The American Bar Association
Young Lawyers Division
2016 Fall Meeting
Detroit, MI

Data Breaches and Cyber Security — Are You Ready?
(CLE)

Westin Book Cadillac Hotel
Friday, October 21st
10:15 a.m. - 11:15 a.m.
Claudia Rast is a shareholder based in Butzel Long's Ann Arbor office. Blending her expertise in law, business, and science, she assists companies in their strategic use of technology, counseling companies in the areas of privacy, cybersecurity, data theft, intellectual property licensing and registration, and the forensic preservation and analysis of electronically stored information. With the rise of cyber events in recent years, her background in forensics, IT environments, and security has become invaluable in working with clients to both defend against and respond to pervasive cyber-attacks. Similarly, Ms. Rast is frequently called upon to negotiate contracts covering the innovative technologies associated with autonomous and connected vehicles, to address security, privacy, IP ownership, and new and potential regulations.

During 2008-2009, she chaired the American Bar Association’s Section of Environment, Energy, and Resources, and in 2013, Rast was appointed by the ABA President to the Cybersecurity Legal Task Force, for a two-year ending in August 2015, and recently re-appointed by the incoming ABA President to another one-year term beginning in August 2016. Rast has been named as a technology industry leader in “Crain’s Detroit Business” and as one of the top 20 Michigan women in computing by the Ann Arbor chapter of the Association for Women in Computing. In 2015, Rast was named to Michigan Lawyer’s Weekly “Leaders in the Law.” She is a frequent speaker on the topics of cybersecurity, privacy and social media. Her publications include the CPA’s Guide to Privacy (Thomson Reuters/Bisk Education 2006, 2012, 2014 & 2016) and a chapter on Privacy & Data Breach for Thompson Reuters’ “Inside the Minds” Aspatore Book series (April 2013).

Rast received her B.S. from the University of Michigan and her J.D. from University of Detroit School of Law, where she was the editor-in-chief of the law review. After law school, she clerked for the Chief Justice of the Michigan Supreme Court. In 2014, Rast completed the course, “Tackling the Challenges of Big Data,” developed and taught by the faculty of the MIT Computer Science and Artificial Intelligence Laboratory in collaboration with MIT Professional Education.
Brigadier General Charly Shugg, USAF (Retired), is a Partner and Chief Operating Officer of the Sylint Group, Incorporated. In that capacity he provides strategic guidance and insight for an elite team of cyber security and digital data forensic professionals providing security strategy and incident response to Fortune 500 companies, non-profit organizations and government entities. In his last Air Force position, he was responsible for providing trained and ready cyber forces to plan and conduct worldwide cyberspace operations. General Shugg was a key architect and strategic planner of the U.S. Air Force’s cyberspace operations program and crafted concepts of operations for multiple worldwide organizations to include USCYBERCOM. In addition, he was the Commander of DoD’s Unmanned Aircraft Systems (UAS) Center of Excellence charged with creating unified UAS concepts of operation. General Shugg has been a featured speaker at numerous UAS and cyberspace events.
Todd Taylor serves as a Member and co-leader of Moore & Van Allen's Commercial & Technology Transactions practice group, as well as its Privacy & Data Security group. Todd focuses his practice on outsourcing, licensing, data privacy and security, technology and supply chain matters.

Before joining Moore & Van Allen, Todd served as an in-house attorney at Bank of America, where he worked extensively on various technology licensing, supply chain, cross-border and third party servicing arrangements.

Mr. Taylor has been engaged to speak for several programs on the topic of data breaches and cyber security including the most recent presentation: “Effective Data Security Management: Keeping Your Data Protected in the Cloud.” Todd has also published several articles regarding the issues surrounding emerging threats and recent developments in corporate cyber security.
Mr. Major is a partner and co-leader of McCarter & English’s Government Contracts & Export Controls Practice Group. Mr. Major focuses his practice on federal procurement, cybersecurity liability and risk management, and litigation. A prolific author and thought leader in the area of cybersecurity, his professional experience involves a wide variety of litigation and counseling matters dealing with procurement laws and federal regulations and standards. His diverse experience includes complex litigation in federal court under the qui tam provisions of the False Claims Act and bid protest actions. He counsels all sizes of companies on issues relating to compliance with government regulations including, among other things, cybersecurity (NIST, FIPS, FedRAMP, and DFARS) requirements, multiple award schedule compliance, Section 508 issues, country of origin requirements under the Buy American and Trade Agreements Acts, cost accounting, and small business requirements. He also regularly conducts internal investigations to assist companies ensure that they are in full compliance with the law. He is an editor of and contributing author to the Cloud Computing Legal Deskbook (Thomson Reuters), an annual publication addressing cloud computing issues and solutions for commercial and government end users and suppliers.

Mr. Major is a retired U.S. Air Force intelligence officer who most recently served as a U.S. Air Force Academy Admissions Liaison Officer for the state of Maryland in the Air Force Reserves.
Richard Rivera is an Associate in the Litigation and Intellectual Property Practices of Smith, Gambrell & Russell, LLP. Mr. Rivera works both in the Litigation and Intellectual Property Practice Groups. His litigation practice is focused on commercial litigation, with a special emphasis in defending actions brought under consumer protection statutes, such as the FDCPA, FCRA, TCPA, and their state-level counterparts. Mr. Rivera is available to assist in most business disputes.

Mr. Rivera’s intellectual property practice is concentrated in advising clients in matters involving intellectual property (trademark and copyright), compliance with state and federal laws governing sweepstakes and other promotional activities, software and internet technology, marketing, and licensing issues. Mr. Rivera also prosecutes trademark and copyright registrations before the United States Patent and Trademark Office and the United States Copyright Office.
CLE Materials
Lawyers & Cybersecurity: Threats, Liabilities & Best Practices

Claudia Rast  |  Butzel Long  |  Ann Arbor, MI  |  rast@butzel.com

Oct. 21, 2016
“Law firms are very attractive targets. They have information from clients on deal negotiations which adversaries have a keen interest in. They’re a treasure trove that is extremely attractive to criminals, foreign governments, adversaries and intelligence entities.”

-- Harvey Rishikof, co-chair of the ABA Cybersecurity Legal Task Force
The Risks to Law Firms

• In 2012, Mandiant estimated that 80% of the 100 largest US law firms were subject to successful data breaches by malicious intruders in 2011.

• March 4, 2016: FBI sends Private Industry Notification
  – “Criminal-Seeking-Hacker” Requests Network Breach for Inside Trading Operation
  – Financially motivated insider trading scheme targets international law firm information
  – Monitoring for material non-public information

• Panama Papers—40 years of client data
  – 2.6 TB (50,000 boxes; 125,000,000 docs)

• March 29, 2016: Crain’s Chicago Russian Hackers seek Elite Chicago Law Firms’ M&A work

• April 20, 2016: FBI Ransomware Alert
Sources, Targets & Risks: It’s Us!

**Source**
- Mobile Computing *(controlling BYOD)*
- Social Media *(online & customer service)*
- Big Data

**Target**
- Critical Infrastructures *(financial, political, energy, water, transportation, ports, manufacturing, chemical, etc.)*
- Trust Infrastructures *(finance, insurance, accounting, legal)*
- The Cloud *(who owns, who controls, where located)*

**Risks**
- Communication Breach: Data Center ↦ ≠ Board Room
- Target Breach: Auto Breach Detection turned “Off” by IT
Why Law Firms are Easy Targets

- Mobile Lawyers & Staff
  - Ubiquitous “Public” WiFi
- Diverse “Work” Venues
  - Conference Centers
  - Hotels
  - Home
  - Foreign Travel
- BYOD
- IoT
- IOLTA Accounts
- Client Trade Secrets
- Client Contacts
- Website “Success Stories”
- Document Management Systems--encryption
- PCI Compliance
The Many Ways to Get “In”

- Device Theft/Loss
- Misuse of Camera/Mic/GPS
- Device Configuration
- Poor Passwords
- Preboot Malware Alters OS
- Faulty OS (Zero-Day vulnerability)
- Malware Injection
- ID Theft (esp. w/same Password across apps)
- Policy Failure (Company; ISP)
Once “In,” What Can They Do?

- Create/modify/delete/execute programs
- Upload/download files
- Create/delete/directories
- List/start/stop processes
- Modify system registry
- Take screenshots of user’s desktop
- Capture keystrokes
- Capture mouse movements
- Harvest passwords
- Start interactive command shell
- Create a remote desktop interface
- Enumerate users
- Enumerate other systems on the network
- Set system to “sleep” (go inactive)
- Log off the current user
- Shut down the system
Deconstructing a Cyber Attack...
Detecting the SpearPhishing Emails

- **Spelling and bad grammar.** Cybercriminals are not known for their grammar and spelling. If you see mistakes in an email, be cautious.

- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message.

![Example links](https://www.woodgrovebank.com/loginscript/user2.jsp) ![Example links](http://192.168.255.205/wood/index.htm)
Detecting the SpearPhishing Emails

• **Threats.** Cybercriminals often use threats that your security has been compromised, sending threats stating that your account would be closed if you don't respond to an email.

• **Spoofing popular websites or companies.** Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.
From: Apple <Apple-id@service>
Date: Friday, 21 February, 2014 9:17 AM
To: "@sheridanc.on.ca" <@sheridanc.on.ca>
Subject: We inform you that your account is about to expire in less than 48 hours

Dear (e) client (e),

We inform you that your account is about to expire in less than 48 hours, it is imperative to conduct an audit of your information for now, otherwise your account will be destroyed. Just click the link below and craft a session using your Apple ID and password...

Check now>

Hovering over the link reveals it points to a non-Apple site - "http://affiliadobomb.com/vb/id_apple/upd"

why this electronic courier you he was sent? The sending of this email applies when the expiration date of your account expires. For more information, see Questions and Answers. thank you, Assistance to Apple customers.

Poor wording and grammar
Dear client,

You are receiving this notification because your Salesforce SSL certificate has expired. In order to continue using Salesforce.com, you are required to update your digital certificate. To download a new Salesforce digital certificate, please visit:


According to our Terms and Conditions, failing to renew the SSL certificate will result in account suspension or cancellation:

http://www.salesforce.com/company/privacy/security.jsp

Thank you for using Salesforce.com

Hovering over the link reveals it points to a non-Salesforce.com site: "class.icinfo.cn/salesforce_ssl_cert.zip"
.cn is for mainland China

Be wary of .zip files
Forged Organization Link

Forged email address

This link downloads malware.

This link downloads malware.

This link downloads malware.
Ethical Obligations for the Legal Professional

• **Duty of Competency: Model Rule 1.1**
  – A lawyer shall provide competent representation
    • And “keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology”

• **Duty of Communication: Model Rule 1.4**
  – A lawyer shall keep the client “reasonably informed about the status of the matter”

• **Duty of Confidentiality: Model Rule 1.6**
  – A lawyer must take reasonable precautions to safeguard information relating to the representation of the client

• **Supervisory Duty: Model Rule 5.1**

• **Responsibilities Regarding Nonlawyer Assistants: Model Rule 5.3**
Breach Costs & Risk Protection

- Average cost per compromised record in 2014: $201
  - For “malicious” attacks: $246/record
  - Compare: Average cost per compromised record in 2010: $210
  - Average cost per compromised record in 2006: $138
- Companies with Incident Response Plan in place
  - Paid $17 less per compromised record
- Companies who alerted customers too soon
  - Paid $15 more per compromised record
- Building the Effective Cyber Risk Culture
  - Engage executive leadership
  - Target cyber risk management and awareness
  - Implement cost-effective technology investments tailored to needs
  - Adopt relevant cyber risk information sharing
Detection: Search for Anomalies & Events

• Detection is a waiting game...
  – Understand a baseline of your network operations
  – what is “normal” for users and systems?
  – Assess unusual or anomalous events including system use and malicious code
  – Determine the impact of the event
  – Elevate events to key personnel

• CISA and Monitoring/Sharing: It’s changed the rules under EPCA
Cyber Liability Insurance

- Data Breach: Failure to protect an individual’s privacy – **1st Party Costs**, Notification, Forensics, Legal Assistance, Credit Monitoring, PR Firms.
- Data Breach: Failure to protect an individual’s privacy – **3rd Party Costs**, Defense Costs & Settlements
- **Network Security**: Loss or damage to a network & data, 1st & 3rd Party (may include lost income)
- **Media Liability**: Web content (Libel, Defamation)
- **Fines & Penalties** (HIPAA, PCI)
- **eVandalism & Extortion**
- **Property loss** from Cyber Perils (Internet of Things)
Best Practices for Individuals

- Set **Browser Security** to Std established by IT
- Do not Borrow a **flash drive** from someone you don’t know; if you’re unsure, have IT scan it
- Never share **passwords**
- Do not click on **links from untrusted sources**—if you’re unsure, forward to IT
- If an **email seems suspicious**, call the sender; always double-check before sending any sensitive data
- **BYOD**—cell phones, iPads, tablets, etc. implement security; mobile device mgt (remote wipe)
Best Practices Overall

- Perform Risk Assessment (Physical Plant, IT Systems & Workforce)
- Segregate & Secure High Risk Information, Operations & Workers
- Encrypt Sensitive Data/Implement Robust Password Policy
- Implement Company-wide Training (Ongoing)
- Incorporate Security By Design
- Cyber Liability Insurance
- Enable Network Security Monitoring & Review of Log Files
- Demand Compliance from Contractors & Suppliers
- Conduct Table-Top Drills
- Have Experts at the Ready If/When an Attack Occurs
RANSOMWARE CONSIDERATIONS:
PREPARATION AND BUILDING A PLAN OF ACTION

Brigadier General Charly Shugg

The Sylint Group
240 N. Washington Blvd. Suite 600
Sarasota, FL 34236 USA

+1.941.951.6015
cshugg@usinfosec.com
RANSOMWARE (CLIENT OR FIRM)

How does it work?
Ransomware is malicious software (malware) designed to encrypt local and network-based files and demand a ransom for decryption. Payment of the ransom is frequently requested in bitcoins (a relatively untraceable currency) via anonymous internet sites.

Remediation Options
Pay the ransom (BitCoin or other anonymous currency)
- Price
- Receive encryption key
- No response

Do not pay the ransom
- Backup Data (Off line, Restore Point, Time to Restore)
COULD IT HAPPEN TO YOU?

Online cyber-criminals and other nefarious attackers are constantly looking for new ways to access users’ systems and then monetize this access. Common methods of breaking into systems are through interactions with a user, often with email attachments (phishing) or internet browsing (drive-bys). Once criminals have access, they can perform any number of activities.

One of the more popular attacks by cyber-criminals is called a “ransomware” or “encrypting malware” attack, where the fraudster infects a computer with malicious software designed to encrypt user files and hold them hostage until payment of a ransom. From a criminal perspective, this is a relatively safe means of making money:

- the victim is ‘happy’ to pay for the return of their files
- there is little perceived harm if the files are returned
- the amount of money charged is frequently less than the cost to respond otherwise

However, these attacks can significantly damage operations, destroy critical systems and irreversibly corrupt data.

In order to better prevent or respond to an attack, it is important to understand the basics behind an attack and the functionality of the malware.
ATTACK METHODOLOGY

An attack starts with a user accidentally executing a small file from an email or website that starts the infection and encryption process. These malicious files are resistant to detection by anti-virus because they change signatures rapidly and use common Windows® commands in their attacks.

Once the file is downloaded and executed on the system, it connects to the internet in order to get some needed components and then begins to encrypt files on the local computer and on network shares accessible from that computer. Files initially targeted for encryption are often the anti-virus definition files and similar preventative applications, which then prevents the system from defending itself against the malware.
ATTACK METHODOLOGY

After the files are encrypted, users are notified of the event and provided some means of contacting the attacker and getting the key, or ‘decrypter’. While some older ransomware attacks used reversible encryption routines or left a trail on the system that could be used to decrypt the files, attackers have generally learned from their ‘mistakes’ and developed new ways of preventing any type of reverse engineering or unlocking.
When preparing for or responding to an attack, there are a number of important considerations that may lessen the likelihood or impact of an encrypting malware attack. There are different degrees of preparation and different techniques.

Preventative steps can prevent the attack in its entirety (e.g., removing mail and internet access), lessen the spread of the attack (e.g., limited access and connections between systems), warn of an ongoing attack (e.g., endpoint sensors) and blunt the effect of the attack (e.g., backups that can be restored).

Responsive steps can assist in controlling the damage and prevent subsequent re-infections or other collateral impact.

**Before**

1. Check Backups
2. Minimize access to network shares
3. Implement mail filters and web proxies
4. Use process monitoring and application whitelisting tools to supplement antivirus

**After**

1. Suspend backups to avoid overwriting good data
2. Stop network shares to prevent spread
3. Review logs to identify culprit
4. Preserve evidence for investigation
PREPARATION & RESPONSE

Preparation

There are effective ways to prevent, or at least significantly mitigate the risks from, encrypting malware attacks. Antivirus may have little effect at stopping the malware because the rapidly changing signatures and malicious tools are difficult or impossible to distinguish from legitimate tools. While AV is still a necessary tool, better defenses include:

- Proxies (e.g., ZScaler, Websense) that monitor user connections to the internet and only allow connections to sites that are known good or have acceptable levels of risk. This can help prevent the initial malware download and can also disrupt the connectivity between the computer and the internet sites that have encryption instructions.

- Incoming mail filters (e.g., Proofpoint) that scan mail and attachments prior to arrival to remove high-threat attachments and identified phishing messages. This can help prevent infected messages from reaching the end-user.

- Application white-listing solutions (e.g., Bit9, McAfee FIM) that prevent programs from executing unless they are on a pre-defined list. This prevents the malware from running.

- Process monitoring tools (e.g., CarbonBlack, Cylance) watch for suspicious applications and generate warnings when unexpected events occur.
PREPARATION & RESPONSE

Preparation Con’t

Before an attack occurs, it is critical to have tested and verified backups of critical systems. This will blunt the attacker’s strategic position in that files can be recovered with little data loss. Time can also be well-spent before an attack by reducing the number of mapped drives available to ‘everyone’, and limiting mappings and permissions to only the smallest population possible. If an infected computer and associated user does not have access to a network share or file, then the contents won’t be maliciously encrypted. Network files are frequently over-shared to people that do not have a job requirement for access, which needlessly increases the exposure and risk of files being encrypted during an attack. For each of the steps in the attack process, there is an opportunity for successful defense, highlighted in the diagram below.
PREPARATION & RESPONSE

Response

Once an attack has begun, there are certain steps that can reduce the impact and assist in the remediation process. A summary of potential response steps includes:

- Shut down shared connections to prevent continuing encryption
- Suspend backup jobs to prevent replacing clean files with encrypted copies that will not restore
- Identify endpoints running suspicious files:
  - Review network connections made to affected shares to identify endpoints
  - Deploy process-monitoring tools to endpoints to detect suspicious files and processes
- Review firewall log and endpoint activity to ensure no simultaneous attacker activity is occurring, as encrypting malware attacks are sometimes used as diversions
PREPARATION & RESPONSE

Response Con’t

(1) Containing the malware, (2) identifying the infected system(s) and (3) suspending backups should be the response priority. Since the malware works by reaching out over the network to connected computers and shares, initial containment can be done by removing network shares and disconnecting mapped drives. While containing and identifying the affected systems, stopping backup processes is necessary to prevent backing up the encrypted files and overwriting older, unencrypted data. Since malware signatures may not be effective, other endpoint tools must be used to detect the malicious files and infected system(s). Sometimes, log files on file servers that were encrypted can be reviewed to look for indicators of systems connecting to large numbers of shares or files simultaneously. Systems that have encrypted files in the root and system folders (e.g., c:\, c:\windows) are usually indicative of systems that are running the encrypting malware, since these folders are not otherwise available via the network. If the encryption process has completed, it is not uncommon for the malware to remove itself. If this is the case, it may be difficult or impossible to find the initial compromised systems unless sufficient logging and analysis solutions are in place prior to the attack.

Once infected systems have been identified, network shares can be brought back online and backups restored. Because of various regulatory requirements, preserving evidence to allow an investigation into indications of data access or exfiltration also becomes important. If a ransom has been paid and decrypter provided, care should be taken that attackers do not introduce different malware or backdoors into the system through the decrypter. Additionally, system and access logs should be reviewed for any indicator that the attack was not a diversion from a more insidious attack.
SPECIFIC ACTION ITEMS

Note: Each case is different, and some of these may or may not apply.

1. Identify Infected Machine via Log Analysis or Endpoint Agent Analysis
2. Contain the Encryption Process until Endpoint is Identified
3. Prevent Reoccurrences
**SPECIFIC ACTION ITEMS:**
**IDENTIFY INFECTED MACHINE VIA LOG ANALYSIS OR ENDPOINT AGENT ANALYSIS**

1. Create a list of servers with encrypted files. On these servers, check Security Event Logs (security.evtx) for users and machines that have connected to the shares with encrypted files.

2. If a process-tracking agent (e.g., CarbonBlack®) is installed, check for endpoints with large numbers of network connections (e.g., NetConn > 5000). This is indicative of the malware reaching out to various network locations and changing files. There are false-positives due to backup and antivirus jobs, but these should be easily filtered out by associated process.

3. Start reviewing machines identified in (1) for evidence of malware. Remember that antivirus may not detect the malware, but tools such as pslist (https://technet.microsoft.com/en-us/sysinternals/pslist ) may show suspicious running files. Infected machines will also likely have encrypted files in local directories (e.g., c:\users\...) whereas machines reached over a network connection will only have shared directories encrypted. Preserve any identified endpoints for future analysis.
SPECIFIC ACTION ITEMS:
CONTAIN THE ENCRYPTION PROCESS UNTIL ENDPOINT IS IDENTIFIED

1. Forcibly disconnect file shares on the file server(s) to stop any currently connected devices.

2. Check share permissions as well as folder permissions and limit permissions to specifically necessary users (not groups). This will limit the potential impact/reach of an infected device.
SPECIFIC ACTION ITEMS: PREVENT REOCCURRENCES

1. Review Mail Filter settings to specifically block Office files with embedded macros and scripts.

2. Review Web Proxy settings to block known and suspicious malicious sites by reputation, and ensure all user browser activity runs through the proxy.

3. Configure watchlists in process monitoring tools to watch for (a) large number of network connections and (b) executables running from Temporary Internet and Outlook folders.
DATA AWARENESS WITHIN THE FIRM

Awareness is key. Make sure your firm can answer the following questions:

1. Who creates “sensitive data”?

2. How is it shared between client and office staff?

3. Where is it stored?

4. How is it protected (at rest and in motion)?
BASIC CYBER HYGIENE FOR FIRMS

Ensure that your firm implements these procedures:

• Access Control

• Encryption (at rest)

• Two Factor Authentication (VPN, Cloud Apps)

• Process Monitors (Endpoint Security / Mobile Device Management)
FURTHER QUESTIONS?

We are experts in advanced technologies, techniques and proven investigative protocols to uncover fraud, malicious conduct, sabotage or other nefarious activities. Sylint has been cited in Westlaw, and has been appointed Special Master to the court in technically complex cases. We have presented numerous cyber security presentations at national cyber security conferences. Our cyber security firm is dedicated to maintaining the highest levels of integrity and ethics in providing our clients with superior cyber investigative and protective services.

Feel free to contact me at cshugg@usinfosec.com if you have any questions or wish to discuss further.
Cloud Privacy & Security for Clients and Lawyers: A U.S. Perspective
CLOUD SERVICES OVERVIEW
Overview of Cloud Services

• In early 2016, RightScale conducted a survey of 1600 tech professionals about the use of cloud computing by their organizations:

- 95% of Respondents Are Using Cloud

- Public Cloud Only: 18%
- Hybrid: 71%
- Private Cloud Only: 6%

Public = 89%
Private = 77%

Source: RightScale 2016 State of the Cloud Report

• According to Synergy Research Group, operator/vendor revenues from cloud services were over $110 billion between Q4 2014 – Q3 2015.
Types of Cloud Services

- **Public Cloud** – services and infrastructure are provided via the Internet to multiple entities.

- **Private Cloud** – services and infrastructure are maintained on a private network (can be onsite or offsite) for single entity.

- **Hybrid Cloud** – integrated cloud service combining elements of both Public and Private Cloud.

- **IaaS** – Infrastructure as a Service.

- **PaaS** – Platform as a Service.

- **SaaS** – Software as a Service.
FEDERAL LAWS, REGULATIONS & GUIDANCE IMPACTING PRIVACY AND SECURITY FOR CLOUD SERVICES
Examples of Federal Data Privacy/Security Laws Impacting Cloud Services

• The Federal Information Security Management Act, 44 USC §3551 et. seq. ("FISMA") – Covers federal agencies and federal contractors who access federal agency databases or information.

• Gramm-Leach-Bliley Act 15 USC, 15 USC §6801- 6809 ("GLBA") – Requires financial institutions to protect security and confidentiality of their customers’ non-public personal information.

• The Fair and Accurate Credit Transactions Act, 15 USC §1681w ("FACTA") – Among other things, contains destruction requirements for consumer reports.

• The Health Insurance Portability and Accountability Act, Pub. Law 104-191 ("HIPAA") & the HITECH Act, 42 USC §§300jj et. seq. & 17901 et. seq. -- Sets out privacy and security obligations of “covered entities” (i.e., health plans, health care clearinghouses, and health care providers).
Examples of Federal Data Privacy/Security Laws Impacting Cloud Services (cont.)


- **Consumer Financial Protection Act**, 12 USC §5481 et. seq. (the “CFPA”) – Prohibits (among other things) unfair, deceptive and abusive practices with respect to consumer financial products and services.
FEDERAL LAWS, REGULATIONS & GUIDANCE: BREACH NOTIFICATION
Federal Data Breach Response & Notification

There is no generally applicable data breach notification law requiring notification by Federal agencies to impacted individuals.

- **FISMA** –
  - In the event of a breach, an impacted federal agency is required to notify US-CERT (a sub-department of DHS).
  - The agency may also need to notify law enforcement and the Office of the Inspector General.
  - There is no requirement under FISMA to notify individuals regarding a data breach.

- **OMB 2007 Guidelines**
  - Under OMB guidelines, federal agencies should engage in a cost-benefit analysis when determining if an external notification to affected individuals is appropriate. Agencies should weigh various factors (e.g., the type of data involved, the likelihood of harm, etc.) in determining whether an external notification to affected individuals is required.
Federal Data Breach Response & Notification: HIPAA/HITECH

• **Notification** -- Covered entities under HIPAA/HITECH must, following the discovery of the breach of unsecured protected health information, notify the impacted individuals in writing (via first class mail, or if previously agreed to by the impacted individuals, email).

  ➢ Subject to certain exceptions, notice be provided no later than 60 calendar days following notice of breach. However, upon request of law enforcement, notice can be delayed if the notice would impede a criminal investigation or damage national security.

  ➢ Depending on size of the breach, prompt notice may also need to be provided to HHS and Media.

• **Notice by Business Associates & Vendors** -- *Notification requirements also exist for business associates and certain third party service providers under HIPAA.*
Federal Data Breach Response & Notification: GLBA

The GLBA Interagency Guidelines for financial institutions contain detailed guidance regarding addressing data breaches. Specifically, an institution's data breach response program should contain procedures for:

- assessing the incident, and identifying the systems and information accessed or misused;
- notifying its primary Federal regulator as soon as possible;
- notifying appropriate law enforcement authorities;
- taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- notifying customers of a security incident involving the unauthorized access or use of the customer's information.
FEDERAL LAWS, REGULATIONS & GUIDANCE: DATA SECURITY
Federal Data Security Laws: Governmental Agencies

- **FISMA** -- Very specific requirements for inventory of information systems, security controls, security plan, risk assessments, certification/accreditation, and continuous monitoring.
Federal Data Security Laws: GLBA

- **GLBA** – Requires financial institutions to protect security and confidentiality of their customers’ non-public personal information.

- **Interagency Guidelines Establishing Information Security Standards** – These are regulations imposed under GLBA, they require financial institutions (among other things) to:
  - maintain an information security program designed to ensure confidentiality of customer information and protect against unauthorized access and anticipated threats to such information; and
  - develop a risk based response program to incidents of unauthorized access to customer information systems.

- **The FTC Safeguards Rule** – Implements GLBA’s requirements for entities under FTC jurisdiction.
Federal Data Security Laws: HIPAA

The HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164)

- The HIPAA Security Rule applies to protected health information in electronic form and requires covered entities to implement certain administrative, physical, and technical safeguards to protect this electronic information.

- **Covered entities must have contracts or other arrangements in place with their business associates that provide satisfactory assurances that the business associates will appropriately safeguard the electronic protected health information they create, receive, maintain, or transmit on behalf of the covered entities.**

- Civil and criminal penalties can be imposed for violations of the HIPAA Security Rule.
Federal Data Security Laws: General

- **Section 5 of FTC Act** – The FTC has used its authority under Section 5 unfairness standard to pursue companies for poor security practices.
  
  - *FTC v. Wyndham* Hotels, 799 F.3d 236 (2015) — FTC alleges Wyndham violated Section 5 by failing to maintain “reasonable and appropriate data security” for consumer data.

- **Sections 1031 & 1036 of the CFPA** – CFPB has authority to prevent unfair, deceptive and abusive acts or practices by covered persons and their service providers in consumer transactions relating to consumer financial products or services. 12 U.S.C. §§ 5531(a) & 5536(a).
  
  - The CFPB recently brought first successful data security enforcement action against a payment platform: *In the Matter of Dwolla, Inc.*, File No. 2016-CFPB-0007.

- **FACTA** -- Requires companies that have records containing consumer reports or derived from consumer reports to take reasonable steps to protect the records when disposing of them.
Federal Guidance Impacting Data Security in Cloud Services Arrangements

• OCC 2013-29
• CFPB 2012-03
• FRB Guidance on Managing Outsourcing Risk (12/5/13)
• FFIEC Booklets and Guidance (e.g., Supervision of Technology Service Providers; Outsourced Cloud Computing)
• HHS Guidance on HIPAA Security Rule
• NIST Guidance Documents
• FTC Start with Security Guide (June 2015)
STATE LAWS & REGULATIONS IMPACTING CLOUD SERVICES
State Breach Notification Laws and Regulations

- Widespread Adoption – Currently 47 states have adopted some form of data breach notification laws.

- Protect “personally identifiable information” – State data breach laws, generally speaking, protect a name in combination with other data (e.g., driver’s license#, ss#, financial account numbers – sometimes in combination with passcode), if not publicly available.

- Notice Requirements -- There is some variation in notice requirements across the states, but notice to affected persons (and/or governmental agencies) is typically triggered when data holder reasonable believes there has been disclosure/access to NPI by an unauthorized person of information not rendered unusable when use of the information has occurred or is reasonably like to occur.
Examples of State Data Security Laws and Regulations

- **California Civ. Code §1798.81.5** – Businesses that own, license or maintain personal information shall implement and maintain reasonable security procedures and practices.

- **Conn. Gen. Stat. §42-471** – Any person in possession of another’s personal information shall safeguard the data, computer files and documents containing such personal information; shall ensure that such data is erased, destroyed or rendered unreadable prior to destruction; and, if SSNs are collected, shall publicly display a privacy protection policy.

- **Massachusetts Safeguards Rule** (ALM GL ch. 93H; 201 CMR 17.00) --
  - Persons owning or licensing personal information shall have a comprehensive written information security program setting forth administrative, technical and physical safeguards.
  - If PI is electronically stored, the info. sec. program must cover computers and wireless systems.
  - Requires oversight of service providers.

- **Nev. Rev. Stat. Ann. §§ 603A.210 & 603A.215** -- Requires, among other things: (a) data collectors maintaining records of PI to implement and maintain reasonable security measures, (b) business entities accessing payment cards for sale of good/services to comply with PCI DSS, and (c) electronic transmission of PI not subject to PCI DSS requires encryption.
Other State Laws Impacting Cloud Services: Uniform Trade Secret Act

Under the Uniform Trade Secret Act, a trade secret is any "information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”
INDUSTRY RULES AND STANDARDS IMPACTING CLOUD SERVICES
Examples of Industry Data Security Standards

• Payment Card Industry Data Security Standard (PCI DSS) –
  - PCI DSS was originally adopted by Visa, MasterCard, Discover, American Express and Japan Credit Bureau.
  - PCI DSS sets forth minimum technical and operational requirements for the protection of cardholder data.
  - PCI DSS applies to all entities involved in payment card processing – including Merchants.


• NIST 800-53 – a set of security controls promulgated for U.S. federal information systems and their third party service providers by the National Institute of Standards and Technology.
OTHER MATTERS IMPACTING CLOUD SERVICES
E.U. & Foreign Privacy Rules

• DON’T FORGET THE E.U.!
  - EU Data Protection Directive 1995
  - General Data Protection Regulation 2016

• Other Foreign jurisdictions also have data privacy laws and regulations impacting transactions and other legal matters.
Litigation Concerns with Cloud Storage

- Under Rule 34 of Federal Rules of Civil Procedure, a party to litigation can be required to produce documents and electronically stored information in a party's possession, custody, or control.

- Similar rules exist at state level as well.
Cyber/Data Breach Insurance can include coverage for:

- third party claims (including, in some cases regulatory and PCI fines),
- initial forensic response,
- repair of network damages,
- notification of breach victims,
- lost revenues,
- business interruption,
- cyber extortion, and
- reputational damages.
CLOUD SERVICES: THE IMPACT ON LAWYERS AND LAW FIRMS
Lawyers and the Cloud: Ethics Rules

- **MRPC 1.1 – Competence**
  
 Comment 8 -- “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”

- **MRPC 1.6 – Confidentiality**
  
  Rule 1.6 (c) -- A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

  Comment 18 – “…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”
Lawyers and the Cloud: Ethics Rules (cont.)

- **MRPC 5.3** – Supervision of Non-Lawyers
  
  - **Rule 5.3(b)** -- “a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer[.]

  - **Comment 3** – “A lawyer may use nonlawyers outside the firm to assist the lawyer . . . includ[ing] . . . using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer’s professional obligations. The extent of this obligation will depend upon the circumstances, including . . . the terms of any arrangements concerning the protection of client information[.]”
Lawyers and the Cloud: Ethics Opinions

At least 20 states have issued ethics opinions approving the use of cloud computing or data storage services by lawyers.

- Opinions require that lawyers and law firms take reasonable efforts to protect data housed in cloud or data storage services.

- Common themes in opinions include the need for lawyer/law firm to:
  
  - perform adequate due diligence on providers;
  - maintain written agreements with cloud vendor regarding confidentiality, security and back-up of data;
  - ensure that lawyer/law firm maintains access to and control of data, and notice of data incidents;
  - periodically reexamine security measures used to protect data; and
  - obtain client consent for storage of sensitive information.

- A few examples of ethics opinions include: 2011 FEO 6 (NC), Formal Ethics Opinion 2011-200 (Pa.), Ethics Opinion 842 9/10/10 (NY), and Advisory Opinion 2215 (Wash.).
Outside Counsel Policies

• DON’T’ FORGET OUTSIDE COUNSEL POLICIES!

• It is a fairly common practice for client in-house legal departments to impose outside counsel policies on law firms that may go above and beyond requirements of ethics rules and opinions for data security.
Moore & Van Allen

Todd C. Taylor
toddtaylor@mvalaw.com
(704) 331-1112
The Information “Superhighway”…

…is more like a beach.
Beaches are fun…
...but you need to see the whole picture...
…before deciding how much fun.
Risk Management is the Key

- Measuring risk is a function of assessing:
  - Threats
  - Vulnerabilities
  - Impacts/Consequences
  - Countermeasures/Preparedness
A Broader Look at “Threat”

What is a cyber threat?

- Hackers/Hacktivists
- Competitors
- Foreign state actors
- Nature
- Employees
- Regulators
- Insurance companies
- Data
  - Type
  - Location
  - Ownership
A Deeper Look at “Vulnerabilities”

- Software bugs
- Broken processes
- Ineffective controls
- Hardware flaws
- Legacy Systems
- Vendor systems
- Employees
- Privacy laws
- Owner restrictions
The Cornucopia of “Impacts”

- Business disruption
- IP theft/loss
- Supply chain infection
- Financial losses
- Reputational damages
- Regulatory fines
- Law suits
- Loss of life
Countermeasures

Compliance vs. Security vs. Proportionality

- Know what you need
- Know what you should have
- Find the right balance

Share your process internally with Audit, Risk, IT, Legal, etc.

Careful not to waive privilege or not be able prove your compliance program.
So what do you do?

YOU’RE GOING TO NEED

A BIGGER BOAT
So what do you do?

- **Don’t be shark bait!** Prepare with a bigger boat
- Know your company data sphere (data systems)
- Know who your experts are (internal and external) who know where the information is
- Have the tools (like Nuix) to access, analyze, and provide the information required
- Matter-of-fact, factual, clear, and calm communications… ALL documented (even if post verbal conversation). Don’t want any miscommunication or misgivings
…It can be done! Coexist.
Ask me how I know…
There’s a lot out there...be ready.

Questions?
We’re here to help...

Alexander W. Major | Partner
McCARTER & ENGLISH, LLP

T: 202-753-3440
C: 410-935-0037
F: 202-354-4604
amajor@mccarter.com
Additional Articles of Interest
THE HUMAN VULNERABILITY

Why the cybersecurity industry has been fighting the wrong battle for 20 years—and how we can reclaim the surrendered ground

by Chris Pogue
Senior Vice President, Cyber Threat Analysis
We are engaged in an information war; a battle to control data in every aspect of our lives. Over the past 20 years, organizations have spent billions of dollars and expended countless hours to protect our most critical information assets.

If all that effort and expenditure had been effective, I would never have built a 15-year career as a penetration tester and computer crimes investigator. In that time, I worked on or oversaw thousands of security assessments and investigations.

This white paper is the culmination of more than six months of research. It has been a labor of love to find a credible answer for that most elusive of questions: why. Why had an entire industry with some of the most intelligent people on the planet fallen so short of its objective? Why are we so consistently defeated by cybercriminals?

Why? All the time I spent in the trenches, all the lessons I learned as a result of the work I performed taught me an undeniable truth: Cybersecurity is not a technology problem; at its heart, it’s a people problem. For two decades we’ve been designing security technology to solve technology problems; in essence, we’ve been fighting the wrong battle. If technology has a role, and I sincerely believe it does, it must be to help solve people problems.

I joined Nuix in 2014 with a singular focus—to help more people. Working at Nuix has made it possible to integrate the intelligence and lessons I learned from all these investigations into a software platform. And not just me—Nuix has hired security professionals with all kinds of skills and experience complementary to mine and incorporated their knowledge into its technology. Together, we are creating a true intelligence multiplier, the likes of which the cybersecurity market has never seen. In short, it’s a game changer.

By merging field knowledge with the power of the Nuix engine, we will give our users an unparalleled capability to deflect, detect, react, respond to, and recover from cybersecurity incidents. This is the missing link that will enable security professionals to reclaim the precious ground we have surrendered to cybercriminals.

Shifting direction, after two decades, will be far from painless for security practitioners and the industry. It is my sincere desire that after reading this work, the industry understands what needs to be done to stem the tide of data breaches, and summons the courage to take action.

I leave you with the words of the 28th President of the United States, Woodrow Wilson: “You are here in order to enable the world to live more amply, with greater vision, with a finer spirit of hope and achievement. You are here to enrich the world.”

Let’s do this!
EXECUTIVE SUMMARY

Over the past 20 years, organizations have expended billions of dollars’ worth of time, energy, and intellectual property pursuing the elusive “next big thing” in cybersecurity. At countless security conferences around the world, vendors have touted their technological achievements and proposed their solutions to scores of hopeful attendees. Despite the collaborative efforts of the entire cyber-industrial machine, very little progress has been made. In fact, by all accounts, the threat landscape has actually gotten worse.

A cursory web search will identify article after article describing data breaches, system hacks, and security faux pas. These incidents happen every day, in every industry, on every continent, targeting every type of data that conceivably holds monetary value. It does not take a brain surgeon to see that whatever the cybersecurity industry has been doing for the past two decades has, very simply, failed. This fact is illustrated in Figure 1 showing the numbers of reported breaches and exposed records in the United States over the past ten years.

Continuing along this path is obviously a fool’s errand, in lockstep with what Albert Einstein so accurately defined as insanity. Instead, I took a step back and asked that most important of all questions: why? Why have so many very smart people spent so much money and effort and made such little progress?

This prompted me to completely reassess the way I was thinking about cybersecurity and start to research the subject in a very different, non-linear manner. I looked outside of the technology industry to see if any other industries had faced similar problems in the past. If they had, how did they solve them?

For approximately six months, I devoured any literature on the subject I could get my hands on—books, industry reports, and news articles on business problem solving, specifically focusing on how organizations identified problems, which approaches were successful and which ones failed, and how long it took to move from identification to definition and ultimately resolution.

My research revealed one industry that faced and solved similar problems, and one whose creative journey to address a dissimilar problem gave me valuable insight that I could apply to the cybersecurity industry. These industries are manufacturing and world healthcare—specifically, the fight against communicable diseases.

In this white paper, I will define the problem facing the cybersecurity industry. I will show that insufficiently defining and therefore inappropriately addressing the problem is the reason for almost two decades of failure. I will then clearly lay out a more comprehensive strategy to address the evolving threat landscape and how the cybersecurity industry can reclaim much of the ground that it has surrendered.

In short, we have all been fighting the wrong battle with the wrong weapons and wondering why we’re not winning the war. So hang on and keep reading; that’s all about to change.

![Figure 1: Annual number of data breaches and exposed records in the United States from 2005 to 2015.](image-url)
THE CEREBRAL VULNERABILITY

The human brain consists of about 200 billion neurons—nerve cells that are linked together by trillions of connections called synapses. As the tiny electrical impulses that make up brain activity shoot across each neuron, they have to travel through these synapses, each of which contains about 1,000 different switches that route each electrical impulse. In total, one human brain contains hundreds of trillions of these neural pathways. This enables our brains to be capable of an amazing 1,016 complex processes per second, which makes them far more powerful than any computer currently in existence. Pretty cool, huh?

For example, researchers in Japan used almost 83,000 processors of one of the world’s most powerful supercomputers, the Fujitsu K, to connect 1.73 billion virtual nerve cells to 10.4 trillion virtual synapses (with 24 bytes of memory in each synapse). In total, this added up to around one petabyte of memory, which is the equivalent of about 250,000 standard personal computers. Even with all this technology, the researchers were able to mimic just one percent of one second’s worth of human brain activity. Their experiment still took 40 seconds to replicate the amount of human brain activity that occurs in the time it takes you or me to blink.

Even though our brains behave so much like supercomputers, they are far from perfect. Philosophers, scholars, and behavioral psychologists have tried for millennia to understand the brain’s nuances and unravel the mysteries of why we make the decisions we make. For example:

- Why does the same set of factors drive one person into action but another to do nothing?
- How can a group of people all see the same event yet each individual walk away with a different interpretation of what happened?
- What drives one person to risk their life for people they have never met and another to take life from those they love?
- Why do some people give freely from what little they have and others take greedily to grow their increasing surplus?

The human brain is fascinating, complex, and powerful, but clearly nowhere close to being perfect.

Cognitive Biases: Bugs in Our Brain Software?

One of these imperfections is a group of cerebral deficiencies known as cognitive biases. A cognitive bias is a limitation in our brain’s ability to process information sufficient for us to make conscientious decisions. Some psychologists believe our cognitive biases help us process information more efficiently, especially in dangerous situations, so our instinctive fight-or-flight mechanism has an advantage. While these biases may be useful in, say, avoiding being eaten by a bear, they also sometimes lead us to make grave mistakes, in many cases without our ever being aware of what we are doing.

Cognitive biases also refer to a systematic pattern of deviation from normal or rational judgment, whereby we draw illogical inferences about other people or situations. Individuals create their own subjective social reality from their perception of the input they receive. An individual’s construction of social reality, not the objective input, dictates their behavior in the social world. Thus, cognitive biases may sometimes lead to perceptual distortion, inaccurate judgment, illogical interpretation, or what is broadly called “irrationality.”

Some cognitive biases also enable us to make faster decisions when timeliness is more valuable than accuracy. An example of this is heuristics, rules that people use to make decisions without necessarily knowing all the facts. Other cognitive biases come about because humans lack the appropriate mental mechanisms to process certain types of information (bounded rationality) or don’t have the capacity to process it in large volumes.

In the world of computers, we call this a vulnerability.

Philosophers, scholars, and behavioral psychologists have tried for millennia to understand the brain’s nuances and unravel the mysteries of why we make the decisions we make.
WHAT IS A BREACH?

In calculating the number of data breaches recorded in the United States in any given year, the Identity Theft Resource Center defines a breach as “an incident in which an individual name plus a Social Security number, driver’s license number, medical record, or financial record (credit/debit cards included) is potentially put at risk because of exposure.”

Similarly, the Ponemon Institute's 2015 Cost of Data Breach study, sponsored by IBM, defines a breach as “an event in which an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format.”

To put it simply, a data breach is any unauthorized party gaining access to protected information for the purposes of benefiting from the theft and subsequent utilization or manipulation of that information.

Every data breach, regardless of the complexity of the attack or the environment in which it occurs, can be broken down into four stages: infiltration, propagation, aggregation, and exfiltration (see Figure 2).

To put this into non-technical terminology, let’s use the example of a bank robbery. A criminal who wants to rob a bank needs to do four things:

• Break into the bank
• Move from the point of entry to the location of the money
• Put the money in a bag
• Make their getaway.

If the criminal fails to perform any one of those actions, the robbery fails.

A data breach is no different. In every data breach, the attacker must:

• Gain access to the target environment (infiltration)
• Move from the point of entry to the location of the targeted data (propagation)
• Harvest the data (aggregation)
• Move it from a system controlled by the victim to a system the attacker controls (exfiltration).

Many aspects of a breach are arguably more complex, but overall, that is how it works. It’s pretty simple, and something that has come to be commonly referred to as the breach breakdown.

Figure 2: The four stages of a data breach.
THE INFILTRATION CAUSATION

The vast majority of cybersecurity activity is focused on preventing the first stage of the breach breakdown: infiltration. (There are plenty of things we can do to make the other three stages harder for cybercriminals, but that’s a whole other discussion.) What makes infiltration possible?

According to the 2015 Ponemon Institute study, “Hackers and criminal insiders cause the most data breaches. Forty-seven percent of all breaches in this year’s study were caused by malicious or criminal attacks.” The study further indicated that 25% were caused by human error.

Let’s do the math: 47% + 25% = 72%. That means the remaining 28% were caused by system glitches. Well, what’s a system glitch?

The report defines a system glitch as a failure of IT and business processes. So it’s not a human being actively making a mistake (because that would be a human error), but neither is it a random and unpreventable event. True, power outages, internet service provider issues, hardware failures, and natural disasters happen and can have unpredictable downstream effects on a computing environment. However, the study is talking about process failure. Presumably, those processes that failed were developed and implemented by humans. Computers are stupid—they do exactly what humans tell them to do. The more logical explanation for these glitches, therefore, is a human being failing to tell the computer to do the right thing.

Let’s face it—that 28% attributed to system glitches simply isn’t accurate.

Additionally, let’s think about who is making these assertions that data breaches were the result of systems failures. It is most likely someone within the organization who knows how the systems are supposed to work and what failure looks like. More than likely, these are the same individuals responsible for some aspect of their company’s cybersecurity posture, if not all of it. To admit that the system didn’t work as planned would mean admitting personal failure, since they are likely responsible for security design or implementation, or both. Humans are very bad at admitting fault, a phenomenon called externalization.

Internalizing Success, Externalizing Blame

When something good happens to someone, their natural response is to internalize the responsibility for that thing as something they caused. “Look what I did,” or “Look at how great I am.” I may be paraphrasing, but you get the idea. You will probably not be shocked to learn that the natural human response to something bad happening is the exact opposite—externalization rather than internalization. When something goes wrong in our lives, we tend to look for some way to project blame onto somebody or something else. Obviously, we are far too skilled and wise to commit such an error, so therefore there must be another party to blame. It’s not MY fault, it’s YOURS. I didn’t do this, THE COMPUTER did.

One of the key findings of my research is that technology is rarely the cause of data breaches. In the more than 2,500 breaches I have investigated, I can count exactly zero that were caused by a random, non-human-initiated system failure.

I am not saying they never happen, just that a basic application of Occam’s razor tells us the cause is much more likely to be elsewhere. (Occam’s razor, or the law of parsimony, is a concept attributed to a 14th century Franciscan friar named William of Occam.i This principle states that when you must choose between several potential scenarios, the one that requires the least number of assumptions is most likely to be correct.) When presented with the two possibilities of complex system glitches or a simple human error, Occam’s razor leans pretty heavily towards human error.

Since there are only a few human-machine hybrids in all the world,¹ I am going to go out on a limb and make what I believe to be the logical assumption that 100% of hackers, malicious insiders, unknowing insiders, and IT and business personnel are human beings. Whether they are attackers (internal and external) seeking to do damage or employees simply making mistakes, 100% of breaches are the result of human behavior.

One of the key findings of my research is that technology is rarely the cause of data breaches—in the more than 2,500 breaches I have investigated, I can count exactly zero that were caused by a random, non-human-initiated system failure.
On Becoming the Underdog

Success or failure is not something binary, a one or a zero, the presence of a charge or the absence of it. There is something else that drives success or failure apart from simple ability and skill. That “thing” represents the essence of what make us human: desire, motivation, drive, and the relentless pursuit of a goal.

If skill and ability were all it took to be successful, sports teams with the most skilled and highly rated athletes would always win. But that’s not the case, is it? Sports history is littered with talented teams who fell to underdogs that figured out a way to work together and achieve victory. This is one of the most compelling reasons to watch sports.

In 1969, the New York Mets had not placed higher than ninth in their first seven seasons as a Major League Baseball team. The odds of them winning the World Series that year were 100-1. Nonetheless, the Mets won more than 100 games that season and went on to be the unlikely World Series champions.

The United States Winter Olympic hockey team in 1980 was seeded seventh in a field of only 12 teams. After upsetting a superior Czechoslovakian team en route to a 4-0-1 record in bracket play, the Americans came to face the Soviet Union in the semifinals of the first medal round. Earlier that year, the same team had lost 10-3 to the Soviets and they were not expected to do much better in this tournament. Yet somehow, the “Miracle on Ice” team of amateurs found a way to win 4-3 against the “best” hockey team in the world at the time. The US then went on to beat Finland 4-2 in the gold medal game, completing an impossible championship run.

So what is the connection between cybersecurity and sports? This is really important. Just like in sports, the success of an organization’s cybersecurity program relies on more than the technical skills of the people who are responsible for the plan. If all that mattered was technical skill, it would simply be a case of knowing that you had to segment the network, deploy firewalls, and use dual factor authentication (for example), and WHAM … you’d be secure.

But it doesn’t work that way, does it?

We are human beings, and we have flaws in the way we think, in the way we interact with other human beings, and in the emotional substance of our decision-making process. Understanding these flaws, and identifying the human aspect of the workplace, is the first and arguably one of the most critical steps we can take in ultimately overcoming them; becoming the underdog and beating the superior opponent.

The Missing Link

Over the past 20 years, the security industry has focused on technology to solve its complex problems. Yet despite decades of research and the myriad security vendors, products, and technological advancements that have emerged year after year, the threat landscape is stronger today that it has ever been, with no signs of abating.

Since no problem is unsolvable, we’re compelled to wonder what critical information has eluded cybersecurity companies and prevented them from stemming the tide of data breaches. I believe this missing link to be human beings.

As I mentioned earlier, I’ve conducted or overseen more than 2,500 data breach investigations during my career. The overwhelming majority were not the result of failures in technology, but of poor decision-making by the people responsible for the victim organization’s security program. Decisions such as using weak or default passwords, leaving open remote access, improperly configuring firewalls, not segregating networks, and using poorly designed or coded applications. These remain among the primary attack vectors cybercriminals use to infiltrate their targets.

In each of these scenarios, the attacks were 100% preventable; the knowledge and the technology existed to prevent the breach from ever taking place. A human being was either ill-informed as to the steps that were required to implement adequate security controls, or simply made the choice to not implement them.

We’ve established that data breaches are the result of human activity. It’s clear that the technology and security knowledge exists to prevent successful breaches. The next logical question is: “Why would someone who knows better make such a poor decision?”

As I sought to find an answer to this question, my research led me identify several factors that play a part in formulating the overall solution. Each has to do with the way we think and act as humans. I don’t think cybersecurity will progress in any meaningful way until we confront and address these issues.
COGNITIVE BIASES

As I've discussed earlier, cognitive biases are tendencies formulated in our brains that can lead to illogical decision making or poor judgement. For many years, psychologists have studied how these biases affect business and economic decisions, interpersonal relationships, and geopolitical relations. Through introspection, training, and role playing, it is difficult (but not impossible) to retrain our brains to behave differently.

Psychologists have identified scores of biases and broken them down into categories including decision making, belief, behavioral, social, and memory error biases. For the purposes of my research, I have focused on five decision-making biases that appear to have the greatest impact on cybersecurity professionals. I believe these are the primary obstacles preventing us from making better choices, ultimately leading to the degraded protection of critical information assets in our care.

Normalcy Bias

If a plumber fixed a leaky pipe in your home, would you expect him to test his work, making certain the leak was fixed before calling the job complete? If you took your car to a mechanic to have your air conditioning serviced, would you expect that he would check to make sure cold air was blowing before saying the job was done? Of course you would! In just about every aspect of business, there is a logical expectation that once services have been performed, there is a mechanism in place to ensure that things are running the way they should.

In many instances during my tenure, I have seen organizations spend hundreds of thousands of dollars on defensive countermeasures and then fail to test them adequately once they were in place. In the rare instances where they performed some testing, it was usually automated or trivial, designed to test specific features against a canned data set rather than to evaluate strategic enhancements to the organization’s security posture. This sort of post-deployment testing, which is increasingly common, in no way adequately represents a realistic attack.

It has always baffled me that behavior which would never be acceptable in any other line of business is almost universally accepted in cybersecurity. Why?

Normalcy bias drives our brains to believe that since something catastrophic, such as a data breach, has not happened in the past, it will not happen in the future. We therefore illogically minimize the possibility of a breach and its potential impact on the organization.

History has shown (and I have said many times) there are really only three types of organizations: those that have been breached, those that are breached, and those that are about to be breached. This is the reality of the current threat landscape.

However, as a result of normalcy bias, we dismiss important tasks such as security technical testing of defensive countermeasures. We postpone vital steps such as creating an incident response plan, testing that plan, conducting realistic response training scenarios, and providing companywide security awareness training—or we take them off the security roadmap entirely in favor of other, more bottom-line-related activities.

Neglect of Probability

Neglect of probability, similarly to normalcy bias, leads decision makers to disregard the probability an incident occurring; we ignore or largely overlook risks and ignore the continuum of the extremes.

You don’t have to be a computer scientist (I’d like to see a rocket that works without computers) to realize that data breaches occur every day despite our seemingly best efforts. It is logical to assume that if your organization stores, processes, or transmits any data of value, it will be a target for attackers—if it hasn’t already become so. I believe many key decision makers fail to accept this fact because of this bias.

While the exact probability is difficult to calculate, it should be obvious by now that just about every type of organization with computing resources will suffer a significant security incident in the foreseeable future. Multiple reports (including the Verizon Data Breach Investigation Report, the FireEye Threat Intelligence Reports, the IDT911 ITRC Data Breach Report, The Experian Industry Forecast Report, and the Ari Kaplan Advisors Defending Data report—see “References and Further Reading” on page 19) indicate that data breaches are on the rise on every continent and in every business vertical. Not accepting this reality is foolish and inappropriately optimistic. It will happen.
COGNITIVE BIASES cont

The Ostrich Effect

The ostrich effect refers to the common (albeit false) belief that an ostrich, when faced with danger, will hide its head in the sand—if it can't see the danger, it doesn't exist. This cognitive bias refers to the similar tendency humans have to ignore problems in the hope that they will go away. Unfortunately, bad guys do bad things and bad stuff happens, whether our heads are in the sand or not.

The truth is that bad things happen to good people; in relation our specific set of circumstances, it does not matter if you are a non-profit providing drinking water to poor children in Africa or an online pornography vendor. If you store process or transmit data that has a black market value, you will be targeted. The sooner everyone everywhere realizes this, the sooner they can start preparing accordingly. Pull your head out (of the sand). This is for real.

Parkinson's Law of Triviality

When I first began to read about Parkinson's Law of Triviality (sometimes referred to as bike-shedding), I immediately felt like it applied to cybersecurity professionals. However, I didn't want my research to be impacted by my own cognitive biases, so I wanted more than a feeling. It wasn't until I attended the 2016 RSA Conference in San Francisco, California, that it made sense. (To be fair, the RSA conference is not the only place this phenomenon is present but it was on my mind while I was there.)

This bias is that humans assign a disproportionate weight to things they understand, and much less to things they don't understand, totally independently of how important those things are.

Here is an easy example. I have had countless conversations about cybersecurity that focus on antivirus (AV), firewalls, and intrusion detections systems (IDS) as the “magic trio” of countermeasures to thwart ne’er-do-wells (I had to work that word in somehow). There is no question those technologies should be part of every organization's defensive posture, but they are nowhere near comprehensive. Many organizations that suffered data breaches had all those technologies in place, so logically their mere presence is not enough to stop attackers. What gives?

The explanation is that most people can wrap their heads around linear solutions such as AV, firewalls, and IDS, while they struggle with more dynamic concepts of vulnerability management, defense in depth, strategic countermeasures, and threat simulations. So instead of tackling the larger, more complex issues, Parkinson's Law of Triviality drives them to focus on the smaller, less complex issues and to think that they are more important than they really are.

CURSE OF KNOWLEDGE

I found the curse of knowledge to be one of the most interesting biases for a variety of reasons. Its mere existence provides a glimpse into the human psyche is that simultaneously illogical and yet completely logical—a cerebral paradox if you will.

When an individual amasses expertise in a certain field, it is understandably the result of many years of research, study, and practical experience; this knowledge is the summation of all of their efforts. However, as their knowledge grows, so does the potential for hubris directed at others who do not have the same level of expertise. They become disdainful of the traits they worked so diligently to overcome.

There is a fine line between confidence and arrogance. During my career, I have often contemplated where this line resides, and how to navigate it in such a way that I am just confident enough to do my job. If I am too confident, then I am arrogant; not confident enough, then I appear to be weak. It is a challenge to be certain, but not an insurmountable one.

Over the years I have come across many people who, for whatever reason, do not share in my understanding or efforts. This failure to understand and control one's intellectual maturity acts as a firewall for any ideas that are not self-generated. I believe this bias is directly responsible for many of the poor decisions we see during cybersecurity incidents.

The most common manifestation of this bias takes form in statements such as “Don’t tell me how to do my job,” and “I’ve been doing this for 15 years, I know what I’m doing.” These statements reveal the curse of knowledge cognitive bias at work, as well as a certain degree of emotional immaturity.

The realm of cybersecurity is so multidimensional, it is simply not plausible to think that any one person know enough to be competent in every possible area; it's madness really.

Think of an inverted pyramid (see Figure 3) whereby the more the individual learns, the more he realizes what he doesn’t know. The curse of knowledge is exactly the opposite in the mind of the impacted individual. They think they know so much but in truth they don’t know enough to even realize how much they don’t know.

Figure 3: The curse of knowledge
THE FAILURE OF THE HUMAN SYSTEM

Data breaches are almost always framed as technical failures. If you read enough media statements issued by organizations that suffered data breaches, you will see a common script: The breaches were the result of super-sophisticated attackers who exploited a completely unknown vulnerability to gain access to the highly protected target systems. All these organizations overstate the technical complexity of the breach, while understating its impact. In just about every instance, they never mention the potential for or presence of human failure.

For further evidence, think about the checklists used in governance, risk, and compliance (GRC) régimes. They all contain volumes of technical security controls dictating how to configure systems, what types of passwords to use, how to deploy firewalls, etc. None of them contain guidance on decision making, staffing, or security strategy. This makes sense if everyone believes we are facing a technical problem; technical solutions solve technical problems. Right? Wrong!

Data breaches are human failures. I refuse to believe that in the past two decades an entire industry full of very smart people has completely failed to develop technology sufficient enough to prevent systems from being compromised.

In fact, the 2015 Defending Data Report found 93% of respondents thought human behavior was the biggest threat to their organization’s security. The Experian 2015 Data Breach Industry Forecast Report says “Employees and negligence are the leading cause of security incidents but remain the least reported issue.” Finally, the 2015 BakerHostetler Data Security Incident Response Report found “human error is most often to blame” in the clients the firm sampled. Specifically, 37% of the breaches the firm litigated in the year leading up to the report’s publication were the direct result of human error.

We are clearly facing a human problem that our industry has been unwilling or unable to address for over 20 years. So my research led me to look outside the cybersecurity industry to see if others had experienced similar human problems and how they solved them.

Two examples were instructive:

- The way the World Health Organization (WHO) combats the threats of communicable diseases
- The way the industrial manufacturing industry has addressed machine-related accidents on assembly lines.

The Ebola Epidemic

In 2013 the World Health Organization was called on to combat the largest and most complex Ebola outbreak on record, in West Africa. By the time the WHO declared the epidemic over, on November 29, 2015, it had identified more than 28,000 cases of Ebola resulting in more than 11,000 deaths.

Colin McIff, Health Attaché to the US Mission to the UN in Geneva, told me the major challenge WHO faced was not a breakdown in medical science—after all, the organization has been handling the spread of communicable diseases for years. Rather, this particular instance was a breakdown in human behavior.

“Depending on the disease, human behavior change can be the most important factor in getting it under control,” he said. “Ebola in West Africa was exactly that situation as a person is actually most infectious just after they died. Local customs for both Christians and Muslims required elaborate burial rituals that brought people in close contact with the highly infectious loved one (very sad really).

“WHO has been rightly dinged for their slow performance in response and this is one of the key factors—they didn’t have anthropologists and local community experts in the loop soon enough to help with the messaging and outreach and it cost us.”

We are clearly facing a human problem that our industry has been unwilling or unable to address for over 20 years.
Theories of Accident Causation

In 1931, Herbert William Heinrich first published his book *Industrial Accident Prevention: A Scientific Approach*. In a famous diagram (see Figure 4), Heinrich summarizes that management controls man failure (knowledge, attitude, fitness, and ability) which causes or permits unsafe acts of persons and unsafe mechanical or physical conditions, which cause accidents. Heinrich’s “domino theory” argued that injuries resulted from accidents; accidents from unsafe acts; which in turn occurred from the faults of people; which had their origin in the social environment.

He theorized that:

- 88% of workplace accidents were caused by unsafe acts (usually by the injured person)
- 10% of workplace accidents were the result of unsafe equipment or conditions
- The remaining 2% were unavoidable.

Nine items make up the unsafe acts that cause 88% of accidents as shown in the Figure 4.

After reading these components, I thought for a long time about how these findings could map to the failures we see in cybersecurity. My mappings are in the table below:

<table>
<thead>
<tr>
<th>CAUSES OF INDUSTRIAL ACCIDENTS</th>
<th>CAUSES OF CYBERSECURITY INCIDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Operating without clearance, failure to secure or warn</td>
<td>Operating without sufficient technical knowledge</td>
</tr>
<tr>
<td>2 Operating or working at unsafe speed</td>
<td>Failure to use the system as it was intended</td>
</tr>
<tr>
<td>3 Making safety devices inoperative</td>
<td>Failure to properly use prevention mechanisms</td>
</tr>
<tr>
<td>4 Using unsafe equipment, or equipment unsafely</td>
<td>Failure to follow documented procedures</td>
</tr>
<tr>
<td>5 Unsafe loading, placing, mixing, combining, etc.</td>
<td>Failure to implement appropriate configuration settings</td>
</tr>
<tr>
<td>6 Taking unsafe position or posture</td>
<td>Failure to take a proper defensive posture</td>
</tr>
<tr>
<td>7 Working on moving or dangerous equipment</td>
<td>Unnecessary interaction with critical computing assets</td>
</tr>
<tr>
<td>8 Distracting, teasing, abusing, startling, etc.</td>
<td>Failure to understand the severity of the situation</td>
</tr>
<tr>
<td>9 Failure to use safe attire, or personal protective devices</td>
<td>Failure to implement proper security controls</td>
</tr>
</tbody>
</table>

Figure 4: Chart of direct and proximate accident causes from Heinrich’s *Industrial Accident Prevention: A Scientific Approach*. 
THE FAILURE OF THE HUMAN SYSTEM cont

Changing Behavior to Prevent Accidents

Heinrich argued that the best way to prevent injuries was to stop accidents from happening. Since the immediate cause of accidents was unsafe acts, eliminating these was the most effective focus of injury prevention programs.

This is the premise of behavior-based safety (BBS) and other industrial safety programs: changing workers’ behavior is the principal means of reducing the number and severity of workplace accidents.

Behavior-based safety applies the science of behavior change to real-world problems. It analyzes what people do and why, then uses an intervention strategy to change that behavior.

A successful BBS program must include all employees, from the CEO to the frontline workers, contractors, and sub-contractors. Achieving changes in behavior requires changes in policy, procedures and systems. These require buy-in and support from all involved in making those decisions.

BBS is not based on assumptions, personal feelings, or common knowledge; it must be based on scientific knowledge.

However, regulators such as the US Occupational Safety and Health Administration do not necessarily focus on the behavioral aspects of the job. One commentator I read accused OSHA of being “all about compliance and findings” and “more comfortable with problems it can see on a clipboard.”

The Connection to Cybersecurity

I found this aspect of BBS programs eerily similar to something security experts have identified and echoed for many years: A successful security program must be holistic. It is a business issue, not an IT issue. Without top-down commitment, evangelization, and support acceptance, ultimately integration at the lower levels of the organization will be impossible.

As with a successful BBS program, a successful cybersecurity program must keep everyone—the CEO down to the newest intern—in lockstep, myopically focused on the singular goal of making the organization safer.

This is also very similar to the way the US military trains during peacetime. I served in the US Army for 13 years in the Field Artillery and Signal Corps. Our primary mission was to remain combat ready at all times.

We trained as if we would be deployed tomorrow, giving rise to the concept train as you fight. We drilled our minds and our bodies each day for one singular purpose: going to war. Likewise industrial manufacturing operators should perform their duties as if a safety incident were just around the corner and cybersecurity professionals should prepare their organizations as if a breach was going to take place at any moment.

The (All Too) Common Causes of Accidents

Digging deeper into BBS programs, I spoke to Rob Caillet, Environmental Health & Safety and Security Manager at a General Electric facility in Fort Worth, Texas that manufactures large locomotive engines. When I asked him what he observed to be the primary social factors present during and after accidents, he told me accident victims usually said something like:

- “I’ve worked on this equipment for 15 years. I know what I’m doing.”
- “What could happen? I’m only working on X.”
- “All that safety stuff is for other people.”
- “This kind of thing won’t happen to me.”
- “That accident has never happened before.”

There it is!

The main cause of failure in the WHO’s handling of the Ebola epidemic and in workplace accidents was exactly the same as the one I identified in the cybersecurity industry. Not medical science, not mechanical failure, not gremlins or system glitches, but human beings who experience the same cognitive biases no matter what job they do and regardless of their physical or intellectual capacity.

I also noticed a very clear correlation between OSHA’s compliance-driven approach and that of GRC regimes such as the Payment Card Industry Data Security Standards, the Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes–Oxley. The manufacturing industry figured out the hard way that checklists and process guidelines will not solve the underlying problems of safety and security because human behavior is the common denominator. Try as you might, you cannot simply provide a checklist and expect people to change.

Like it or not, we are the problem.
THE PATH BEFORE US

Now we can see that this is a human problem, the logical conclusion is that we need a human solution. This is where it gets tricky.

Do we keep trying the same things we’ve been trying for close to 20 years with no visible impact? Or do we take a lesson from WHO and the manufacturing industry, and implement a solution that has proven to be successful? Specifically, should we stop trying to solve the problem in a linear, technical manner and shift to a more human-centric approach?

Consistent with Heinrich’s theory, I believe we should engineer out as many manual intersection points as possible. By reducing the number of times human beings need to make a decision, we minimize the opportunity for mistakes. Then, for those areas where human interaction is inevitable, provide comprehensive training and simulations to better prepare individuals to make those decisions.

This would foster a marriage of human intelligence and technology in a manner that the cybersecurity industry has not adopted to any significant degree.

In my experience, network and security operations centers (NOCs and SOCs) use mechanisms such as AV, IDS, or security incident event management (SIEM) solutions to look across huge numbers of alerts. As a result, actual malicious activity is frequently buried under the volume of false positives.

In most cases, the configuration settings of these monitoring solutions have not been adjusted during an actual threat scenario. (Often these systems remain at their default settings or have nominal adjustments made by the vendor at disparate intervals). This means the tools are not configured to spot an actual attack in progress. In my experience, this capability is vital for an organization to defend itself during an attack and to conduct comprehensive investigations afterward.

In addition, many of the individuals working in these centers have never been trained on correlating the alerts they see with actual human activity; creating a widening knowledge gap that prevents them from being truly effective.

Even if their tools were configured properly, performing as intended, and displaying alerts of actual, no-kidding attacks, the humans sitting in the SOC or NOC lack the knowledge to understand what they are looking at, why it’s important, and what to do about it.

There are organizations that are doing this really well today, but the rest are spending vast sums of money on tools and technology in the hopes of protecting their critical data. Unfortunately, they are falling short of that goal by failing to implement the most important component of their defensive posture: trained people.

Escalation of Commitment

Changing the course we have been on for a long time houses its own bias: *escalation of commitment*. This bias is the pattern of behavior in which humans continue to rationalize their decisions and behavior, even when they cause clearly negative outcomes, rather than alter their course. As we look back on all of the time and money we spent fighting the wrong battle, there will naturally be some resistance to change.

We must also overcome another pesky cognitive bias, conservatism. *Conservatism bias* (as opposed to political or social conservatism) is the tendency for humans to insufficiently revise their beliefs even when they are presented with compelling new evidence. This is the root of the saying (and the bane of my existence) “But we've always done things this way!”

It is going to be a very tough pill to swallow, since humans do not like to admit fault for anything (remember externalization?). Identifying and overcoming our cognitive biases take a tremendous amount of emotional maturity, something technical people (including me) are not the best at, if you believe the stereotypes.

The logical question now is, as an industry are we mentally and emotionally mature enough to push beyond our cerebral programming and alter our destiny? Can we break a decades-old bad habit?

As we look back on all of the time and money we spent fighting the wrong battle, there will naturally be some resistance to change.
Outthinking our Brains, or, the Way Forward

Economist and social philosopher Adam Smith described it this way in his 1776 book, *The Wealth of Nations*: “It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest.” Do we want to survive, thrive, or simply go gently into that goodnight?

We now know that we are dealing with a cerebral vulnerability that can be “patched,” to use technical vernacular. Doing so will require the courage to admit we have been wrong, the strength to alter course, and the resolve to see it through. This is a very tall order, but history has shown if we can do these things, we will be successful and start to take back the ground we have surrendered to the enemy.

Our industry is densely populated with very intelligent, very technical people who want to solve problems through technology. This is not a shortcoming on their part, just how they are naturally wired. They are quantitative thinkers, binary—if there is a technical problem, there must be a technical solution. However, two decades of less than stellar results has proven otherwise.

Bringing the real problem into focus reveals what we have been dealing with all this time: not a shortcoming in technical capability, but the ugly messiness of people.

As a leader and member of highly technical security teams over the past 15 years, I can personally attest to the fact that emotional intelligence and maturity are not highly valued in this field. These teams have included brilliant technical minds who wrote books and computer scripts and programs capable of doing truly amazing things. Their knowledge was vast and impressive—they were true masters of their craft. However, their technical acumen overshadowed their lack of emotional maturity, and rightfully so. They were measured and paid on their ability to solve technical problems.

So, in a sense, the cybersecurity industry has done this to ourselves. We have focused so heavily on technical knowledge and capability that we have created an entire population of workers who are frankly not that great with people. Now, if we do things the right way, we must ask these technical experts to solve a largely human problem.

Do you really anticipate anything other than resistance, futile as it may be?

---

Bringing the real problem into focus reveals what we have been dealing with all this time: not a shortcoming in technical capability, but the ugly messiness of people.
TURNING THE SHIP AROUND

I had a commander in the army who once told me “Don’t come to me with problems unless you have a solution.” So, in line with my military training, I submit two plans for changing the course we find ourselves on. I have separated this plan into two sections, a Battle Plan, which is a higher level, strategic plan; and an Action Plan, which is a more granular tactical plan focusing on how to execute on the Battle Plan.

**THE BATTLE PLAN**

1. **Admit**
   
   Admit there is a problem. This is step one in every recovery program for good reason. You cannot begin to address a problem that you can’t or won’t admit is actually there.

2. **Identify**
   
   Identify which cognitive biases are present in your organization. This will take emotional maturity at all levels—to the best of my knowledge, every person at every company everywhere in the world is a human being. Expect tremendous resistance at this stage of the process. Progress here will essentially involve admitting personal shortcomings at various levels, up to and including the CEO.

   Organizational leadership will face the question, “Which is more important: your ego or the success of your organization?” You can only choose one answer.

3. **Automate**
   
   Science the %^#& outta it! Engineer out as many human decision points as possible. Technical people get nervous about the word “automation” for good reason. In many instances their job relies on a manual process that, if automated, could mean the loss of employment.

   It’s important to clearly state that you are reducing human decision points, not eliminating them, and that the remaining intersection points will require enhanced decision-making capability from those individuals responsible for them. You should follow this up with extensive, realistic scenario-based training to give people those skills.

4. **Learn**
   
   Let other people make bad decisions and be happy to learn from them. Seriously, do that! There are so many breaches that can be analyzed that there really is no reason why our industry should not have volumes of post-incident review documentation to learn from.

   Organizations should implement an after-action review process for all breaches, whether they’re publicly disclosed or not. It’s true that when you are in the middle of trying to fix an urgent problem, the last thing you have time for is being a case study for someone else. Still, if you think beyond the impact to your own organization about what can be learned from your incident, it will help others avoid a similar situation. That can only benefit everyone involved, including you.

   So ask yourself: what can we learn from this breach? How can these lessons improve your organization’s security posture? If you are dealing with an internal incident, how can you use your experience to help others?

5. **Hire**
   
   Hire for success. You should seek to employ the right kind of people, rather than the most geographically convenient ones or those with a certain skillset. You will need people who can follow processes and procedures, can take direction, and are less egocentric and more mission focused.

   Historically, the hiring process for technical jobs has mainly focused on whether or not the applicant already has the technical skills to perform the tasks required for the job. While this may seem logical, we have two decades of evidence to substantiate that it’s a very poor hiring strategy. Curse you, pesky evidence!
## THE ACTION PLAN

1. **Realize there is a problem, and that we are going to do something about it**
   
   While step 1 of the Battle Plan is admitting there is a problem, the first step in the Action Plan is to commit to taking action. Think of the difference between saying “I need to start going to the gym” and showing up at the gym on Monday morning. Count the cost, commit, and act!

2. **Garner or provide top-down support**
   
   Just like a BBS program, a security program cannot be successful without top-down commitment, support, and evangelization. This is absolutely critical; the leadership of your organization must be utterly committed to the security program or it will become an exercise in futility and a colossal waste of money, time, and energy.

3. **Identify cognitive biases and implement a mechanism to overcome them**
   
   This is going to take some serious mental and emotional maturity within the organization as these biases will be present in every member of the staff, from the CEO down. As you seek to implement this phase, I highly recommend retaining the services of a professional executive coach or organizational change consultant. It will not be easy, it will not be pleasant, and it will very likely cause a lot of political and social upheaval within the company.

4. **Understand the return on investment for security**
   
   Spending time, energy and resources on security is not a net loss. When weighed up against the costs of post-breach litigation, the fines that regulatory bodies can levy, and the decrease in revenue from losses of customer confidence and market share, there is tremendous wisdom to investing in security.

5. **Understand that GRC regimes are only part of the solution**
   
   You are kidding yourself if you think you can checkbox your way to a secure environment. If GRC regimes alone could prevent data breaches, payment card breaches would have ceased in 1999 when Visa first released the Cardholder Information Security Program.

   Compliance will never ever equal security ... ever. Now, it can still be a good idea to align your security posture with a compliance régime—or in many cases, a requirement. But you should never expect that compliance alone will make your environment safe from attackers.

6. **Look for wisdom in other areas of industry**
   
   As this white paper has shown, you can learn valuable lessons from other, older businesses. Do not be so precious as to think our industry is unique. The two examples I chose—the spread of communicable diseases and the manufacturing industry—provided a wealth of knowledge and many parallels. Other areas very likely will have similar wisdom to share. I hope others will do as I have done and write about these nuggets of hidden knowledge.

7. **Institute a “train as you fight” security philosophy**
   
   Just like the military is myopically focused on going to war, cybersecurity professionals should focus on preparing for a cyberattack. Doing so will put your organization in a much better position to handle a real incident when it happens. And it will happen. Remember the organizations that are breached and don’t know it yet? Train as if every day is that day.
Ok, so this is great: We have identified the problem, we have a Battle Plan and an Action Plan, so now all we need to do is go and implement it, right?

Well, it’s not quite that easy (it never is).

Here’s the Catch-22—everybody in the cybersecurity industry knows there is a worldwide skills shortage; we have far more openings than we have people to fill them. Organizations are trying to bridge this gap by finding enough bodies that closely align with the skills they’re looking for. They’ve learned to overlook or ignore prospective employees’ lack of non-technical people skills.

Remember, though, that technical ability alone is not enough; if it were, breaches wouldn’t occur in such great numbers and with such frequency. Now organizations will have to take a very short list of people who have the technical skills to fill their cybersecurity vacancies and try to identify the individuals who also possess the mental and emotional maturity to effectively contribute to this next generation of strategic security solutions.

I realize this may not be realistic in the short term; business needs may require immediate action. However, if organizations become more aware of the need to identify and hire candidates who possess these non-technical skills, they can start the process of hiring for long-term success. In other words, they need to start looking for Mr. or Ms. Right rather than Mr. or Ms. Rightnow.

---

### THE ACTION PLAN

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Create a culture of security-minded employees</td>
</tr>
<tr>
<td></td>
<td>Security is everyone’s responsibility. This is not a clever cliché, but a reflection of the current threat landscape. Client-side attacks such as social engineering, spear phishing, and browser-based exploits are among the most common and most effective attack vectors. Every employee, contractor, third party vendor, intern, or volunteer should understand the basics of identifying, deflecting, and reporting these attacks.</td>
</tr>
<tr>
<td>9.</td>
<td>Realize security is a journey, not a destination</td>
</tr>
<tr>
<td></td>
<td>Becoming secure is not something you do, it’s something you are. You will not reach the end of a strategic initiative, declare victory, and celebrate your hard work. There is no beginning or end to this journey. It’s sort of like getting fit; you don’t go to the gym for a year, announce one day that you’ve achieved fitness, and never run another mile or lift another weight. This is a long-term commitment that will change and evolve or time. Like physical exercise, it will get easier as time goes by, but you will never be done.</td>
</tr>
<tr>
<td>10.</td>
<td>The marriage of human intelligence and technology is the key to victory</td>
</tr>
<tr>
<td></td>
<td>As with the industrial manufacturing industry, the goal is to engineer out as many human intersection points as possible to reduce the opportunity for errors. In those areas where automation cannot replace human interaction, the people in those positions should be extensively trained and equipped with software that will act as an intelligence multiplier. This marriage of technology and human intelligence represents the path forward and what I believe to be the crucial element in reclaiming surrendered ground.</td>
</tr>
</tbody>
</table>
**THE SUMMATION OF THE PSYCHE**

“Our brains are supercomputers, but like all computer systems we have vulnerabilities that need to be identified and remediated. Throughout this white paper, I have clearly shown that data breaches are caused by human action or inaction.

The cybersecurity industry has historically thought of data breaches as a technology problem, but all the evidence indicates that they are really a human problem. Based on the lessons learned from WHO and Heinrich, preventing breaches requires changing behavior and reducing the number of opportunities for people to make mistakes.

We now find ourselves at a crossroads where decision makers need to choose the “same ole same ole,” or innovation.

Do cybersecurity practitioners have the mental and emotional maturity to overcome the cognitive biases identified in this paper, admit we have been fighting the wrong battle for two decades, and learn from those mistakes?

The cybersecurity industry is in a very interesting place. Our collective experience does not easily lend itself to the situation we find ourselves in. If we are not careful and hyper-cognizant of our decisions, we could very easily be led astray.

L.M. Montgomery, author of the Anne of Green Gables novels, eloquently said, “We all make mistakes, dear, so just put it behind you. We should regret our mistakes and learn from them, but never carry them forward into the future with us.”

Our brains are amazingly fast and accurate at recognizing patterns. We collect all sorts of data and we create mental shortcuts to make sense of the world. To illustrate this point, did you know that none of us actually reads the individual letters in words beyond elementary school; rather, we recognize words or word patterns and quickly draw meaning from what we see. This is why we can decipher writing that is jumbled, backwards, or drastically misspelled (see Figure 5).

Whether or not we act on those patterns depends on our emotional maturity, specifically on something called emotional tags. These tags provide the framework for us to develop a sense that what we are seeing is a good thing or a bad thing. Put simply, we don’t make fact-based decisions; we make emotional choices based on pattern recognition.

Our focus, as we move forward, should be on the patterns and tags associated with the marriage of people and technology. By reducing the number of human decision points through technology, we can dramatically reduce the opportunity for mistakes and failure. Then we can focus our pattern recognition efforts on realistic attack scenarios, provide military style training and education, and conduct ongoing threat simulations. Doing so will enable the individuals at the remaining intersection points to be exponentially more prepared and subsequently more successful than they have ever been.

One final thought: The status quo bias can be summed up with the saying “If it ain’t broke, don’t fix it.” This bias takes the current reference point and views any sort of deviation as a perceived loss. Do we have what it takes to outsmart our own brains and stop ourselves from repeating the mistakes of the past? Hopefully we can set ourselves up for the next 20 years and we can get serious about security, start addressing the real human vulnerability, and start reclaiming surrendered ground.

---

*“Excellence is never an accident. It is always the result of high intention, sincere effort, and intelligent execution; it represents the wise choice of many alternatives—choice, not chance, determines your destiny.”* 

*Will Durant, The Story of Philosophy*
References and Further Reading


George Dvorsky, “The 12 cognitive biases that prevent you from being rational”, *io9*, September 2013


FireEye Threat Intelligence Reports


Frank Pennachio, “Going beyond the Limits: A 10-Year Study Conducted by DuPont Found That 96 Percent of Accidents at the Company Were the Result of Unsafe Actions by Employees Going beyond Their Limits, Rather Than Unsafe Conditions”, *Occupational Hazards*, September 2008


---


ii Ibid.


ix Frank Pennachio, “Going beyond the Limits: A 10-Year Study Conducted by DuPont Found That 96 Percent of Accidents at the Company Were the Result of Unsafe Actions by Employees Going beyond Their Limits, Rather Than Unsafe Conditions”, *Occupational Hazards*, September 2008
Christopher E. Pogue

Chris Pogue is the Senior Vice President of Nuix’s Cyber Threat Analysis security consulting team, and a member of the US Secret Service Electronic Crimes Task Force.

Pogue is responsible for the company’s security services organization; he oversees critical investigations and contracts, and key markets throughout the United States. His team focuses on incident response, breach preparedness, penetration testing and malware reverse engineering.

Over his career, Pogue has led multiple professional security services organizations and corporate security initiatives to investigate thousands of security breaches worldwide. His extensive experience is drawn from careers as a cybercrimes investigator, ethical hacker, military officer, and law enforcement and military instructor.

In 2010, Pogue was named a SANS Thought Leader.

Pogue served in the United States Army as a Signal Corps Warrant Officer and Field Artillery Sergeant. He distinguished himself as an Honor Graduate from a variety of Army Academies and Schools and received multiple awards and commendations for excellence.

To find out more about Nuix’s approach to addressing cybersecurity threats visit:

nuix.com/security-intelligence

ABOUT NUIX

Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.
Preparing for the Inevitable Cyber Intrusion: Practical Realities for Environmental, Energy, and Resources Lawyers

By
Claudia Rast

Abstract: Technology and its workplace applications have allowed entities and their inside and outside counsel to become increasingly more efficient and organized. This efficiency comes with a distinct downside, however, as ubiquitous connectivity cedes to pervasive vulnerability. “Big Data” is now “Deep Learning” and the “Internet of Things”. Having massive amounts of digital information at one’s fingertips is both a marvel and a recipe for disaster. The reality of the risks is becoming part of the daily news cycle, as cyber threats increase in scope and damage. At particular risk in the U.S. are those entities comprising our critical infrastructure. The Department of Homeland Security identifies sixteen “Critical Infrastructure” sectors in the country: “Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” DHS website, http://www.dhs.gov/what-critical-infrastructure. As trusted counsel, lawyers can and should offer informed advice both prior to and when the cyber intrusion occurs.

I. Companies—and their Legal Counsel—are Vulnerable to Cyber Attacks, Particularly those in Critical Infrastructure Areas

Increasingly, companies are being forced to deploy advanced IT measures to repel the pervasive threats posed by cyber intrusions. Such intrusions can be directed at any number of targets: some as seemingly innocuous as the names and email addresses of a company’s staff (for use in phishing or social engineering exploits) to more traditional targets. These threats present themselves in two major categories: (1) the general loss of confidential information, ranging from trade secrets and other intellectual property to pre-public deal information and (2) the loss of operational integrity and availability caused by malicious interference, resulting in the malfunctioning of systems or the inability to access the systems, or both. Former National Security Administration Director Keith Alexander estimated the annual economic losses stemming from cybersecurity breaches at $250 billion. That estimate is just based upon what we think we know.

As lawyers and counsel to companies in sectors such as manufacturing, energy (oil, gas, electric, nuclear, wind, solar), natural resources, water treatment, etc., we find ourselves at the heart of representing many of the “critical infrastructure” companies in the country. The Department of Homeland Security defines critical infrastructure as “the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof,” and such critical infrastructure companies are possible high-value targets precisely because the companies’ operations are so essential. Examples of such companies include petroleum refineries, water treatment plants, nuclear
power plants, natural gas pipelines, chemical manufacturers, pharmaceutical labs, hydroelectric plants, and others. A debilitating malfunction, or the inability to access the industrial control systems to correct a malfunction, at one of these facilities could lead to devastating economic, health, and environmental losses.

As legal counsel to such companies, we have a special responsibility to understand the potential security threats and to take proactive steps to guard against vulnerabilities. Those proactive steps should include understanding and guarding against not only the threat potentials that may be unique to our clients, but also those threats that target our own practices as lawyers.

II. The Lawyer’s Ethical Obligations for “Technological Competence”

Does the average lawyer have the technological proficiency to understand the ways and means of today’s cyber threat agents? Sadly, many do not. And do we realize that it is our ethical obligation to our clients to have this proficiency? This is not to suggest that we must become information technology (IT) experts, but it does mean that we must be cautious and risk aware about using unprotected public WiFi on our mobile business devices, that we don’t upload client documents to public cloud apps without ensuring proper encryption both in transit and at rest, and that we know enough about our firm or company’s IT infrastructure to keep high-value, high-risk information and documents in carefully segmented and secure locations.

The best way to understand the requirement that we have some basic level of technological competency about cybersecurity is to examine the recent changes to the rules governing our ethical obligations, specifically Rules 1.1 (competency) and 1.6 (confidentiality) of the ABA Model Rules of Professional Conduct, which were updated in August 2012 by vote of the ABA’s House of Delegates. In the context of cybersecurity, one focus of the 2012 amendments to the Model Rules was on protecting client information from inadvertent disclosure by ensuring competent representation. But what does “competent representation” mean in your everyday practice?

The critical change to Rule 1.1 arises from the modification to Comment [8], noted in bold below:

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (emphasis added).

To illustrate the point, let’s use an example of a new client which is a company that has developed a game-changing technology that makes the cost of producing electricity from solar energy much more competitive. The client seeks help to sort through applicable federal and
state environmental and energy regulations. Would you think twice about accepting that representation, assuming, of course, that you were versed in this energy area? If this client asked you to describe the IT security protections that your firm had in place to protect the company’s sensitive trade-secret and patent information, could you? Would you have a colleague that could help? Would your IT manager’s answer satisfy the client?

These questions may sound obscure, far-fetched, or paranoid, but they are becoming increasingly relevant and critical to all lawyers and corporate counsel in particular. Companies that have experienced security breaches at the hands of their unknowing, vulnerable suppliers—their lawyers—are beginning to demand confirmation of security compliance at the outset of the representation. Cybersecurity questionnaires are gaining traction among companies when they seek new legal representation or have security concerns about a particular matter, and the lawyer who hasn’t seen or responded to such a questionnaire should be prepared to do so in the near future.

Separately, Model Rule 1.6 (c) states in part that: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” The operative phrases here are “reasonable efforts” and “information relating to the representation of a client.” Where a lawyer once could rely on locked doors, mechanical shredding of sensitive paper documents, and discreet and professional colleagues and staff, the challenges posed in a digital world of increasingly mobile devices require constant diligence and continued education. Should you know that public WiFi is inherently insecure and that conducting client business in such an environment may not be a “reasonable” effort to prevent unauthorized disclosure?

III. Legislative Update: CISA

On December 18, 2015, President Obama signed into law the Cybersecurity Information Sharing Act (CISA), a controversial measure designed to encourage businesses and government agencies to “improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats.” The controversy stems from the concerns privacy and security advocates have when companies submit customer records to the government as part of the information sharing aspect of the legislation. Privacy advocates are concerned about what the government will do with the customer records that companies will submit to it, given the government’s vulnerability to cyber attacks, noting the hack into the Office of Personnel Management in June 2015, resulting in the disclosure of personal data on 21.5 million individuals. Security advocates point out that the federal government already has such an information sharing network in place—in 2003, the Department of Homeland Security established United States Computer Emergency Readiness Team (“US-CERT”) to collect, analyze, disseminate, and respond to cybersecurity information shared among government agencies, the private sector, and researchers.
The concept of information sharing is a valid one, however. Malware, when installed, will leave “indicators of compromise” ("IOC") that once identified by security professionals can be shared within the cybersecurity community (government, private security and researchers). While CISA would assist in the information sharing process by the collection of cyber threat data, CISA does not clearly define who would manage the collected data or how the collected data would be used or disseminated. Indeed, most of CISA is devoted to how the collected data would be shared among government agencies.

IV. Recommendations for the Lawyer

What to do in the face of these risks? A great resource is The ABA Cybersecurity Handbook published in July 2013 and available both in paperback and eBook versions. This handbook is continually updated on the Cybersecurity Task Force’s website and its “resources” webpage at http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html. Former ABA President Laurel Bellows created this task force in 2012, and the work of this task force led the ABA in August 2013 to formally adopt a Resolution condemning “unauthorized, illegal governmental, organizational and individual intrusions into the computer networks utilized by lawyers and law firm.”

A data security plan begins with thorough organization. The following best practices seek to minimize potential data breaches and other security risks.

✓ **Identify, Inventory and Segregate Sensitive Data.** These documents should be readily identifiable in the company’s Document Retention & Destruction Policy.

✓ **Maintain a Current Network Diagram of IT Systems.** This is one of the first documents that you review in the event of a breach. It is best to have it handy and not to have to create it under time pressure.

✓ **Train In-House IT Staff.** It is critical to have knowledgeable people that are capable of conducting a thorough data and IT inventory and security audit. Have forensic specialists vetted and ready to assist IT staff when the data breach occurs.

✓ **Create Data Security Policies to:**
  - Govern the development, acquisition, implementation and maintenance of IT systems
  - Ensure that backup and disaster recovery planning processes are consistent with privacy policies and procedures and document retention and destruction policies
  - Classify and protect sensitive data
  - Assess planned changes to systems for their potential effect on privacy and test changes prior to implementation
• Document sign-off by IT Manager and Business Unit Manager before implementation

✓ **Acquire Cyber-Risk Insurance Coverage.** Distinguish if first-party insurance, third-party or both provide the necessary coverages since coverages may vary among carriers. In addition, assess coverage for:
  - Data Breach: Failure to protect an individual’s privacy – 1st Party Costs, Notification, Forensics, Legal Assistance, Credit Monitoring, PR Firms
  - Data Breach: Failure to protect an individual’s privacy – 3rd Party Costs, Defense Costs & Settlements
  - Network Security (loss or damage to a network & data, which may include lost income)
  - Media Liability: Web content (Libel, Defamation)
  - Fines & Penalties (HIPAA, PCI)
  - eVandalism & Extortion
  - Property loss from Cyber Perils (Internet of Things)

✓ **Understand what Defines a Security Breach.** Generally, any “unauthorized acquisition” of data “that compromises” the security, confidentiality, or integrity of personal information maintained by the business will be considered an actionable data breach. Under HIPAA/HITECH, data breach means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted and compromises the security or privacy of the protected health information.

✓ **Learn the Definitions of Personally Identifiable Information, Protected Health Information, Individually Identifiable Health Information, etc.** For example, Personally Identifiable Information can be a user name or email address—it does not have to be the person’s legal name or street address. State laws may define Personally Identifiable Information differently, one state to the next. Forty-seven states and the District of Columbia have data breach laws.

✓ **Notify Owners of Compromised Data.**

✓ **Monitor Employee Interactions.** Monitor employee interactions with valuable data in order to identify patterns of use and analyze ignorance or abuse of existing policies. In doing so, best practices can be integrated among employees over time. This leads to an increasing security-oriented behavior that ultimately inures the benefit of the company’s security.

✓ **Encrypt Sensitive Data.** Most state laws do not require breach notification to data owners if the compromised data is encrypted. Useful tips regarding encryption are:
• Using NIST-approved Advanced Encryption Standard (AES) for bulk data encryption.
• Encryption keys should be used in safe places where they cannot be easily stolen.
• Key-access keys must be used in hardware-protected environments (e.g., dedicated servers, Hierarchical Storage Management (HSM) or self-encrypting hard disk drivers).
• When using all credit card transactions the best solution is public key cryptography such as NIST-approved RSA or elliptic curve.
• All encryption keys (cryptographic materials) must be monitored

✓ Create Robust Passwords.
• Monitor access controls among staff
• Create attack-resistance passwords
• Implement compartmentalization and segmentation methods to avoid expansion of the breach

✓ Protect IT System from External Risks. It is critical to fully protect (i) networks and networked resources from fraudulent devices and software (e.g., tablets, smart phones, etc.), (ii) IT systems from inappropriate access (take into account the differences between authentication – authorization – administration), and (iii) data from unauthorized disclosure, unwarranted alteration, or removal.

In summary, control your data:
• Develop a document retention and destruction policy: if you don’t need it, and are not legally required to retain it, delete it
• Enable Network Security Monitoring & Review of Log Files (Lesson Learned from Target)
• Restrict Remote Access
• Segregate & Secure High Risk Information, Operations & Workers
• Encrypt Sensitive Data
• Implement a Robust Password Policy & Enforce It
• Demand Compliance from Contractors & Suppliers (Another Lesson from Target)
• Implement Company-wide Training (Ongoing)
• Name staff to serve as the “first responders”—the Rapid Response Team—when a data breach occurs
• Conduct Table-Top Drills
• Acquire Cyber Liability Insurance
• Have Experts at the Ready When an Attack Occurs

And for the IT Department:
• Collect, Analyze & Share Tactical Threat Intelligence, Especially Indicators of Compromise
• Focus on Better & Faster Detection
• Establish Metrics: “Number of Compromised Systems” & “Mean Time To Detection” in Networks; Use Metrics to Drive Security
• Evaluate Threat Landscape to Prioritize Treatment Strategy (It’s not a “One-Size Fits All” World)
• Track Workforce: Who’s Who, What they Do & When they Go

A last recommendation for you and your client or company is the National Institute of Standards and Technology (NIST) Cybersecurity Framework released in its final form in February 2014. The Framework’s focus is on critical infrastructure companies and provides a detailed process to assess cyber risks. In the absence of anything else, the Framework has become a standard tool in the cybersecurity risk assessment process.
Thank you for attending Our Program:

“Data Breaches and Cyber Security – Are You Ready?”

Presented by the ABA YLD Litigation Committee

Co-Sponsored by the ABA YLD International Law Committee and the ABA YLD Science and Technology Law Committee

SPECIAL THANK YOU to Abigail Bridgman, Lisa Mays, Jon McGill, Ashley Thomas, and Cabell Clay for assisting in the organization of this wonderful program and to our speakers for donating your time and expertise to the panel

Lauren A. Marsicano
Liebler, Gonzalez & Portuondo

Co-Chair
ABA YLD Litigation Committee