Quarantine
- Social Distancing

**Recogniton**
- Antiviral Rx
- Post-exposure
- Vaccines (not available for SARS-CoV2)

**Susceptibility Probability**
- Immune enhancement methods: Healthy Living (exercise, proper sleep, proper nutrition), Treat co-morbidities, Pre-exposure vaccine (not available), Avoid things that hamper the immune system (decrease stress, stop smoking, etc.)
Epidemic Curve of the Confirmed Cases of Coronavirus Disease 2019 (COVID-19)

Wu Z, McGoogan
JM. JAMA 24 Feb
2020
doi:10.1001/jama.20
20.2648
Fundamentally, China and South Korea took a Pragmatic, Systematic Approach Using Standard Tools For Containment

1. Tailored response to number of cases in each of their regions as they became affected
2. Mobilized collective action and cooperation by the population to the response
   a) Willing to isolate
   b) Willing to take hygienic methods (hand, respiratory, environment)
3. Followed a systematic, science-driven response with the application of modern, data-driven technology
4. Applied a “Shift in mindset.” In other words, they recognized that “this virus is here, we must go after every case, and every contact of every case, and treat all persons as best as possible.”
   • **This included readiness planning. This means what they did was:**
     a) Repurpose hospitals and spaces to accommodate the number of cases, including providing the best possible care for all individuals, do intensive contact tracing, and having enough supplies, equipment (e.g. Ventilators, PPE, Extracorporeal membrane oxygenation devices, etc).
     b) Recognize that you can use one isolation ward for multiple confirmed positive cases
     c) China recognized that most transmissions were family-based, not community-based so they closely followed family clusters and their close contacts.
     d) Be aware that patients with COVID19 need 2 to 6 weeks or more to recover.
     e) Be ready to adapt as knowledge increases
5. Cooperation between their provinces such that personnel, equipment, meds went from where they had it to where they needed it as it was needed.
6. Phased restart to their economy as cases go down, recognizing that cases will continue at a lowered, more manageable level until a vaccine or other radical way to interfere with the chains of contagion are developed.
Prevent the Spread of SARS-CoV2 in your workplace

1. Make sure **workplaces are clean and hygienic**
   - Surfaces (e.g. desks and tables) and objects (e.g. telephones, keyboards) need to be wiped with disinfectant regularly
     - Why? Because contamination on surfaces touched by employees and customers is **one of the main ways that COVID-19 spreads**

2. **Promote regular and thorough hand-washing** by employees, contractors and the elderly inhabitants of the ALS/Nursing home
   - Hand sanitizing dispensers must be located in prominent places around workplace.
     - Make sure these dispensers are regularly refilled
     - Display posters promoting hand-washing
     - Communication measures: offering guidance to promote hand-washing
     - Make sure staff, contractors and customers have access to places where they can wash their hands with soap and water : Why? Because washing kills the virus prevents spread of COVID-19
3. Promote good respiratory hygiene in the workplace
   • Display posters promoting respiratory hygiene, combine this with communication
   • Ensure that surgical masks and paper tissues are available at your workplaces for use by those with any respiratory illness.

4. Advise employees and Contractors to consult National Travel advice before going on any travel
   • Brief your employees and contractors to consult CDC, and your State DOH
5. If COVID-19 is now a community transmitted disease in the USA, thus
   • Anyone with a respiratory illness must stay home, ideally work from home
   • Communicate that masking symptoms with meds is not enough, they must stay at home until they are well
   • Display posters
   • Assure workers there time off counts as Sick leaves
1. Understand Risk
   - Attendees may unwittingly bring SARS-CoV2 (virus of COVID-19) to the meeting
   - Attendees may unwittingly be exposed to virus of COVID-19 at the meeting
   - 1/5 of people who catch COVID-19 needs hospital treatment (i.e. 20%)
1. **Reduce Risk**

   A. Check community risk status from authorities in your area and any new rules / regulations or targeted advise
      A. Know WHERE COVID19 is circulating in your community

   B. Develop and agree on a preparedness plan
      • Consider if a face-to-face meeting is truly needed
      • Can the face-to-face meeting be scaled down to fewer attendees
      • Establish and inform about alternative communication channels with key partners and customers
How to manage COVID-19 risk when organizing meetings & events

1. Reduce Risk

C. Preorder sufficient supplies and materials for participants including hand sanitizer and surgical mask if anyone develops respiratory symptoms during the meeting.

D. Advise all possible attendees NOT to attend if they have or develop respiratory symptoms or feel unwell.

E. Obtain the contact details of all organizers, participants, caterers, and visitors (cell number, e-mails, where they are staying)
   • State clearly that their details WILL be shared with the local public health authorities if any participant becomes unwell.
   • If they don’t agree – they cannot attend
How to manage COVID-19 risk when organizing meetings & events

1. Reduce Risk
   
   C. Preorder sufficient supplies and materials for participants including hand sanitizer and surgical mask if anyone develops respiratory symptoms during the meeting.

   D. Advise all possible attendees NOT to attend if they have or develop respiratory symptoms or feel unwell.

   E. Obtain the contact details of all organizers, participants, caterers, and visitors (cell number, e-mails, where they are staying)
      
      • State clearly that their details WILL be shared with the local public health authorities if any participant becomes unwell.
      • If they don’t agree – they cannot attend
How to manage COVID-19 risk when organizing meetings & events

1. Reduce Risk
   
   F. Build trust. For example, as an icebreaker, practice ways to say hello without touching.
   
   G. Encourage regular hand-washing or use of an alcohol rub by all participants at the meeting or event.
   
   H. Encourage participants to cover their face with the bend of their elbow or a tissue if they cough or sneeze. Supply tissues and closed bins to dispose of them in.
   
   I. Provide contact details or a health hotline number that participants can call for advice or to give information.
   
   J. Arrange seating so participants are about 6 feet apart.
   
   K. Ventilate – keep windows and doors open if at all possible.
   
   L. If someone feels unwell, call the local hotline.
For more information

• Aileen.Marty@fiu.edu
Chapter 2
Understanding Cybersecurity Risks
Lucy L. Thomson

I. New Technologies Create Unprecedented Challenges for Lawyers

This case [United States v. Iat Hong] of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals.¹

Preet Bharara, United States Attorney, Southern District of New York (2016)

As the frequency and sophistication of cyber attacks have increased in recent years, cyber criminals have targeted law firms due to the vast amount of client and firm information they collect and store. Numerous law firm data breaches have compromised sensitive and proprietary information, and hackers have gained access to entire law firm networks.

Both large and small law firms have been the target of hacker attacks in the United States as well as abroad. The law firm Mossack Fonseca, located in Panama, was involved in reportedly the largest data breach ever in terms of the volume of records stolen. Over the past 40 years, the firm has set up

about 250,000 offshore companies, collecting and storing a treasure trove of individuals’ confidential financial information in the process.\(^2\)

The breach (referred to as “leaks” by the media) included 11.5 million confidential documents dating from the 1970s through late 2015. The 2.6 terabytes of leaked data include 4.8 million e-mails, 3 million database files, 2.2 million PDFs, 1.1 million images, and 320,000 text documents.

The source of the breach, using the pseudonym John Doe, sent encrypted files anonymously to the German newspaper *Süddeutsche Zeitung* and shared them with more than 100 other media outlets.\(^3\) The U.S.-based International Consortium of Investigative Journalists published a searchable database of 214,000 offshore entities uncovered by the “Panama Papers” leak.\(^4\) In an open letter published on the Panama Papers website, Doe announced that he stole the information to expose the use of shell companies to “carry out a wide array of serious crimes that go beyond evading taxes,” and that he believed members of Mossack Fonseca “should have to answer for their roles in these crimes.”\(^5\)

International news outlets published articles on the leak, revealing corruption on a massive scale. Repercussions from the leak have been felt around the world. The compromised data exposed the existence of offshore

---


about 250,000 offshore companies, collecting and storing a treasure trove of individuals’ confidential financial information in the process.²

The breach (referred to as “leaks” by the media) included 11.5 million confidential documents dating from the 1970s through late 2015. The 2.6 terabytes of leaked data include 4.8 million e-mails, 3 million database files, 2.2 million PDFs, 1.1 million images, and 320,000 text documents.

The source of the breach, using the pseudonym John Doe, sent encrypted files anonymously to the German newspaper Süddeutsche Zeitung and shared them with more than 100 other media outlets.³ The U.S.-based International Consortium of Investigative Journalists published a searchable database of 214,000 offshore entities uncovered by the “Panama Papers” leak.⁴ In an open letter published on the Panama Papers website, Doe announced that he stole the information to expose the use of shell companies to “carry out a wide array of serious crimes that go beyond evading taxes,” and that he believed members of Mossack Fonseca “should have to answer for their roles in these crimes.”⁵

International news outlets published articles on the leak, revealing corruption on a massive scale. Repercussions from the leak have been felt around the world. The compromised data exposed the existence of offshore

---


⁵. McCallion et al., supra note 4.
accounts of world leaders, company executives, celebrities, and others. Iceland’s prime minister resigned. Mossack Fonseca shut down several firms and resigned as the registered agent for over 1,000 companies. The U.S. Department of Justice announced that it had launched a criminal investigation into the leak and the tax avoidance schemes it revealed.

Around the same time, in March 2016 the Federal Bureau of Investigation (FBI) Cyber Division issued an alert advising that hackers are specifically targeting international law firms as part of an insider-trading scheme. Three Chinese nationals were subsequently indicted for securities and wire fraud for hacking into prominent international law firms with offices in New York City and trading on confidential, nonpublic information they obtained from the e-mail accounts of law firm partners who worked on high-profile mergers and acquisitions (M&A) transactions.

These are among the most high-profile law firm breaches. Lawyers and law firms are attacked daily and are facing unprecedented challenges from the widespread use of electronic records, mobile devices, and the emerging Internet of Things (IoT). Gone are the days when lawyers wrote memos and briefs on yellow legal pads and determined legal positions after consulting libraries of beautifully maintained books. Seeking efficiencies from new technologies, most lawyers and law firms use e-mail extensively, have smartphones, and work on laptops and tablets. State-of-the-art computer devices are the cornerstones of the “electronic courtrooms” of the future.

In addition to technology usage, how and where lawyers and law firms store and process data vary significantly. Many law firms operate data centers with global networks of computers, servers, mobile devices, websites, and social media. These firms perform the full range of information security, data governance, preservation, and incident response functions. Others outsource these responsibilities. Law firms are also exploring the use of cloud computing for storing and processing client and firm records. Some have implemented “bring your own device” (BYOD) or “bring your own technology” (BYOT) policies in the organization.

---


7. United States v. Iat Hong, 16 Cr. 360 (S.D.N.Y. 2016).
**IoT in the Workplace.** The convergence of information technology and physical operations in which computers control a broad array of consumer and industrial devices and systems presents new security concerns for lawyers and law firms. It is predicted that by 2020 there will be more than 26 billion devices connected to the Internet. As law firms are modernized, they will likely include IoT devices such as security cameras, wireless locks, motion sensors, automated lighting and window shades, and climate control. Technologists are creating the “infrastructure of the smart office.” Their goal is to create an “intelligent workplace,” including smartphones, wearables, and applications, to provide solutions to problems, facilitate decision making, measure performance, and take care of most routine tasks.

**Legal Outsourcing.** It is now common practice for law firms to outsource a variety of services to external vendors and business partners located domestically and overseas. Legal organizations interconnect their networks electronically for a variety of purposes ranging from information technology (IT), finance, accounting, and human resources to procurement, contract management, data analytics, and investigations. Legal process outsourcing is a growing trend; law firms and corporate legal departments are outsourcing legal work such as litigation support for document review, due diligence, legal research, and law libraries. Much of the billions of dollars law firms spend on e-discovery services and forensic investigations is used to hire outside vendors.

This ever-growing paradigm presents increased risk for lawyers and their practices. The expectation of security is growing, and therefore the responsibility for protecting information, whether held within the firm or outsourced to a third party, is also increasing.

---

A. Responsibilities to Protect Sensitive and Confidential Data

Lawyers must safeguard client records, as well as their own business records, including intellectual property, attorney work product, and financial and employment records, to name a few. Electronic records are an integral part of every lawyer’s business.\(^{11}\)

Throughout the course of representing clients, lawyers receive volumes of sensitive and confidential data and information—attorney-client privileged information, client trade secrets, and all types of personally identifiable information (PII), financial, healthcare, law enforcement, and many other types of records.

Law practices also receive sensitive and confidential information through litigation or compulsory process, or as a result of investigations or adversary actions against individuals and organizations. In these cases, not only adversaries, but also innocent third parties, are often swept up in lawsuits or other legal proceedings. Given that lawyers have access to the most sensitive and secret information in civil and criminal cases—including private investigations, records sealed or under a protective order, classified data, grand jury records, and other information with requirements for secrecy—it is critical that this information is protected from breaches and unlawful exposure.

In addition, law firms acquire a staggering array of sensitive information in e-discovery. It is a sobering fact that much of the data and information obtained by law practices may have been created, used, and maintained in a secure environment, and then transferred, often without the knowledge, agreement, or consent of the individual or organization that created or collected the information, to an environment where the extent of security protections may be unknown or is not assured.\(^{12}\)

To protect confidential information, lawyers and law firms must know what data they have, where it resides, its level of sensitivity, and how it is secured. In addition to the more obvious places for data such as computer

\(^{11}\) See Chapter 4 for an in-depth discussion of the responsibilities of lawyers to protect sensitive and confidential information.

\(^{12}\) Until a law firm has conducted a risk assessment and adopted a comprehensive information security program, it will not be in a position to vouch for an appropriate level of security and its ability to protect sensitive and confidential data and information, if requested by a client or the court.
servers, desktop and laptop computers, and mobile devices, information may reside in other, somewhat less expected locations. For example, back-ups can contain significant amounts of sensitive information. Also, sensitive data may be downloaded from e-mail onto a mobile device and then saved locally. These devices are likely to be linked to the user, not the law firm, which means that the sensitive data is then backed up to the user’s personal cloud account, completely outside law firm control.

B. Lawyers and Law Firms Are Prime Targets: The Significant Resulting Damage

Due to the huge volume of critical information lawyers collect about companies and individuals, hackers are targeting law firms. Much of the valuable data law firms hold—particularly intellectual property, strategic business data, and knowledge of M&A and international transactions—carries obligations associated with attorney-client privileged data. Loss of such data due to a data breach can destroy the privilege.

Similarly, protective orders imposed by courts to preserve the secrecy of sensitive data may be violated in the event of a data breach. Although Rule 26(b) of the Federal Rules of Civil Procedure allows broad discovery on a variety of issues, Rule 26(c)(7) allows a court to issue an order that “a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a designated way.” If a data breach were to occur at a firm subject to such an order, arguably that order would be violated and the firm might face serious consequences.

From a business perspective, a breach of security or information loss by a law firm can have significant negative effects. The consequences to clients and even innocent third parties of a data breach can be devastating, potentially subjecting them to identity theft, fraud, negative publicity, and even financial ruin. If a firm loses client information, the reputational harm alone may lead a client to take its business elsewhere or potential clients to turn to other firms. For lawyers in the firm, a data breach may result in ethical violations that have serious impacts.13

13. Chapter 4 provides an in-depth discussion of the responsibilities of lawyers to protect sensitive and confidential information.
II. Protecting the Confidentiality, Integrity, and Availability of Data

Massive data breaches are occurring with alarming frequency. Lawyers and law firms must build strong information security programs to prevent, detect, and address risks of data loss. Protecting confidentiality, integrity, and availability are the three cornerstones of every security program.

In light of the massive data breaches in recent years, much attention has been given to protecting the confidentiality of personal data and sensitive information. The largest data breaches—spanning the financial, healthcare, retail, and government sectors—illustrate the heightened risk to millions of individuals when large datasets of sensitive personal information are compromised: Yahoo, 1.5 billion user accounts compromised (2013 and 2014); e-Bay, 145 million records breached (2014); Target Stores, 110 million (2013); Sony Online Entertainment, 102 million (2011); JP Morgan Chase, 76 million (2014); Anthem BlueCross BlueShield, 69–80 million (2015); Home Depot, 56 million (2014); TJX, 46 million (2006–07); and Office of Personnel Management (OPM), 22.5 million security clearance records, 5 million fingerprints (2015).

Databases are vulnerable to attacks from both insiders and hackers. These vulnerabilities are well documented and include the use of default and weak passwords, failure to patch known vulnerabilities, misconfigurations, and granting of excessive privileges to users. Specific security measures must be taken to protect personal data in the databases of legal organizations.14

Specific security measures that should be taken to protect personal data include (1) inventory your databases; (2) classify systems with sensitive data; (3) scan for vulnerabilities and misconfigurations, keep up to date with security patches, enforce strong passwords, and audit configurations and settings; (4) identify privileged users; (5) validate access to sensitive data and assign restricted permissions on tables with sensitive information; (6) prioritize and fix what you can; (7) monitor database activity; and (8) encrypt data in transit and at rest using network-level encryption and column-level encryption.

18  THE ABA CYBERSECURITY HANDBOOK

The Intelligence Community’s 2017 Worldwide Threat Assessment\textsuperscript{15} and the Foreign Cyber Threats report\textsuperscript{16} identify prominent cyber adversaries—nation-states (Russia, China, North Korea, and Iran), terrorist groups, and cyber criminals. In addition, “hacktivists” launch cyber attacks that are politically or ideologically motivated. The cyber report points out that “the breadth of cyber threats posed to U.S. national and economic security has become increasingly diverse, sophisticated, and serious, leading to physical, security, economic, and psychological consequences.” Many of these threat actors have significant resources, funded by nation-states or through sophisticated money-laundering operations.

One of the most important observations of the 2015 Worldwide Threat Assessment is that future cyber attacks will be conducted to compromise the \textit{integrity} of information, with a potentially devastating impact on key information systems that constitute the underpinnings of the economy:

In the future . . . we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e. accuracy and reliability) instead of deleting it or disrupting access to it. Decision-making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.\textsuperscript{17}

In recent years, cyber attacks designed to restrict the \textit{availability} of websites and services have been launched, primarily with distributed denial of service (DDoS) attacks in which multiple compromised computers,

\begin{itemize}
\item \textsuperscript{15} The Honorable Daniel R. Coats, Dir. of Nat’l Intelligence, Statement for the Record to the Senate Select Comm. on Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Community (May 11, 2017), https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.
\end{itemize}
often infected with a Trojan virus, are used to overwhelm a single targeted system; computer viruses that delete user data; or ransomware that encrypts data and demands payment for the encryption key to restore access to the data.

In an October 2016 DDoS attack, the Murai botnet scoured the web for IoT devices protected only by factory-default usernames and passwords. It then enlisted these vulnerable IoT devices such as Internet-connected cameras and DVRs to send junk traffic and temporarily overwhelm popular Internet sites including Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix; these websites could no longer accommodate legitimate visitors or users.

To prevent data breaches, it is essential to analyze and understand the root causes of security failures and develop a specific plan to address them. Analysis of the types of breaches that have occurred is illuminating; the conclusion is often that most of these breaches did not have to happen. To protect some of the most valuable and vulnerable assets of all organizations—data and information—lawyers and law firms will need to build strong information security programs that focus on protecting the confidentiality, integrity, and availability of information. This is not only good business practice; it will also help firms avoid the high costs associated with responding to data breaches, potential liability, negative press, embarrassment, and ultimately loss of trust of clients, judges, and the public.

18. A “Trojan” virus is a type of malware disguised as legitimate software that will enable a cyber criminal to gain access to a user’s system and spy on him, steal sensitive data, and gain backdoor access.

19. The high costs of responding to data breaches in terms of expenditures for detection, escalation, notification, and response, along with legal, investigative, and administrative expenses, customer defections, opportunity loss, reputation management, and costs associated with customer support such as information hotlines and credit monitoring subscriptions, have been well documented. PONEMON INST. LLC, 2016 COST OF CYBER CRIME STUDY & THE RISK OF BUSINESS INNOVATION (Oct. 2016), http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf. These costs are likely to rise as the notification requirements in the data breach laws become more stringent, increasing the numbers of individuals who must be notified; and the liability imposed by courts and administrative agencies for data breaches increases significantly.
III. Security Breaches on the Rise: Threats and Vulnerabilities Illustrated

Many different types of attacks occur against lawyers and law firms. The following are some examples.\(^\text{20}\) In each case, the bottom line is that the firm did not adequately identify and address information security risk with proper controls. As a result, millions of files were compromised, leading not only to data loss, but also reputational loss, lawsuits, and opportunity costs.

A. Hacking and Advanced Persistent Threats

Data breach trends over the past several years show that hackers were responsible for more than a third of the thousands of data breaches.\(^\text{21}\) Several of the largest breaches involved sophisticated global organizations of hackers who infiltrated information systems at vulnerable points—where sensitive personal records were unsecured—even though those same records were encrypted in company networks.\(^\text{22}\) Organizations that collect, process, or store large amounts of PII or intellectual property and strategic business data of high value to criminals have become prime targets of state-sponsored hackers and overseas organized crime.\(^\text{23}\)

Over the past decade, advanced persistent threats (APTs) have been among the most serious types of cyber attacks because their focus is espionage. Often originating in the Asia-Pacific countries, APTs employ zero-day exploits (taking advantage of vulnerabilities in software that are known, but not yet fixed) and social-engineering techniques against company employees to breach networks. The typical intrusion by an APT involves undetected  

---

\(^\text{20}\) The FBI 2016 Internet Crime Report highlights the types of crimes reported by businesses and individuals to the Internet Crime Complaint Center (IC3), “2016 Hot Topics” include scams such as business e-mail compromise (BEC), ransomware, tech support fraud, and extortion. In 2016, IC3 received a total of 298,728 complaints with reported losses in excess of $1.3 billion. FBI 2016 Internet Crime Report, https://pdf.ic3.gov/2016_IC3Report.pdf.


access into a victim computer system (in violation of federal and state law) and then the theft of significant amounts of data. Through the intrusions, hackers establish a foothold into a company’s network, sometimes for years, and even after a company has discovered them and taken corrective measures.24

The data breach of Mossack Fonseca that compromised the confidential records of the entire firm was the result of the failure to provide appropriate data security.25 The Panamanian firm employed outdated software—older versions of open source web server software—with critical vulnerabilities that were widely known among hackers, including for its customer portal. Updates to the software were available, but the firm had not updated or properly patched its web server.

Security experts suggested that because Mossack Fonseca’s web server software was many months out of date, the security failure was particularly egregious, considering the sensitivity of their clients’ information. The firm failed to take the most rudimentary steps to protect their confidential client data.26

Similarly, a class action lawsuit filed in 2016 by clients of Johnson Bell, a Chicago law firm, alleged that the firm “left its clients’ confidential information unsecured and unprotected,” exposing plaintiffs to heightened risk of injury. According to the complaint, (1) the firm’s time-tracking system utilized out-of-date software (the 2005 version of Webtime software JBoss was so old it was no longer maintained or supported) and it suffered from a critical vulnerability that hackers could exploit to install ransomware on the network; (2) the virtual private network (VPN) was vulnerable to


man-in-the-middle attacks; and (3) the firm’s e-mail system used weak encryption that could be broken (similar to that used by Mossack Fonseca). This case has since gone to arbitration.

B. Social Engineering and Phishing Attacks

Cyber risks have evolved beyond traditional hacking to include sophisticated social engineering scams that rely on unwitting insiders to effectuate the scheme. Criminals use trickery to outwit their victims, creating a sense of urgency combined with fear. In the past several years, organizations around the world have been the victims of multimillion-dollar fraud schemes that were successfully perpetrated online using social engineering.

**Phishing Attacks.** Phishing is among the attack vectors used most often by hackers to launch cyber attacks. The main perpetrators of phishing attacks are organized crime syndicates and state-affiliated actors. “The most devastating attacks by the most sophisticated attackers almost always begin with the simple act of spear-phishing,” then-Homeland Security Secretary Jeh Johnson observed at the November 2016 Financial Crimes and Cybersecurity Symposium hosted by the Manhattan District Attorney’s office.

Phishing has been a long-standing cyber threat for law firms. As long ago as 2009, the FBI warned that hackers were targeting U.S. law firms to steal confidential information. In 2011 the Washington, D.C., law firm

---

31. John Roberts, *Homeland Security Chief Cites Phishing as Top Hacking Threat*, Fortune (Nov. 20, 2016), http://fortune.com/2016/11/20/jeh-johnson-phishing/. Spear-phishing occurs when an individual is targeted for an attack, and emails or other means are used to convince the individual to click on a link that then launches the attack into the person’s computer and potentially the entire network.
Wiley Rein was a victim of a massive attack by Chinese hackers referred to as Byzantine Candor that encompassed 20 major companies. Security researchers have referred to the hackers as the “Comment group” since they infiltrated computers using hidden web page computer code known as “comments.” Their attack methodology began with phishing attacks that transmitted malware (malicious code) in e-mails to members of the firm. Audit log files showed that the malware enabled the hackers to access encrypted passwords they were able to crack offline. The hackers accessed the firm’s network and stole sensitive data by acting as network administrators, collecting critical data and exfiltrating it over the course of months. The thousands of pages of e-mails the hackers stole included confidential communications with clients.

Three Toronto law firms were the victims of targeted phishing attacks eventually traced to computers in China, with commercial espionage the presumed motive. In one case, after a bookkeeper clicked on an e-mail attachment, a “Trojan banker” virus established a “backdoor” through the bookkeeper’s computer. The program mimicked a bank’s website and lured unsuspecting users to enter critical personal and account information. It then transmitted this information to hackers, enabling the hackers to monitor deposits into the account. In December 2012 they stole a six-figure amount of money from the firm’s trust account. Law firms, which are known to have substantial funds in these accounts, are often targets of this type of hacking.

**Insider-Trading Schemes.** Hackers targeted international law firms in an insider-trading operation. The FBI issued an alert in March 2016 (see Figure 1) after agents discovered a post on an undisclosed “cybercriminal forum” in which someone was seeking to hire hackers to break into international law firms’ computer networks and steal data for an insider-trading

---


35. *Don’t Take the Bait*, supra note 32.

scheme.37 According to the Wall Street Journal, “a posting appeared on an underground Russian website called DarkMoney.cc, in which the person offered to sell his phishing services to other would-be cyber thieves and identified specific law firms as potential targets.”38

Three Chinese nationals were subsequently indicted for securities and wire fraud for hacking into prominent international law firms with offices in New York City and trading on confidential, non-public information they obtained from the e-mail accounts of law firm partners who worked on high-profile M&A transactions.39 According to the indictment, the hackers stole log-in credentials of a law firm employee to access the firm’s e-mail server and plant malware that would allow them to access the server. They

37. Friedman, supra note 6.
Understanding Cybersecurity Risks

then logged into e-mail accounts of partners at the firm to glean details of pending mergers, including pricing information. They traded on that information before the deals were made public. The hackers targeted seven firms, traded in five public companies, and made profits of over $4 million in the process.

In a related case, the Securities and Exchange Commission brought a civil action for securities violations against the three Chinese traders for fraudulently trading on hacked nonpublic information stolen from two New York–based law firms. A default judgment was entered against the defendants on May 9, 2017.

C. Ransomware

Ransomware is a massive cyber threat for organizations, particularly small and medium-size businesses such as law firms. Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities attacked recently by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

The Kaspersky security firm emphasized that in 2016, “ransomware continued to rampage across the world, tightening its hold on data and devices, and on individuals and businesses.” In a ransomware attack in May 2017, hackers unleashed an attack that disabled nearly 230,000 computers globally. Named WannaCry, the ransomware affected tens of thousands

---

44. Id.
of organization in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The consequences for critical infrastructure in the health and telecommunications sector were serious and far-reaching. At least 16 hospitals in the United Kingdom were forced to divert patients who required emergency services. Telefonica, one of Spain’s largest telecommunications companies, responded by shutting down many of its computers and VPN connections.

Reports indicated the hacking group behind the WannaCry campaign gained access to enterprise servers through malicious software that exploited a vulnerability in older Windows software—the Server Message Block (SMB) service, which Windows computers rely on to share files and printers across a local network. A patch was available to address the vulnerability, but the organizations attacked had not applied it. In June, a new strain of ransomware named Petya hit organizations worldwide that had not yet applied the necessary patch, including Ukraine government offices, banks, and power companies; the Danish transport and energy firm Maersk; and the Russian energy company Rosneft. It also led to a multiday shutdown of the international law firm DLA Piper. Another strain of malware was designed to destroy documents rather than merely encrypt them.

Ransomware attacks affect lawyers and law firms as much as any other organization. For example, Russian hackers used social-engineering tactics against a Miami law firm, healthcare clinics, and accounting and payroll processing firms to gain access to their computer networks and upload

49. Iain Thomson, Everything You Need to Know about the Petya, or, NotPetya Nasty Trashing PCs Worldwide: This Isn’t Ransomware—It’s Merry Chaos, REGISTER (June 28, 2017), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.
malware. After stealing confidential client records (including personal and financial data, spreadsheets of client records, medical records, and log-in credentials), one hacker who identified himself as “Return” encrypted the companies’ business and client information and then demanded that the companies pay ransom to regain access to the files and ensure that the victims’ data would not be publicly dumped or put up for sale on the dark web.

In another case, an email that looked like it was coming from the phone system with voicemail messages as an attachment was the attack vector for a ransomware attack on a small North Carolina law firm. Finally, according to a lawsuit filed against its insurer for denying its ransomware damages claim, Providence, Rhode Island, law firm Moses Afonso Ryan Ltd. reported that a hacker held the firm captive for months by encrypting all its files and then demanding $25,000 in ransom to be paid in anonymous cyber currency to restore access.


D. Business E-mail Compromise

Business e-mail compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers or businesses that regularly perform wire transfer payments. The scam, which has targeted businesses of all sizes, is carried out by compromising legitimate e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. The FBI has seen a 2,370 percent increase in exposed losses since January 2015. Victims have been identified in all 50 states and 151 countries.54

CEO Fraud and W-2 Phishing Schemes. According to an “urgent alert” issued by the Internal Revenue Service (IRS), criminals are now combining CEO fraud and W-2 phishing schemes to target a far broader range of organizations than ever before. IRS Commissioner John Koskinen characterized the fraud as “one of the most dangerous email phishing scams we’ve seen in a long time.”55 Fraudulent requests are sent utilizing a business executive’s compromised e-mail. The targeted recipients are frequently the entities in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section. Some of these incidents are isolated and others occur before a fraudulent wire transfer request.

Law firms have been the targets of these W-2 phishing attacks. In April 2016 Proskauer Rose in New York determined that an employee in its payroll department received a fraudulent e-mail requesting copies of W-2s of firm personnel.56 A Sandler & Travis Trade Advisory Services (STTAS) employee received a request for all 2015 employees’ W-2 information; after these records were provided, it was discovered that the request had been

Understanding Cybersecurity Risks

made from a fraudulent account by an individual purporting to be an STTAS executive. 57

**Hacktivist Law Firm Attacks.** A large volume of e-mail with client documents attached was stolen from Puckett & Faraj, a small law firm in Alexandria, Virginia, in early 2012 by the hacking group Anonymous. 58 Detailed legal documents about the firm’s defense of high-profile military defendants accused of war crimes were stolen, as well as lawyer correspondence relating to other clients and matters. The hackers were able to gain access to Google e-mail accounts because the firm failed to use strong passwords, and by exploiting vulnerabilities in the firm’s website. 59 The law firm apparently was targeted by the hackers for representing a U.S. Marine convicted of negligent dereliction of duty in a 2005 attack in Haditha, Iraq, that resulted in the deaths of 24 unarmed civilians.

E. **Malicious Insiders**

Malicious insider attacks are on the rise and pose a serious threat to the security of sensitive information. 60 These activities have accounted for more than 600 breaches resulting in the compromise of 44.8 million personal records in recent years. 61

Criminals are using the dark web to recruit employees who have access to corporate networks to become “rogue insiders.” 62 The motivation of employees to steal data may range from financial gain (theft of trade secrets

60. See VERIZON, supra note 30, at 35–39.
and other sensitive information for sale) to revenge for perceived wrongs committed against them. Individuals who abuse administrative privileges, and security failures such as not suspending system access for terminated employees, cause many breaches.

Malicious insiders pose a serious risk for law firms. For example, a federal grand jury in Pittsburgh indicted a legal secretary who had been fired from a law firm. She and two colleagues were charged with hacking into a computer server at the law firm where they installed software that could be used to capture passwords of anyone on the firm’s network. Subsequently they illegally obtained personal financial information of law firm employees.63

High-profile criminal cases in the financial sector illustrate the extent of the fraud that can be caused by malicious insiders. In one of the most publicized insider cases, a computer technician who worked in Bank of New York Mellon’s IT department stole the identities of 2,000 bank employees and opened bank and brokerage accounts. He then used the accounts to steal more than $1.1 million from charities, nonprofit groups, and other entities.64 The defendant pleaded guilty to grand larceny, money laundering, and computer tampering.

Defending an organization’s perimeter from external attack does not protect against valuable information seeping out because of insider malfeasance, whether that behavior is characterized as malicious, mischievous, ignorant, or accidental.65 Carnegie Mellon University has published a list of best practices to minimize the risk of insider attacks.66

---

F. Mobile Devices

As the use of mobile devices explodes around the globe, concerns about the security of data and communications with mobile devices are increasing. While mobile devices are an integral part of the legal environment, and smartphones, tablets, and laptops have become essential tools for attorneys and support staff alike, they can be full of confidential client communications and by their design present numerous risks. They are often lost or stolen, and the data on them may be accessed with little difficulty. The contents of mobile devices may be unprotected because many devices have no password or only a weak password that can be broken.

From a security perspective, experts have identified three “attack surfaces” associated with mobile devices—the device itself, the operating system (OS) on the device, and the external service providers. Figure 2 provides examples of some of the common attacks or other failures of well-known good security policy that can lead to compromise of confidential, sensitive, and proprietary law firm data and information.

The device may be stolen, the data on it may be stolen, and the various sensors, such as a camera and microphone, may be surreptitiously turned on. The operating system itself may be faulty, or preboot Trojans (malware


69. The opinion of the Supreme Court in Riley v. California, 573 U.S. __, 34 S. Ct. 2473 (2014), concerning individuals’ expectations of privacy in cell phones, underscores the need for protecting the contents of mobile devices. “One of the most notable distinguishing features of modern cell phones is their immense storage capacity.” Id., 34 S. Ct. at 2490. “[Cell phones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.” Id.

70. Often mobile device users do not realize that when accepting certain applications, policies include the provider’s right to turn on a camera and/or microphone.
that affects preboot operations) may “jailbreak” the OS protections, or the OS may permit weak passwords. Provider failures cover the failure of IT management (policies to manage mobile devices remotely), as well as malicious application injection and data theft. In addition, hackers have inserted malware into applications (apps) so when users download them onto mobile devices the malware allows hackers to gain access to sensitive information. Hackers can intercept unencrypted data or messages as they are transmitted to and from mobile devices (“man-in-the-middle” attack) and inject new messages between the parties. The Federal Trade Commission has brought a number of cases charging that companies engaged in unfair and deceptive practices for marketing mobile devices and software

71. “Jailbreak” means installing software on a phone to “break open” the phone’s OS security and allow a user to modify anything it protects. This is a well-known form of privilege escalation that usurps OS isolation assumptions.
with security vulnerabilities or that exposed personal data without consumers’ knowledge.\textsuperscript{72}

Over the past ten years, more than one-third of data breaches resulted from the theft or loss of laptops, computers, hard drives, backup tapes, PDAs, or other portable media containing unencrypted personal information, including medical, education, and financial records.\textsuperscript{73} Widely publicized breaches illustrate the sheer magnitude of the exposure of personal records and the potential damage to millions of individuals when these devices are lost or stolen.\textsuperscript{74}

In March 2017, Horizon Healthcare Services, Inc. agreed to pay $1.1 million and improve its security practices after two laptops containing the personal information of 690,000 New Jersey policyholders were stolen. The data was not encrypted as required by federal law.\textsuperscript{75}

The vulnerabilities are particularly serious if the mobile devices are used to communicate with legal clients by e-mail or through social media, or to view, process, or store confidential client data or information. Data breaches in such cases can be prevented by encrypting the data on the devices, enforcing procedures that do not permit individuals to transport sensitive data on moveable media, keeping careful track of the devices, and having the highest standards and requirements for couriers to move backup tapes and CDs to off-site storage facilities or from one location to the another.

**Requirements for Mobility in a Legal Environment.** Seeking efficiencies from new technologies, many organizations are considering whether to implement BYOD or BYOT policies. BYOD may appear to be a good approach for organizations seeking to reduce costs and accommodate a generation of younger lawyers who are investing in the latest mobile devices,

\textsuperscript{72} FTC, Mobile Technology Issues, https://www.ftc.gov/news-events/media-resources/mobile-technology.


\textsuperscript{74} Examples include TriCare-SAIC (4.6 million records breached); Bank of New York Mellon (4.5 million records breached); Sutter Physicians Service and Foundation of California (4.2 million medical records breached); Educational Credit Management Co. (3.3 million records breached); and Jacobi Medical Center NY (1.7 million medical records breached).

\textsuperscript{75} Privacy Rights Clearinghouse, Data Breaches, https://www.privacyrights.org/data-breaches.
but the practice carries potential risks that are not well understood. Adopting a BYOD program carries with it significant responsibilities from both an information governance and technical perspective.\(^76\)

While there are a number of steps a law firm should take to protect confidential data on mobile devices if it chooses to permit personal devices on the network, several are key. Where possible, the law firm should use mobile device management that provides a centralized way to manage mobile devices remotely, including, significantly, the ability to check a lost device’s geographic location and lock or erase it remotely. Only known users and devices should be permitted on the network; app providers should be known as well. Phones that have been jailbroken or rooted should not be permitted on the network. Phones and tablets that are used to create, transmit, or store sensitive data, even in e-mail, should have centralized management of passwords with acceptable password policies, and all user data should be encrypted. Such management software is readily available from many vendors.

G. Cloud Computing and Wi-Fi Risks
Because of the increased flexibility and efficiency afforded by computing resources available on demand, law firms are using cloud services for processing and storing confidential client data and records. However, cloud computing introduces IT security and privacy risks related to outsourcing the administration and physical control of sensitive data to a third-party vendor and maintenance of the data on shared computing platforms, risks that will need to be carefully evaluated and addressed by legal entities that intend to put client data in the cloud.\(^77\)

---


Storing documents in a cloud service such as Dropbox creates risks. The cloud should be considered a public repository, and sensitive documents should be encrypted before they are placed there. The 2012 Dropbox breach underscores this point; an unencrypted document with users’ e-mail addresses was accessed illegally and the users were subjected to a flood of spam.  

New York–based law firm White & Case restricts attorneys from using file-hosting programs such as Dropbox.

Wireless communication creates opportunities for hackers to intercept sensitive data such as passwords for logging in to corporate networks and online banking sites. Public Wi-Fi locations such as airports, hotels, and coffee shops—convenient places to check e-mail—often do not have security features necessary to protect confidential client data. Hackers can use a proxy server to create a fake Wi-Fi hotspot (an “evil twin”) and intercept or redirect confidential communications.

H. Improper Disposal of Personal Information

Sensitive personal records in paper, as well as digital formats, must be protected. At least 31 states and Puerto Rico have enacted laws that require entities to destroy, properly dispose of, or otherwise make personal information unreadable or undecipherable.

Documents containing sensitive personal information—wills, a divorce document with children’s names and birthdays, and child protective services reports—were found by a local resident in a dumpster located outside the


St. Petersburg, Florida, law firm of a lawyer who practices marital, family, and estate law.81

In 2016 a man using the Wyandotte, Michigan, recycling center came upon documents that raised a red flag. The resident observed: “I just found tons of personal court documents like bankruptcy files, wills and power of attorney papers, along with birth and death certificates. It looks like someone emptied all of the files to get recycled and for the public to see. This stuff could cause a lot of trouble in the right hands.”82

Hundreds of personal documents from the Walz and Associates law firm were found in 2013 in a Bernalillo County recycling center in Tijeras, New Mexico; they contained the criminal histories, depositions, and even medical records of dozens of people.83

I. Business Partners Can Be a Weak Link— A Two-Edged Sword for Law Firms

Third-party business partners and vendors can provide a pathway into companies of strategic interest to global hackers.84 From the point of view of hackers, law firms are considered “business partners” of major corporate clients with a trove of proprietary data—a weak link to be exploited.

Similarly, it can be said that the security of a law firm is only as strong as that of its weakest business partner. Law firms and corporate legal departments are outsourcing a variety of legal work to outside businesses located domestically and overseas. The seriousness of this problem is illustrated by the breach of the website of HBGary, a cybersecurity firm that investigates data breaches and conducts investigations, in which two major law firms were implicated publicly.

84. INTELLIGENCE Ctr. Report, APT1, supra note 23.
The hacker group Anonymous seized control of HBGary’s website, defaced its pages, extracted more than 60,000 company e-mails, and deleted backup files. It then posted those e-mails in a searchable form on the Internet.85 The released e-mails created a frenzy of media coverage in major publications.86 News reports indicate that Washington, D.C., law firm Hunton & Williams had hired HBGary as an outsourcing partner to conduct investigations for its clients. The firm suffered embarrassment and its work on behalf of its client the Chamber of Commerce was discussed in extensive media coverage. A fallout of the breach was the filing of an ethics complaint against three Hunton & Williams attorneys.87

The confidential e-mails that were stolen from HBGary also revealed extensive details about industrial espionage by hackers in China, Russia, and other countries against law firms and major corporations.88 The Atlanta-based law firm King and Spalding was mentioned along with Google, which said in January 2010 it had “lost intellectual property assets to hackers based in China,” and Adobe, which reported similar hacker attacks. Intel Corporation said “it was attacked in a ‘sophisticated incident’ around the same time as Google.”89 The need for law firms to assess the security practices of their business partners should be clear from the widespread ramifications of this breach.

86. These media outlets included the New York Times, Washington Post, Los Angeles Times, Forbes, and NPR; tech publications such as Ars Technica, Wired, Tech News, the Tech Herald, and the Hacker News; legal publications such as Law Tech News, Corporate Counsel, Legal Times, and National Law Journal; and independent media such as Think Progress, the Brad Blog, Salon, and FireDogLake.
89. Id.
IV. Addressing Threats and Risks to Law Firm Security

A. What Is “Information Security”?
The breaches and threats described above stem from a frequent absence of security across law firms and other practices in which lawyers are present. To address these risks, lawyers need to understand information security and the basics of risk management.

Simply put, information security involves protection of digital assets. It is critical for law firms to have appropriate security because of the huge volume of data lawyers collect about companies and individuals. Just as the government, companies, and individuals protect their physical assets, information security must be an integral part of any technology solution.

“Information security” can be defined as a risk management process that security professionals undertake to protect the confidentiality, integrity, and availability of information and information systems. The process includes identifying the universe of possible threats to information assets, determining whether the assets are vulnerable to the threats, and implementing appropriate and cost-effective safeguards to address the threats. A threat is the possibility that any man-made, accidental, or natural event may damage information or information systems. Vulnerabilities exist when there is an absence of, or weakness in, a safeguard to address a threat, leaving information assets unprotected.

Several private sector organizations and the National Institute of Standards and Technology (NIST) have issued standards, guidance, and compliance tools organizations may use to develop and implement their security plans. These are based on a common body of knowledge among security professionals of what steps are needed to protect sensitive data and information systems.90


The various IT security associations provide other resources. See, e.g., SANS, http://www.sans.org. The ISO/IEC Information Security Management System family of standards are based on the governing principle that an organization should design, implement, and maintain a coherent set of processes and systems to manage risks to its information assets, thereby ensuring acceptable levels of information security. See Int’l Org. for Standardization, http://www.iso.org.
B. Why Is Information Security Important?
As the examples discussed above demonstrate, lack of information security can lead to significant losses for lawyers and law firms. Business could be temporarily disrupted, or if a sustained attack or breach of security occurs, the continuity of the law firm’s business could be severely affected and, in the worst scenario, the firm could be forced out of business.

Ultimately, a firm could face substantial and hard-to-quantify liability if a data breach occurs. Instead of waiting for a breach to take place, law firms should implement proactive measures that will significantly lessen the likelihood of a compromise. These actions can potentially lead to reduced likelihood of liability.

C. Who Is Responsible?
Information security must be adopted at the highest level of a law firm and flow down through the rest of the organization. Without such “buy in” by the firm management, there will be no incentive for all members of the firm to adopt appropriate technology and follow good security practices.

D. The Need for Risk Assessment
Information security is based on a systematic assessment of risks that are present in a particular operating environment. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed.

A risk management program that assesses threats and vulnerabilities regularly, applying an understanding of the type and severity of the associated risks, should be established across the firm. Information security is not a mystery—it is based on a systematic assessment of threats and risks that are present in a particular information system.

The principal goal of the law firm’s risk management process should be to protect the organization and its ability to perform its mission, not just its IT assets. A risk analysis process includes, but is not limited to, the following activities:

1. Evaluating the likelihood and impact of potential risks to sensitive and confidential information;
2. Implementing appropriate security measures to address the risks identified in the risk analysis;
3. Documenting the chosen security measures and, where required, the rationale for adopting those measures; and
4. Maintaining continuous, reasonable, and appropriate security protections.

The purpose of a risk assessment is to inform law firm decision makers and support risk responses by identifying (1) relevant threats to the law firm or threats directed through outside organizations against the law firm; (2) vulnerabilities both internal and external to the law firm; (3) impact (i.e., harm) to the firm and its clients that may occur given the potential for threats exploiting vulnerabilities; and (4) likelihood that harm will occur. The result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring). Based on a risk assessment, appropriate security controls can be selected, implemented, and continuously monitored so that risks and vulnerabilities are reduced to a reasonable and appropriate level.91

Risk analysis should be an ongoing process in which the law firm regularly reviews its records to track access to confidential records and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to sensitive and confidential information. The NIST Framework for Improving Critical Infrastructure Cybersecurity provides a common language for organizations to use in assessing security risks and a framework for determining the maturity of their cybersecurity program.92

---

91. NIST requires management, operational, and technical safeguards.
E. Achieving Optimal Network Security through Continuous Monitoring

To protect against data breaches, the legal profession, as well as companies and government agencies, must take immediate action to strengthen their security posture. To properly support an organization’s risk management program, security must be incorporated into the architecture and design of the organization’s information systems and supporting IT assets.

This includes continuous monitoring of systems, security status, and risks. Continuous monitoring of systems and networks is essential to protect against the broad range of serious threats to information systems. Robust continuous monitoring will provide law firm executives with the information necessary to make cost-effective, risk-based decisions.

Continuous monitoring is designed to provide meaningful, actionable intelligence and reporting—instead of merely collecting data. Situational awareness will inform law firms about the threat to, vulnerability of, and compliance posture of the system, as well as provide information about incidents that will need to be investigated. Potential threats must be investigated, and targeted attacks can be detected in advance or addressed as they occur, enabling a highly proactive security posture. The results of continuous monitoring will ensure that all the information necessary to address security incidents and potential attacks is readily available for analysis and review. The objective is to address the multitude of security threats and risks in a timely, disciplined, and structured fashion.

93. The Center for Internet Security’s Critical Security Controls for Effective Cyber Defense V 6.1 provides guidance to maximize the impact of government and private sector security efforts, and identifies 20 critical priority controls, most of which can be continuously monitored. Ctr. for Internet Sec., CIS Controls, https://www.cisecurity.org/controls/. The CIS website provides a wealth of valuable information about the leading information security methodologies and how they relate to each other.

V. Steps to Protect Confidential Law Firm Records and Prevent Data Breaches: Top Considerations

Law firms that collect, use, store, and share sensitive, confidential, and proprietary information must protect the information and ensure that it is not compromised by hackers or malicious insiders, inadvertently accessed, or lost. The following is a list of top considerations for lawyers and law practices when addressing information security and data protection.

1. **Develop a comprehensive information security plan** specifically designed to prevent data breaches. The plan must include appropriate security for all aspects of the computer network, including *technical, operational, and management controls*. For example, spear phishing is currently a common attack methodology used by hackers; address it by creating a culture of security throughout the law firm and enforce security policies to combat this problem.

2. **Conduct a risk assessment.** Carefully document how the security controls selected and implemented address all risks identified. Ensure that information security continuous monitoring is a part of organization-wide risk management.

3. **Follow security-by-design principles.** To properly support an organization’s risk management framework, security must be incorporated into the architecture and design of the organization’s information systems and supporting IT assets.

4. **Prioritize the use of scarce resources to address the most serious problems.** Prioritize security resources so that the most critical and vulnerable aspects of the system are addressed first. Consider the recommendations of experts about how to prioritize.95 Address the most common threats such as phishing attacks, ransomware, BEC, stolen credentials, and software patching. Understand key risks and threats and stay informed about new ones as they are discovered.

---

95. *See, e.g.*, CIS Controls, *supra* note 94.
5. *Do not purchase or implement* devices, software, or systems with known vulnerabilities. Work with vendors and business partners who provide products and services with appropriate security. Use procurements as an opportunity to specify requirements for appropriate security in vendor contracts and business partner agreements.

6. **Secure the law firm’s sensitive data using appropriate encryption technology.** Remember that inadequate or inappropriate key management can result in data breaches and/or loss of data; ensure that appropriate encryption is utilized on mobile devices.

7. **Where possible, use mobile device management** to protect confidential data on mobile devices, including the ability to lock or erase a lost device remotely, and check its geographic location.

8. **Allow only known users and devices** onto the network; app providers should be known as well. Phones that have been jailbroken or rooted should not be permitted on the network. Phones and tablets that are used to create, transmit, or store sensitive data, even in e-mail, should have centralized management of passwords with acceptable password policies, and all user data should be encrypted.

9. **Develop a data retention and destruction plan** so personal data is not at risk—sanitize regularly.

10. **Be prepared if a data breach occurs.** Build internal firm teams of first responders who have been briefed on the security issues and their implications, so they do not have to think through such things for the very first time in the middle of a security incident or data breach. Identify and build bridges with Internet service providers, law enforcement, and other security resources so you know who to go to when an incident or breach occurs, and so they know who you are.96 Work with the Legal Services Information Sharing and Analysis Organization (LS-ISAO) and take advantage of their resources and expertise.97

---

96. The FBI 2016 Internet Crime Report, *supra* note 20, includes a section on the importance of law enforcement collaboration and partnerships with the private sector and Intelligence Community.

Chapter 13
Get SMART on Data Protection
Training and How to Create
a Culture of Awareness
Ruth Hill Bro and Jill D. Rhodes

I. Data Protection Training Basics and Core Principles

Any business that works with personal and sensitive data must develop a strategy for protecting that data. When assessing how to do so, organizations, including law firms, often mistakenly rely on technology as the solution. In fact, four factors are key to implementing a proper information security and data protection program in any setting:

- Establishing the appropriate **governance** for the data, such as policies and the oversight of an executive level committee tasked with reducing data protection risk;
- Ensuring that the **people** working with the data know how best to protect it;
- Assessing data protection and usage **processes**; and
- Employing appropriate **technology** to protect the network.

These four factors work together to develop an overarching and effective program.
This chapter focuses on the people aspect of that equation, but other factors (e.g., governance and processes) also come into play. Most data missteps in law firms and other businesses are directly linked to something an employee or contractor did, whether intentionally or unintentionally. The easiest way to address this risk is to educate employees and others about the risk and their role in protecting personal and sensitive data.

Education and training can be provided by many facets of the organization, whether human resources (HR), the chief privacy officer (CPO), the chief information security officer (CISO), or others. Regardless of which groups do the training, it is critical that they work together to produce a common vision and message that is then disseminated across the organization.

A. Why Train on Data Protection?

All organizations, including law firms, are increasingly recognizing that data underpins virtually everything that they do and—like other valuable business assets—should be protected.

The trend is to adopt a reasoned and comprehensive strategy that makes data protection a part of the corporate culture and the job of every individual working for the business (partners, associates, paralegals, interns/law students, information technology (IT), HR, executives, administrators, administrative assistants, and other staff). Such an approach is designed to:

- Minimize missteps that can hit the bottom line (costly litigation; time and resources consumed in responding to government, press, or attorney disciplinary commission inquiries or investigations; adverse media coverage; damage to client or customer relationships; and so on), and
- Help businesses achieve a competitive advantage, enhance their profile and image, and enrich their relationship with clients and customers.

1. This trend is in keeping with the “Privacy by Design” (PbD) and “Security by Design” (SbD) movements that are transforming the way that businesses protect data in an information-driven age. See, e.g., Privacy by Design: The 7 Foundational Principles, by Ann Cavoukian, Ph.D., Distinguished Expert-in-Residence, Privacy by Design Centre of Excellence, Ryerson University and former Ontario Privacy Commissioner, at http://www.ryerson.ca/pbdce; see also Fed. Trade Comm’n, Start with Security: A Guide for Business, http://www.ftc.gov/startwithsecurity for insights and guidance on SbD gleaned from over 50 FTC data security settlements.
Yet making data protection a part of the corporate culture is easier said than done:

- Properly addressing data protection issues can require a comprehensive understanding of rapidly changing applicable law in 50 states and territories, at the federal level, and globally (where client or customer data might originate, where third parties might be providing U.S.-based businesses with 24/7 services, etc.). Many laws (particularly for government entities and regulated industries) and lawyers’ professional rules of responsibility expressly or by implication require appropriate data protection training for employees and sometimes contractors as well.2

- Command of the law is not enough, as businesses are often tried in the court of public opinion or are challenged by third-party watchdog groups, regardless of the current legality of the entity’s practices.

- Likewise, technological innovation is occurring at a startling and accelerating pace. The Internet, mobile devices, and ever-more-sophisticated computer technology (all connected to each other and always on) make it easy to collect, analyze, combine, reproduce, and disseminate data, thereby enhancing efficiency and cost-effectiveness but also escalating the risk of making catastrophic mistakes at the speed of light. Yet employees often do not really understand that the latest “smart” technology at work or home (TVs, appliances, toys or gadgets, automated fish tanks, security cameras, digital assistants, voice-controlled smart home hubs, etc.) could be invisibly eavesdropping on confidential discussions using connected microphones, spying via built-in cameras, or providing a new attack vector for accessing the organization’s digital assets.

Change is the watchword, and businesses and their cultures must be nimble in spotting trends and addressing issues that were not even on the radar screen months before.

Business leaders often breathe a sigh of relief once the state-of-the-art security system is installed and comprehensive data protection policies and

2. Please see Chapters 4 and 6 of this Handbook for further discussion about the types of legal and professional responsibility requirements placed on lawyers and law firms, which often include education and training.
procedures have been established. Yet notwithstanding adoption of the latest technology and sound data protection principles, businesses are only as strong as their weakest (human) link:

- The disgruntled or downsized “Gen X” employee who has it in for the organization and whose system access was not terminated on the last day of employment.
- The IT director who fails to install patches on a regular basis, thereby leaving networks vulnerable.
- The HR employee who leaves sensitive employee records unlocked or in electronic files with inadequate access restrictions.
- The associate who unwittingly compromises the firm’s client relationships through a lost laptop, phone, or unencrypted flash drive left on an airplane or in a taxi or rideshare vehicle.
- The super-connected, tech-savvy “Millennial” employee who overshares on social media and underestimates how that may sabotage the company’s confidential data.
- The road-warrior employee whose actions (or inaction) regarding the latest mobile technology (including “bring your own device”) may violate internal data security policies or rules of professional responsibility.
- The “Baby Boomer” senior partner who unleashes ransomware by clicking on a link that looks like it came from a colleague or board member.
- The administrative assistant who provides extensive client or firm information after receiving a fraudulent e-mail that appears to be coming from her supervisor or a firm or business executive requesting information.
- The third-party vendor who stores data overseas without appropriate security controls.

Countless studies, audit trails, and surveys over the years have repeatedly confirmed that the biggest data protection threats come from within one’s own organization. Most missteps are unintentional. Many mistakes can be avoided and risks can be minimized with appropriate training and awareness-raising. Yet this is often an overlooked component of data protection initiatives—the missing link when it comes to security.
B. What Does SMART Training Look Like?
What does training actually mean, and what are businesses doing to address data protection’s weakest link? Over the years, this question has been posed to CPOs drawn from various industries, locations, and corporate cultures, and a consistent pattern of answers has emerged. In short, when conducting training, businesses need to be SMART:

- Start training on hiring.
- Measure what you do.
- Annually provide training.
- Raise awareness and provide updates continually.
- Tailor training by role.

In considering these SMART training steps and what they mean for one’s business, it is important to keep in mind that the particular data protection training that is right for one entity is not necessarily right for another, even if they are in the same industry or are law firms of similar size. Businesses differ in many ways—for example, the degree of centralization, their corporate cultures, the jurisdictions in which they operate, their objectives, their resources and budget, their existing data protection infrastructure, their buy-in from senior management, and so on.

1. **S—Start Training on Hiring**
Given the fundamental role of data in everything a business does, training on how to protect that data should start on day one. Data protection training should be provided to all new employees and, increasingly, to contractors as well. In cases where it is not feasible to do such training for all employees initially (due to bandwidth, budget, or other constraints), businesses might choose to focus training on selected employees (e.g., HR personnel and those in key business roles or units).

---

3. Chapter co-author Ruth Hill Bro has posed such training questions since 2005 in her recurring column called *CPO Corner: Interviews with Leading Chief Privacy Officers*, which features 17 questions designed to identify trends and best practices, showcase the diverse range of CPOs, and capture key benchmarking and practical implementation information regarding data protection issues; see interviews posted at ABA, Section of Science & Technology Law: E-Privacy Law Committee, http://www.ambar.org/eprivacy.
In the employee context, training is provided as a part of employee orientation. Such training can take different forms, using a variety of media:

- An initial in-person, instructor-led session (large group, small group, or one-on-one, as appropriate), which can encourage interaction (but may not always be scalable or practical for some organizations in all situations), and/or
- An intranet/computer-based training module.

Coverage can include a wide range of topics, including:

- High-level overviews applicable to all employees and contractors;
- Instruction on relevant data protection laws and regulations (and professional rules of responsibility, where applicable), internal policies and procedures, fundamentals of the relevant technology, and industry best practices;
- Protecting confidentiality and security of data; and
- Steps to take when addressing a suspected data breach.

Such training should be coordinated with other training (regarding records management, code of conduct, etc.) and should be reviewed to avoid contradictions and conflicts in approach and message. Consideration should be given to whether the time, format, and content are suitable across different parts of the organization. Issues of translation, local law, and local customs can come into play here as well.

2. Measure What You Do

Measurement and assessment are a core component of many of these initial training sessions as well as in follow-up training. Administering tests (e.g., a graded online quiz) can help to confirm understanding and gauge the overall effectiveness of the training; it can also help to ensure that the work has actually been done. For example, employees and contractors could be required to correctly answer four of five assessment questions at the end of each training section. Broader measurements—such
as comparisons of incidents and types of missteps before and after training—can also help businesses to make training more effective while demonstrating return on investment (which can be important in making the case for budget).

3. **A—Annually Provide Training**
   It is prudent (and in some cases required under applicable law, rules, or policies) to ensure that employees annually receive a data protection training update, along with corresponding assessments or tests. Where relevant, certification or continuing legal education (CLE) or professional responsibility credit could be provided, thereby offering an additional incentive to do the training. Such follow-up instruction is often computer-based, so it can be deployed to diverse geographic locations and in a time frame that is convenient for the person receiving the training. Sometimes these annual updates are a part of annual recertification regarding business conduct guidelines.

4. **R—Raise Awareness and Provide Updates Continually**
   It is impossible to integrate appropriate data security practices into a culture by using just introductory training on hiring and mandatory annual training. To address this, businesses need to look for ways to raise data awareness and update employees on data protection on an ongoing basis. This is due to a number of factors, including the speed with which the issues change, the different ways in which people learn, the need for reinforcement, and so on. With ongoing awareness-raising, law firms and other businesses can integrate information security practices in such a way that they become as commonplace as turning on a computer.

5. **T—Tailor Training by Role**
   Going beyond high-level, one-size-fits-all training allows for training to be tailored to focus on specific roles of individuals, different generational challenges, and specific requirements for contractors and third parties. Tailoring of data protection training can take various forms, depending on the organization:
• Start with a Data Protection 101 online course that is available on demand (successfully completing it results in a certificate). The basic module can then be supplemented by training and awareness-raising specific to role (HR, those involved heavily in data handling, contractors, product design, engineering, sales, senior executives, lawyers, paralegals, administrative assistants, etc.), business unit, geographic location, and the like.

• Determine who should receive direct training from, or at least meet in person with, the CPO, CISO, CIO or IT director, legal counsel, or other qualified trainers. It is helpful for those tasked with training to meet with selected employees to learn about their data practices and then tailor training efforts accordingly. For example, some CPOs meet regularly with the company’s engineering, product design, and sales teams to raise important issues in planning meetings and gain insights to develop appropriate training.

• Ask data protection officers (or other relevant individuals) associated with the business lines to develop training and tools to enable the application of data protection policies to their respective areas.

• Hire specialists, internally or externally, to refine and enhance training efforts.

• Not all training and awareness-raising comes from within. Small firms or solo practitioners, those who lack specialized staff, and others looking for cost-effective approaches should take advantage of online training modules, relevant CLE courses and conferences, resources offered by bar associations (the American Bar Association and the ABA’s Sections, Divisions, and Forums; state and local bar associations; specialty bar associations; etc.), training publications, and the like.

• As noted above, training for some roles (e.g., lawyers) may be accompanied by certification or CLE or professional responsibility credit.

Businesses that use SMART training can provide the missing link that will help make data protection a part of the culture and turn their employees into one of their strongest links when it comes to protecting one of the most valuable assets of any business.
II. SMART Training in Action

Implementing a SMART training program does not have to be complicated or require significant budget. The program pays for itself by reducing the risk of data loss and increasing awareness about data protection.

A. Understanding the Basics of Employees: Role and Generational Differences

First, any training program should assess and understand the recipients of the training. As mentioned above, the role of the employee in the organization will make a difference in the type of training received. An associate working with e-discovery matters and technology every day will have different considerations than a mail clerk or even other associates and partners in the firm.

In addition, generational differences play a role in how training should be developed, the type of training and communication that a person prefers to receive, and how best to provide the training. Cam Marston, in his practical and often humorous book Generational Insights: Practical Solutions for Understanding and Engaging a Generationally Disconnected Workforce,4 discusses how each generation differs in its approach to learning:

- **Baby Boomers** (born 1946–1964) tend to continue to hold key leadership positions (e.g., partners) in the organization. They focus on work ethic and often measure it in terms of hours spent, rather than productivity. They value face time and relationships and seek loyalty. They look for those willing to put in whatever time is necessary to complete the task and support the team.5 When training Baby Boomers, it is critical to include preevaluation of technology skills and training that is participatory but not intimidating.6
- **Generation Xers** (born 1965–1979) often have a more entrepreneurial spirit and are focused on challenging or reinventing the status quo.

---

5. Id. at 33–34.
6. Id. at 39.
They tend to seek open communication, no matter their title or status. Unlike Baby Boomers, Gen Xers focus on productivity rather than time. They often seek a person, not a company, where their loyalty will lie. Training programs should address the Gen X employee’s career goals and be flexible, providing options and choices. For Gen Xers to see training as valuable, senior-level management must demonstrate its commitment to the training as valuable.

- **Millennials** (born 1980–2000) tend to be the most idealistic of the three groups. Unlike Gen Xers, who prefer to work independently with few checkpoints, Millennials want constant communication and positive reinforcement and prefer regular checkpoints at each phase of their work. Training programs for Millennials need to be group-oriented (where practical), interactive, and fun. They prefer that everyone be allowed to take a role in some part of the teaching as well as the learning.

Given the diverse nature of the workforce and the different means by which people learn and absorb information, any training or education campaign must integrate a variety of employee perspectives and capabilities and incorporate a variety of approaches.

**B. Building an Effective and Diverse Program**

Leveraging the **SMART** principles described above, any organization can quickly and easily build an ongoing training and education campaign.

First, it is critical to make the campaign fun and creative. While the message of data protection is serious, the delivery does not need to be. People of all generations tend to learn more through consistent messaging that has a direct impact on their lives. Those working on the data protection training should develop easy, fun, and catchy slogans that employees will remember.

---

7. *Id.* at 35.
8. *Id.* at 41.
9. *Id.* at 35, 37.
10. *Id.* at 42.
Get SMART on Data Protection

One example is the SAFE program, an information security awareness program that was developed for Option Care Enterprises, Inc. as a way to help employees remember how best to protect and secure sensitive information:

Secure the organization’s data: Where are you storing client data? How are you deleting it?

Asset protection: Do you know where your computer/iPad/phone is?

Friend or Foe: Who is sending you an email? Is it something you expected or phishing?

Encrypt: Are you encrypting sensitive emails before sending them out?

A program such as SAFE can be used throughout the year to educate staff; different themes within each of the four SAFE categories above can be featured.

Next, identify something, such as a mascot, that represents the organization and symbolizes data protection to help lighten the delivery of a serious message. For example, Option Care, which provides infusion services to patients in their homes, uses a mascot named “The Infuser.”

The Infuser’s motto is “Infusing Security into Everything We Do.” Every time employees see this mascot and message, they are reminded about protecting sensitive information. It is a fun, easy, and quick cue that costs very little to the organization to develop and implement.

Third, ensure that training is continuous, and use various methods to implement it. In addition to mandatory training at specific times (when employees join the organization and subsequent annual training), continuous education is key to any successful cultural transformation. The following are some ideas to keep the momentum going:

11. The SAFE program was developed by Option Care CISO Jill Rhodes, who is also an author of this chapter and co-editor of this Handbook. For further information on the program, contact Ms. Rhodes at jill.rhodes@optioncare.com.
Leverage current newsletters, and place brief articles within them that discuss data protection.

Conduct e-mail campaigns (monthly or as needed) with data protection guidelines, relevant media coverage, and so on to remind everyone (or otherwise make them aware) of relevant policies and practices.

Offer periodic “Data Protection Awareness Weeks” or “Security Awareness Drives” with guest speakers and other special events.

Strategically place wall posters and other communications that promote data protection.

Publish monthly articles on the company and line-of-business intranet home pages to raise data protection awareness.

Send periodic e-mails to highlight ongoing opportunities for online training and in-person sessions conducted by members of the data protection team or outside speakers.

Develop white papers and other material related to relevant data protection topics (aiming for greater frequency and detail over time).

Remind employees that data protection training is an important part of their job by including it as a factor in their annual performance evaluation; celebrate successes and reward those who meet the objectives (and, if needed, identify opportunities for growth and improvement).

Fourth, involve employees directly. Hold data protection competitions between divisions, offices, or floors in a building with the goal of identifying an employee/group activity that protected the organization’s information in a noteworthy way. Recognize the individual or group winners, name them in the monthly newsletter or blog, and provide a pizza lunch for the winner—the more recognition, the better.

Build an ambassador/liaison or similar program across the organization. Whether it is by office, region, subject matter expertise, or business unit, identify a way to have a data protection representative in each. Although senior leadership is important, the representative should be a mid-level employee who still has influence with peers, subordinates, and leadership. Meet with the data protection ambassadors/liaisons regularly to discuss data protection issues and (in line with the discussion about Millennials above) ensure that they are a part of the solution by having them serve as
the leaders who will train and educate the employees they work with on a regular basis.

Educate employees about how to protect data at home as well as in the workplace. Data protection does not start when a person logs into the network or end when she shuts down for the evening. Everyone’s family members and friends are constantly touching sensitive and/or personal digital data. Whether it is through social media or new mobile apps, data is being collected. By educating employees to protect data in all facets of their lives, they will approach data protection more holistically in their daily work life.

All of these methods are easy, cheap, fun, and effective ways to communicate and educate employees about enhancing data protection in the organization. As noted earlier, it is critical to find ways to measure the success of these campaigns (the “M” in “SMART” training).

C. Measuring Success (Through Phishing Campaigns and Other Means)
One of the easiest ways to measure the success of a campaign is to test employees by phishing them directly. Phishing normally occurs when a malicious e-mail is sent either directly to an individual (spear phishing) or to many in the hope that the target will click on a link within the e-mail and then spread a virus that could infect the individual’s computer, at a minimum, or the entire enterprise network. Ransomware, discussed throughout this Handbook, has often been caused by phishing.

As part of a SAFE campaign (Friend or Foe), organizations can implement their own company-wide phishing campaign, sending “malicious” e-mails to employees, as someone trying to harm the organization would do. When an employee clicks on the e-mail, instead of infecting the system, the employee receives an educational message about the phishing e-mail and the fact that had it been real, harm could have come to the organization. This type of campaign measures the click rate and, when conducted regularly, can be used to monitor those who are clicking regularly. As a result, specific training can be developed for those individuals or groups. Phishing programs provide a quantitative measurement related to security awareness.

Reporting numbers also can provide both quantitative and qualitative opportunities for measuring success. As more training and education occurs, the number of incidents reported to appropriate leadership will also increase.
Increased reporting could be anything from the reporting of a specific data breach or loss incident to reporting of phishing e-mails. As these incidents are tracked, greater information becomes available about employee knowledge and understanding of data protection.

In the end, a data breach or loss will most likely occur as a result of something an employee did or did not do. The best way to prevent such missteps is to educate the people in the organization about how they can better protect the information around them.

III. Ten Key Points

1. Make data protection a part of the corporate culture and the job of every individual.
2. Recognize that the biggest risks to data come from the people working for the organization and that training and raising awareness are essential to reducing those risks.
4. Recognize that one size doesn’t fit all; it is important to undertake training that fits a business’s own needs.
5. Build a program that represents the organization’s employees both from a role perspective and a generational one.
6. Make any training campaign fun and interesting—let the employees lead it through ambassador/liaison programs and in other ways.
7. Train employees on how to protect information in all facets of their lives, not just in the workplace. By helping them protect their family and friends at home, they will further integrate these practices at work.
8. Reward! Reward! Reward! Use competitions with prizes to further induce employees to become more aware and supportive of data protection across the organization.
9. Measure success through phishing programs and tracking of reporting of incidents and responses.
10. Know that training and awareness-raising is a never-ending journey (not a destination) that can require changes in direction in response to changes in the law, technology, media coverage, and one’s own experiences and new business initiatives. Adapt accordingly, while keeping message delivery mechanisms light and easy to understand for all of the people who work for the organization.
Additional Resources


EEOC Guidance

“What you Should Know About the ADA, the Rehabilitation Act and the Coronavirus,” https://www.eeoc.gov/eeoc/newsroom/wysk/wysk_ada_rehabilitaion_act_coronavirus.cfm.