Arnold & Porter

Cybersecurity Risks and Considerations for 2018

June 5, 2018

Arnold & Porter

Cybersecurity Risks and Considerations for 2018

June 5, 2018
5:30 p.m. – 8:00 p.m. ET

Table of Contents

Agenda ..... Tab 1

Presentation Slides ..... Tab 2

Practice Overviews ..... Tab 3

Cybersecurity, Data Breach Rapid Response Team

Supporting Materials ..... Tab 4

- NYDFS Issues New Cybersecurity Reporting Guidance
- SEC Issues Cybersecurity Guidance
- NYDFS Issues New Cybersecurity FAQs
- Nuts and Bolts of Data Breaches and Identity Fraud
- New York Department of Financial Services Issues Additional Cybersecurity FAQs
- New York Department of Financial Services Issues Final Cybersecurity Regulations
- 2018 Cybersecurity Predictions

Speaker Biographies ..... Tab 5

Marcus A. Asner, Michael A. Mancusi, Nancy L. Perkins, Edward M. Stroz, Kevin M. Toomey

Arnold & Porter

Tab 1: Agenda

Arnold & Porter

Cybersecurity Risks and Considerations for 2018

June 5, 2018
5:30 p.m. – 8:00 p.m. ET

Agenda

5:30 – 5:35 p.m. ET	Welcome and Introduction
5:35 – 6:50 p.m. ET	Presentation
	Speakers:
	Marcus A. Asner, *Partner, Arnold & Porter, Privacy and Data Security, Anti-Corruption and White Collar; former Chief of the SDNY Major Crimes and Computer Hacking/Intellectual Property (n/k/a Complex Frauds) unit*
	Michael A. Mancusi, *Partner, Arnold & Porter; former Enforcement Attorney at the Office of the Comptroller of the Currency*
	Nancy L. Perkins, *Counsel, Arnold & Porter, Financial Services*
	Edward M. Stroz, *Founder and Co-President, Stroz Friedberg, an Aon company and global leader in investigations, intelligence and risk management*
	Kevin M. Toomey, *Associate, Arnold & Porter, Financial Services*
6:50 – 7:00 p.m. ET	Question-and-Answer Session
7:00 – 8:00 p.m. ET	Cocktails

1.5 NY and CA CLE credit and 1.25 IL CLE credit (all pending)
Other jurisdictions may also be available

Arnold & Porter

Tab 2: Presentation Slides

Arnold & Porter

Cybersecurity Risks and Considerations for 2018

Marcus A. Asner, Arnold & Porter, Privacy and Data Security, Anti-Corruption and White Collar
Michael A. Mancusi, Arnold & Porter, Financial Services
Nancy L. Perkins, Arnold & Porter, Financial Services
Edward M. Stroz, Founder and Co-President, Stroz Friedberg
Kevin M. Toomey, Arnold & Porter, Financial Services

June 5, 2018

Overview

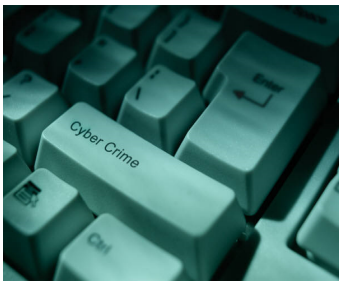
- Preparing for and responding to a data security incident, addressing both technical and legal issues
- Navigating the regulatory and enforcement framework, including complying with notification requirements
- Understanding the SEC's "Statement and Guidance on Public Company Cybersecurity Disclosures"—Important considerations for vendor contracts and oversight
- Complying with NY Department of Financial Services Part 500, including preparing for examinations and enforcement risk
- Recognizing the potential applicability of other privacy and security regimes, including the EU General Data Protection Regulation (GDPR)

"There are only two types of companies: those that have been hacked and those that will be."

— Former FBI Director Robert Mueller

Cyber Threats

- Hacking
  - Mischief and data destruction
- Botnets
- Dedicated Denial of Service (DDOS) attacks
- Ransomware
- Corporate espionage
- Foreign economic espionage/ National security



Preparation

- Prevention
  - State-of-the-art firewalls; password protocols etc.
- Limiting the damage
  - Risk assessment
  - Inventory of data
  - Segmenting data
  - Control of insiders
- Vendor management protocols
- Incident response plan
  - Law firms; vendors; involving law enforcement; notifying victims, government authorities, and the press
- Training/fire drills/tabletop exercises
- Insurance coverage

Setting the Stage

- Anonymous phone call claiming:
  - Insider has committed data breach
  - Data being offered for sale on Russian carding site
  - Account numbers and passwords allegedly stolen
- Threatens to go public
- What's next?

Response

- Investigating the Attack (forensics, interviews, etc.)
- Preserving Evidence
- Coordinating with Law Enforcement and Regulators
- Victim Notification
- Government Agency Notification
- Notifying and Handling the Press
- Examinations
- Civil Litigation and Regulatory Enforcement

Regulatory Framework

SEC Cybersecurity Guidance

- SEC published interpretive guidance on February 21, 2018
- Designed to assist public companies in preparing disclosures about cybersecurity risks and incidents
- Reinforces and expands prior guidance issued by the SEC's Division of Corporation Finance in October of 2011
- Applies customary material risk disclosure concepts to cybersecurity risks
- Highlights:
  - Importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents
  - Application of insider trading prohibitions in the cybersecurity context
  - Need for full disclosures of material nonpublic information about cybersecurity risks or incidents

NY Department of Financial Services' Cybersecurity Regulation (23 NYCRR Part 500)

- Part 500 became effective on March 1, 2017 and has garnered widespread attention from banks, insurance companies and other financial services firms.
- New York State-chartered or licensed banks, insurance companies, licensed lenders, check cashers, money transmitters, and their holding companies, and other firms that are licensed by, operating under approval orders of, or otherwise subject to regulation by the DFS are subject to Part 500.
- Covered Entities were required to submit initial certifications of compliance by February 15, 2018.
- Transitional periods require Covered Entities to comply with numerous requirements relating to cybersecurity controls.
  - **September 3, 2018** - Covered Entities are required to be in compliance with the requirements relating to:
    - audit trails;
    - application security;
    - data retention limitations;
    - monitoring policies, procedures, and controls; and
    - encryption of nonpublic information.
  - **March 1, 2019** - Covered Entities are required to be in compliance with the requirement to implement a third-party service provider security policy.

EU GDPR: Key Elements

- EU GDPR regulates the "processing" of "personal data" concerning individuals within the EU
- Enforcement began on May 25, 2018.
- Intended to strengthen and unify data protection rules across the EU
- Aims to provide individuals with significantly more control in respect of processing of their "personal data" (and "special categories of data")
- Potential high maximum fines for non-compliance, up to:
  - greater of €20m or 4% global group turnover; or
  - greater of €10m or 2% global group turnover (for less serious matters)
- New data breach requirements: self-reporting within 72 hours

EU GDPR: Who is Regulated?

- Anyone with an "establishment" in the EU that processes personal data
  - does not matter if the processing takes place in the EU
  - does not matter if the data are of persons in the EU
  - *establishment*: "effective and real exercise of activity through stable arrangements"
- Anyone not established in the EU but who:
  - Processes personal data of persons who are in the EU, ***and***
  - The processing relates to:
    - offering goods or services to such persons, or
    - monitoring the behavior in the EU of such persons

Contacts

Marcus A. Asner
Arnold & Porter

Privacy and Data Security,
Anti-Corruption and White Collar

Michael A. Mancusi
Arnold & Porter

Financial Services

Nancy L. Perkins
Arnold & Porter

Financial Services

Edward M. Stroz
Founder and Co-President
Stroz Friedberg

Kevin M. Toomey
Arnold & Porter

Financial Services

Arnold & Porter

Tab 3: Practice Overviews

CYBERSECURITY

arnoldporter.com

Arnold & Porter

Our government contracts lawyers work closely with colleagues across the firm to meet the specialized cybersecurity needs of defense, aerospace, Internet, software, hardware, and other companies doing business with the Federal Government.

Arnold & Porter fields an across-the-board Cybersecurity practice.

Our team litigates data security breach cases; counsels on a full range of compliance, regulatory, and liability issues; represents government contractors in procurement-related cybersecurity matters; and advises clients on strategy and policy matters involving cyber capabilities, defensive and offensive cyber operations, and vulnerability management. Government contractors face particular cybersecurity challenges because, while they are subject to many of the same regulatory requirements and cyber challenges as other companies, they also face US government procurement mandates related to the protection of US government information and networks, and must meet requirements arising from the security clearances that the contractors hold. Our government contracts lawyers work closely with colleagues across the firm to meet the specialized cybersecurity needs of defense, aerospace, Internet, software, hardware, and other companies doing business with the Federal Government.

We regularly advise clients regarding privacy and data security regimes that apply to the health care, financial services, and other consumer-facing sectors. We defend data security breach cases for major corporations in the Internet, software, consumer, and government services industries.

The national security, homeland security, and law enforcement government experience of our attorneys provides an additional dimension of insight and expertise. Our lawyers have served in senior US government legal and policy positions, and that experience helps them advise clients about working effectively with the government and anticipating and planning for government action. The United States and many other advanced nation-states have elevated cybersecurity and cyber operations to the highest levels of their national security, law enforcement, diplomatic, technological, and economic priorities and planning. We help clients relate their immediate cybersecurity challenges to governments' cyber strategies, plans, and procurement activities.

- Advised defense contractors and hardware manufacturers on compliance with US government cybersecurity and supply chain security requirements, including the Department of Defense (DoD) Rule on Adequate Security and Cyber Incident Reporting for unclassified controlled technical information (UCTI).
- Counseled companies involved in national security and technology regarding legal restrictions on cyber capabilities, active

defense, and other steps they can take to protect their networks and those of their clients under the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act (ECPA), and the Stored Communications Act (SCA).

- Represented major US retailers and aerospace companies on data breaches, including customer notice requirements and government inquiries regarding such breaches.
- Developed procedures for managing vulnerability and enterprise risk related to cybersecurity issues for both government contractors and commercial technology companies.
- Advised government contractors, other companies, and individuals on issues relating to classified information, including personnel and facilities clearances, reporting of adverse information, and compliance with security requirements.
- Counseled DoD contractors on US government requirements relating to information assurance capabilities and personnel security aspects of information technology products and services used by DoD and its contractors.
- Represented a software and services company on congressional, regulatory, and government procurement issues related to responsibility and liability for the security and reliability of computer network systems and software.
- Represented a national bank in the development and US government review of privacy and security protections for outsourcing arrangements for a foreign software company to develop and maintain software involved in the delivery of services to US government customers.
- Advised clients on legislative and public policy developments related to cybersecurity, information sharing, computer crime, and electronic surveillance.
- Drafted privacy policies governing companies' collection and use of customer data.

Recognition

- *Chambers Global*: Privacy & Data Security (USA) (2010-2018)
- *Chambers USA*: Privacy & Data Security (2008-2018)
- *The Legal 500 US*: Cyber Law (2017)
- *Washingtonian* Magazine: "Top Lawyers" – Cybersecurity (2015, 2017)

Clients say, "They have been superb. They know the law, they're very practical, they're extremely knowledgeable and they're very responsive and available," and "They certainly have a lot of expertise in the national security sector and they have an excellent cybersecurity practice."

— Chambers USA

Key Contacts

Charles A. Blanchard

Partner, Washington, DC
charles.blanchard@arnoldporter.com

+1 202.942.5805

Adam Golodner

Senior Counsel, Washington, DC
adam.golodner@arnoldporter.com

+1 202.942.6860

Kenneth L. Chernof

Partner, Washington, DC
kenneth.chernof@arnoldporter.com

+1 202.942.5940

Nicholas L. Townsend

Counsel, Washington, DC
nicholas.townsend@arnoldporter.com

+1 202.942.5249

Ronald D. Lee

Partner, Washington, DC
ronald.lee@arnoldporter.com

+1 202.942.5380

Nancy L. Perkins

Counsel, Washington, DC
nancy.perkins@arnoldporter.com

+1 202.942.5065

DATA BREACH RAPID RESPONSE TEAM

arnoldporter.com

Arnold & Porter

Arnold & Porter's Privacy and Data Security practice assists businesses in a wide range of industries—from e-commerce start-ups to global FORTUNE 100 companies—in the increasingly challenging task of protecting data consistent with applicable law.

Information capital is the most valuable resource in today's economy.

Worldwide data theft has surpassed physical property theft in frequency and loss of assets, making data security a vital component of the basic operations of every business. Being prepared for a data breach can prove crucial to a company's operations, its reputation, and even its survival. Arnold & Porter's Data Breach Rapid Response Team helps clients develop a data breach response plan and stands ready to help victims of data breaches immediately fortify defenses and minimize both short-term and long-term losses.

Multidisciplinary Practice

Our Data Breach team is distinguished as a proven, comprehensive service group bringing together the full force of our integrated **white collar**, **privacy**, **cyber-security**, **healthcare**, **financial services**, **corporate**, **intellectual property**, **employment**, and **litigation experience** to help our corporate clients develop properly tailored response plans, and to protect victims of a breach from the first instance of a breach, through each stage of crisis management.

Our Approach

Arnold & Porter provides practical and thoughtful legal and strategic counseling to clients by employing a multipronged approach. We understand that advising and representing companies in sensitive data breach matters involves integrating substantive legal advice; detailed knowledge of companies' objectives, business units, and factual situations; and familiarity with the government's priorities, processes, and approaches. Our team incorporates these principles in a step-by-step practical project plan tailored to each matter and client with an eye towards the full life cycle of the response including:

- Breach Response Procedure & Policy
- Notification
- Partnering with Law Enforcement
- Communications Management
- Anticipating Protracted Litigation
- Witness Services

Team members have worked closely with federal and state law enforcement authorities on numerous data breach crises.

We have deep knowledge of the data protection and notification requirements of the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act, Gramm-Leach-Bliley Act, NYDFS cybersecurity regulation, HIPAA, HITECH, and the EU data protection laws. We are supported by colleagues with extensive backgrounds in high-ranking government positions. Together, we are fully versed in the broad range of state, federal, and international privacy laws, and understand how to efficiently navigate the complexities of responding to a data breach.

Deep Experience

Our team of high-level government and national security professionals provides a breadth of experience that rivals any other firm. Former positions include:

- Chief of Major Crimes and Computer Hacking/ Intellectual Property Unit at the US Attorney's Office in the Southern District of New York
- General Counsel for the Central Intelligence Agency
- Chief of Staff to the Associate Attorney General
- Associate Deputy Attorney General and Director of the Executive Office for National Security at the US Department of Justice
- General Counsel for the National Security Agency
- General Counsel of the US Army and US Air Force
- Counselor to the Attorney General for National Security
- Deputy Associate Attorney General
- Legal Adviser at the Department of State
- Chief Counsel for the National Telecommunications and Information Administration

Highlights of Representations Include:

- **UK-based financial institution** in connection with the theft of account information relating to several million customer accounts.
- **Major bank** on legal, technological, and policy measures to prepare for, respond to, and recover from breaches of data security caused by loss, theft or other compromise of digital information.
- **The Bank of Ethiopia Citibank Breach** Led the investigation into a recent account take over which led to the theft of approximately $27 million from a Citibank account belonging to the National Bank of Ethiopia.
- Assisted **insurance company** in meeting its privacy and security obligations under the Gramm-Leach-Bliley Act.
- **Multi-billion dollar bank holding company** in comprehensive internal investigation of the organization's information technology systems and controls in response to an internal whistleblower complaint of insufficient systems and controls.
- **National bank** in development and government review of privacy and security protections for a foreign software company to develop and maintain software involved in the delivery of services to US government customers.
- **Large broker-dealer** on compliance with the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA).
- **Large state chartered bank** in meeting its privacy and security obligations under the Gramm-Leach-Bliley Act.
- Counsel **numerous financial institutions** on compliance with the New York Department of Financial Services' Part 500 cybersecurity rules.
- **Financial institutions** in the development and implementation of incident response plans.
- Advised **Internet retailer** on compliance with the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA), including the new FACTA rules on data sharing and identity theft prevention.
- **Major investment bank** in support of the client's consumer finance investment group, advising the client regarding regulatory and consumer-protection issues for a potential transaction.
- **Financial technology company** on a variety of banking regulatory, BSA/AML, and data privacy/cybersecurity issues.
- **International financial services firm** on information security, computer crime, electronic surveillance, and workplace privacy issues.
- Advising **insurance company** on compliance with the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA), including the new FACTA rules on data sharing and identity theft prevention.

Recognition

- *Chambers Global*: Privacy & Data Security (USA) (2010-2018)
- *Chambers USA* Privacy & Data Security (2008-2018)
- *The Legal 500 US* Technology: Data Protection and Privacy (2014-2017) and Cyber Law (2017)
- *Cybersecurity Docket* Ronald D. Lee and Adam Golodner named to the *"Incident Response 30"* (2016)
- *National Law Journal* Ronald D. Lee and Adam Golodner named *"Cybersecurity and Data Privacy Trailblazer"* (2015)
- *Washingtonian* Magazine *"Top Lawyers"* – Cybersecurity (2015, 2017)

Key Contacts

Marcus A. Asner
Partner, New York
marcus.asner@arnoldporter.com
+1 212.836.7222

Adam Golodner
Senior Counsel, Washington, DC
adam.golodner@arnoldporter.com
+1 202.942.6860

Charles A. Blanchard
Partner, Washington, DC
charles.blanchard@arnoldporter.com
+1 202.942.5805

Nancy L. Perkins
Counsel, Washington, DC
nancy.perkins@arnoldporter.com
+1 202.942.5065

Ronald D. Lee
Partner, Washington, DC
ronald.lee@arnoldporter.com
+1 202.942.5380

Daniel Jacobson
Associate, Washington, DC
daniel.jacobson@arnoldporter.com
+1 202.942.5602

Michael A. Mancusi
Partner, Washington, DC
michael.mancusi@arnoldporter.com
+1 202.942.5302

Kevin M. Toomey
Associate, Washington, DC
kevin.toomey@arnoldporter.com
+1 202.942.5874

Arnold & Porter

Tab 4: Supporting Materials

Arnold & Porter

March 9, 2018

NYDFS Issues New Cybersecurity Reporting Guidance

Advisory

By David F. Freeman, Jr., Marcus A. Asner, Michael A. Mancusi, Brian C. McCormally, Adam Golodner, Nancy L. Perkins, Anthony Raglani, Kevin M. Toomey

On March 2, 2018, the New York Department of Financial Services (DFS) notified certain Covered Entities, as well as certain of their employees, agents and representatives who are also Covered Entities, of their failure to file a certification of compliance with the DFS's cybersecurity regulations codified at 23 N.Y.C.R.R. Part 500 (Part 500). Shortly thereafter, the DFS issued new guidance regarding the reporting obligations of Covered Entities under Part 500. Banks and other financial services firms and their subsidiaries and affiliates, particularly those that have been notified by the DFS as described above, should review the guidance closely to ensure that applicable Part 500 filing and compliance obligations are being fulfilled in a timely and satisfactory manner.

As discussed in prior Advisories (here, here, here and here), Part 500 requires Covered Entities to adopt and maintain a cybersecurity program and corresponding cybersecurity policies and procedures. Although in some ways Part 500 is similar to federal requirements and guidance on cybersecurity for banks and securities firms, it differs in certain material respects and imposes substantial reporting obligations upon Covered Entities. Several provisions of Part 500 became effective on March 1, 2017, and by February 15, 2018, Covered Entities were required to submit to the DFS their initial certifications of compliance with such provisions. Additional requirements of Part 500 related to risk assessments, penetration testing and vulnerability assessments, multi-factor authentication and risk-based cybersecurity awareness training became effective on March 1, 2018, while other provisions of Part 500, including the encryption of nonpublic information and third-party service provider compliance, will be phased into effect through March 1, 2019.

Among other things, the new guidance provides that Covered Entities that were notified by the DFS should file their certifications of compliance "as soon as possible" and that any continued failure to certify compliance with Part 500 will be viewed by the DFS as an indication of a substantive deficiency in the Covered Entity's cybersecurity program. Of particular interest, the new guidance also notes that all Covered Entities—even those that filed a notice of exemption from Part 500 pursuant to Section 500.19—must file a certification of compliance with the DFS.[1]

The DFS's cybersecurity reporting guidance is reproduced in full below.

Why did I receive this notice?

All regulated entities and licensed persons of the Department of Financial Services (DFS) were required to file a cybersecurity regulation Certification of Compliance under 23 NYCRR 500 by February 15, 2018. Our records indicate that to date you have not made such filings under the regulation. Please be aware that if you hold more than one license, then you need to file a separate Certification of Compliance for each license you hold.

What if I am late with my filing?

All Covered Entities that have failed to submit the Certification and that are in compliance with the regulation should do so via the DFS cybersecurity portal as soon as possible. The DFS Certification of Compliance is a critical governance pillar for the cybersecurity program of DFS regulated entities, and DFS takes compliance with the regulation seriously. The Department will consider a failure to submit a Certification of Compliance as an indicator that the cybersecurity program of the Covered Entity has a substantive deficiency.

What if I filed for an exemption from the cybersecurity regulations?

People who received the reminder are required to file the Certificate of Compliance even if you filed for an exemption under 23 NYCRR Part 500.19. These exemptions have been tailored to address particular circumstances and include requirements that the Department believes are necessary for exempted entities. Covered Entities are required to file a Certificate of Compliance to confirm that they are in compliance with those provisions of the regulation that apply to the Covered Entity.

I have a receipt showing I filed already?

Please look at the receipt. If the receipt number you received begins with an "E" then it is a receipt for filing a Notice of Exemption and **not** a receipt for filing the required Certificate of Compliance. Your exemption does not excuse the filing noticed below. The Certification of Compliance is to cover the period as of December 31, 2017 for all requirements of the cybersecurity regulation in force by that date. If the receipt number starts with a "C" email cyberregcomments@dfs.ny.gov with your name, license number and the receipt number from your cybersecurity Certificate of Compliance filing.

When will I receive a reply to my email?

DFS will reply to emails received in the above email box within 30 days.

Does this apply to me?

Section 500.01(c) defines a Covered Entity for purposes of the Regulation as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." You will need to determine the applicability of the regulation to your particular circumstances.

How do a file a Certification of Compliance?

Certifications of Compliance should be filed electronically via the DFS Web Portal. Please click the big orange box on the right hand corner that says "Cybersecurity Filing." The Covered Entity will first be prompted to create an account and log in to the DFS Web Portal, then directed to the filing interface. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

* * *

Covered Entities interested in assistance with implementing measures to comply with Part 500 are encouraged to contact any of the authors listed below or your Arnold & Porter contact. The firm's Financial Services team would be pleased to assist with any questions you may have about Part 500, the filing of certifications of compliance or notices of exemption, upcoming examinations, or cybersecurity risk management and compliance more broadly.

1 Section 500.19 provides limited exemptions from Part 500 for, among other persons and entities, certain smaller institutions with minimal contacts with New York State, entities that do not maintain or are not responsible for information systems or the handling of nonpublic information, and for employees, agents, representatives and designees of Covered Entities who are themselves Covered Entities, but are covered by the cybersecurity program of another Covered Entity.

Arnold & Porter

March 1, 2018

SEC Issues Cybersecurity Guidance

Advisory

By Joel I. Greenberg, Sara Adler

In response to the evolving landscape of cybersecurity threats, and the negative and potentially substantial consequences for companies that fall victim to cybersecurity incidents, on February 21, 2018, the SEC published interpretive guidance (Guidance) to assist public companies in preparing disclosures about cybersecurity risks and incidents.[1] The Guidance applies the customary disclosure concepts that apply to material risks to cybersecurity risks, and reinforces and expands prior guidance issued by the SEC's Division of Corporation Finance in October of 2011. In addition, the Guidance addresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents, the application of insider trading prohibitions in the cybersecurity context, and the need for companies and their insiders to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.

Overall, the Guidance does not represent a departure from generally applicable securities law disclosure requirements. It does, however, suggest that registrants should expect increased Staff focus on cybersecurity disclosures.

Disclosure Framework

The Guidance instructs companies to consider the materiality of cybersecurity risks and incidents when preparing their registration statements, and periodic and current reports.[2] Although current disclosure rules don't explicitly refer to cybersecurity risks and incidents, disclosures may be required as they would be in the case of other material risks and incidents.

Periodic reports require timely and ongoing information regarding a company's business and operations, risk factors, legal proceedings, financial statements, disclosure controls and procedures (DCPs) and corporate governance, and are required to include management's discussion and analysis of financial condition and results of operations (MD+A), all of which may require disclosure of cybersecurity risks and incidents. Registration statements must include all material facts necessary to make the statements therein not misleading.[3] The Guidance instructs companies to consider the adequacy of their cybersecurity-related disclosure in this context. Companies can use current reports on Forms 8-K and 6-K to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents. The Guidance encourages companies to use such forms to disclose cybersecurity matters (noting that this practice reduces the risk of selective disclosure and trading in their securities on the basis of material non-public information). The Guidance also urges companies to avoid generic cybersecurity-related disclosure, and to provide specific information that is useful to investors.

Factors to be considered in determining disclosure obligations regarding cybersecurity risks and incidents include the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and the impact of the incident on the company's operations.[4] Although the Guidance states that detailed disclosures that could compromise a company's cybersecurity efforts are not required, companies are expected to disclose cybersecurity risks and incidents that are material to investors, including associated financial, legal, or reputational consequences.

Although the SEC recognizes that all facts may not be initially available, and that ongoing investigations (including cooperation with law enforcement) may affect the scope of disclosure, this alone would not permit avoidance of disclosure. The Guidance also reminds companies that they may have a duty to correct prior disclosure determined to have been untrue (or to have omitted a material fact necessary to make the disclosure not misleading) at the time it was made, and a duty to update disclosure that becomes materially inaccurate after it is made.

Specific Rules

Risk Factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in their securities speculative or risky. Companies should disclose cybersecurity risks if they are among such factors, including risks that arise in connection with acquisitions. Issues to consider in evaluating cybersecurity risk factor disclosure include: the severity and frequency of any prior cybersecurity incidents; the probability and potential magnitude of cybersecurity incidents; the adequacy and cost of preventative actions; limits on the ability to prevent or mitigate certain cybersecurity risks; aspects of the company's business that give rise to material cybersecurity risks; costs associated with maintaining cybersecurity protections; the potential for reputational harm; regulations that may affect requirements relating to cybersecurity and associated costs; and litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents. Companies may need to disclose previous or ongoing cybersecurity incidents or other past events (including those involving suppliers, customers, or competitors) in order to place these discussions in the appropriate context.

MD+A

Item 303 of Regulation S-K and Item 5 of Form 20-F require companies to discuss their financial condition, changes in financial condition and results of operations, including events, trends, or uncertainties that are reasonably likely to have a material effect on their results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition, and such other information that the company believes to be necessary to an understanding of the foregoing. Factors to consider with respect to MD+A disclosure include the costs related to ongoing cybersecurity efforts and cybersecurity incidents, and the risk of potential cybersecurity incidents. In addition to immediate costs of a cybersecurity incident, a host of other costs may also be relevant to the analysis, including costs related to: the loss of intellectual property; preventative measures; insurance; litigation and/or regulatory investigations; compliance with legislation; remediation; reputational harm; and the loss of competitive advantage. Companies are also instructed to consider the impact of cyber incidents on each of their reportable segments.

Description of Business

Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions. Disclosure is required where cybersecurity incidents or risks materially affect any of these items.

Legal Proceedings

Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party. This includes any such proceedings relating to cybersecurity issues.

Financial Statement Disclosures

Cybersecurity risks and incidents may affect a company's financial statements. Relevant examples in the Guidance include: expenses related to investigation, breach notification, remediation and litigation; loss of revenue; warranty or other claims; insurance premium increases; diminished future cash flows; asset impairments; recognition of liabilities; or increased financing costs. Financial reporting and control systems are expected to be designed to provide reasonable assurance that information about the financial range and magnitude of cybersecurity incidents would be incorporated into the financial statements on a timely basis.

Board Risk Oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require disclosure of the role of a company's board of directors in risk oversight. If cybersecurity risks are material to a company's business, this discussion should include the nature of the board's role in overseeing the management of such risk, including disclosures regarding the company's cybersecurity risk management program, and how the board engages with management on cybersecurity issues.

DCPs

The Guidance encourages companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including whether sufficient DCPs are in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to allow timely decisions regarding required disclosure. DCPs should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact, evaluate their

significance, provide for open communication between technical experts and disclosure advisors, and make timely related disclosures.

Exchange Act Rules 13a-14 and 15d-14 require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of DCPs, and Item 307 of Regulation S-K and Item 15(a) of Form 20-F require companies to disclose conclusions on the effectiveness of DCPs. These items should consider the adequacy of controls and procedures for identifying and assessing cybersecurity risks and incidents, and require management to consider whether there are deficiencies in the DCPs that render them ineffective.

Insider Trading

Information about a company's cybersecurity risks and incidents may constitute material nonpublic information. Accordingly, directors, officers, and other corporate insiders would violate the antifraud provisions of federal securities laws if they trade in the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.

The Guidance also encourages companies to consider how their codes of ethics and insider trading policies address trading on the basis of material nonpublic information related to cybersecurity risks and incidents. Companies are instructed to consider implementing restrictions on insider trading during an investigation and assessment of significant cybersecurity incidents.

Regulation FD and Selective Disclosure

Companies are expected to have policies and procedures in place to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made in accordance with that regulation.

1 The Guidance pertains to public operating companies, and does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations.

2 Listed companies are also reminded of obligations to make prompt public disclosure of material information that may be imposed by stock exchange listing requirements.

3 Omitted information is considered to be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available.

4 A traditional materiality analysis requires consideration of the probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity.

Arnold & Porter

February 27, 2018

NYDFS Issues New Cybersecurity FAQs

Advisory

By Erik Walsh, David F. Freeman, Jr., Marcus A. Asner, Adam Golodner, Michael A. Mancusi, Brian C. McCormally, Nancy L. Perkins, Anthony Raglani, Kevin M. Toomey

On February 23, the New York Department of Financial Services (DFS) issued four additional frequently asked questions and responses (FAQs) relating to its new cybersecurity regulation (Part 500).*1* Part 500, several provisions of which became effective on March 1, 2017, has garnered widespread attention from banks, insurance companies and other financial services firms. Covered Entities were required to submit the first annual certifications of compliance to the DFS by February 15, 2018. The four new FAQs supplement earlier releases of FAQs in 2017.*2*

As previously discussed (here, here, and here), Part 500 requires Covered Entities to adopt and maintain a cybersecurity program and corresponding cybersecurity policies and procedures. Although in some ways Part 500 is similar to federal requirements and guidance on cybersecurity for banks and securities firms, it differs in details and imposes substantial reporting obligations. Covered Entities are now required to be in compliance with the majority of the regulation's requirements. Additional requirements of Part 500 related to risk assessments, penetration testing and vulnerability assessments, multi-factor authentication, and risk-based training phase in between March 1, 2018 and March 1, 2019.

These new FAQs are issued as the New York financial services industry prepares for the first wave of DFS examinations that will evaluate a Covered Entity's compliance with Part 500. In January, Superintendent Vullo announced that the "DFS will now be incorporating cybersecurity in all examinations, including adding questions related to cybersecurity to 'first day letters[.]'"*3* Such examinations may lead to matters requiring attention and, potentially, subsequent enforcement actions.

The new FAQs provide additional guidance as Covered Entities continue to navigate compliance with Part 500. Specifically, three of the new FAQs provide guidance on determining whether certain classes of companies qualify as Covered Entities and, thus, are subject to Part 500. The DFS' analyses focus on whether a company is "authorized" so as to fit within the definition of Covered Entity under Section 500.01(c). New FAQ #3 clarifies Covered Entities' obligations when considering merger and acquisition-related strategic options, including that various aspects of the entity's cybersecurity program must be periodically reviewed and tailored to the risk profile of the resulting entity and that cybersecurity due diligence should be prioritized. Although most acquirors already follow sophisticated due diligence processes when evaluating strategic opportunities, the new FAQ underscores the importance of demonstrating to the DFS that cybersecurity was a key consideration.

The four new FAQs are reproduced below.

1. Are Exempt Mortgage Servicers Covered Entities under 23 NYCRR 500?

Under N.Y. Bank Law § 590(2)(b-1), an exempt entity will need to prove its "exempt organization" status. Since the notification is not an authorization from the Department, an Exempt Mortgage Servicer, under N.Y. Bank Law § 590(2)(b-1), will not fit the definition of a Covered Entity under 500.01(c). However, Exempt Mortgage Loan Servicers that also hold a license, registration, or received approval under the provisions of Part 418.2(e) are required to prove exemption and comply with regulation. With respect to DFS's cybersecurity regulation, given the ever-increasing cybersecurity risks that financial institutions face, DFS strongly encourages all financial institutions, including exempt Mortgage Servicers, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

2. Are Not-for-profit Mortgage Brokers Covered Entities under 23 NYCRR 500?

Yes. Not-for-profit Mortgage Brokers are Covered Entities under 23 NYCRR 500. 3 NYCRR Part 39.4(e) provides that Mortgage Brokers "which seek exemption may submit a letter application" to the Mortgage Banking unit of the Department at the address set forth in section 1.1 of Supervisory Policy G 1, "together with such information as may be prescribed by" the Superintendent. As this authorization is necessary for a Not-for-profit Mortgage Broker, it is a Covered Entity under 23 NYCRR 500.

3. Do Covered Entities have any obligations when acquiring or merging with a new company?

Section 500.09(a) states that the "Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations." Furthermore, Section 500.08(b) states that the institution's application security "procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity." As such, when Covered Entities are acquiring or merging with a new company, Covered Entities will need to do a factual analysis of how these regulatory requirements apply to that particular acquisition. Some important considerations include, but are not limited to, what business the acquired company engages in, the target company's risk for cybersecurity including its availability of PII, the safety and soundness of the Covered Entity, and the integration of data systems. The Department emphasizes that Covered Entities need to have a serious due diligence process and cybersecurity should be a priority when considering any new acquisitions.

4. Are Health Maintenance Organizations (HMOs) and continuing care retirement communities (CCRCs) Covered Entities?

Yes. Both HMOs and CCRCs are Covered Entities. Pursuant to the Public Health Law, HMOs must receive authorization and prior approval of the forms they use and the rates they charge for comprehensive health insurance in New York. The Public Health Law subjects HMOs to DFS authority by making provisions of the Insurance Law applicable to them. CCRCs are required by Insurance Law Section 1119 to have contracts and rates reviewed and authorized by DFS. The Public Health Law also subjects HMOs and CCRCs to the examination authority of the Department. As this authorization is fundamental to the ability to conduct their businesses, HMOs and CCRCs are Covered Entities because they are "operating under or required to operate under" DFS authorizations pursuant to the Insurance Law. Moreover, since these entities have sensitive, private data, their compliance with cybersecurity protection is necessary.*4*

* * *

Covered Entities interested in assistance with implementing measures to comply with Part 500 are encouraged to contact any of the authors listed below or your Arnold & Porter contact. The Firm's financial services team would be pleased to assist with any questions you may have about Part 500, upcoming examinations, or cybersecurity compliance more broadly.

1 Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Part 500.

2 New York State-chartered or licensed banks, insurance companies, licensed lenders, check cashers, money transmitters, and their holding companies, and other firms that are licensed by, operating under approval orders of, or otherwise subject to regulation by the DFS are subject to Part 500. Part 500 does not purport to treat federally-chartered banks or federal branches of non-US banks licensed by the Office of the Comptroller of the Currency (OCC) as Covered Entities. Part 500 directly regulates Covered Entities that operate under DFS licenses or approvals, and also has an indirect impact on their internal and third-party vendors and service providers, as well as affiliates that support or share data platforms and systems with DFS-regulated firms.

3 DFS Superintendent Vullo Issues Cybersecurity Filing Deadline Reminder (Jan. 22, 2018).

4 Frequently Asked Questions Regarding 23 NYCRR 500 (Feb. 23, 2018).

Nuts and Bolts of Data Breaches and Identity Fraud

By Marcus A. Asner

Data breaches are very much in the headlines these days. It seems that hardly a week goes by without a story about a major new breach, often involving the personal information of hundreds of thousands or even millions of victims. The financial services industry gets hit especially hard, suffering more breaches than any other industry, and often falling victim to identity thieves who exploit the stolen data to steal money.

Marcus A. Asner

So, how do we stop the bad guys? We probably can't – at least not entirely. But banks certainly can take steps to protect themselves. An important starting point, I believe, is to learn how identity thieves actually work: How do they go about stealing data? And how do they exploit the data they've stolen? By gaining insight into how thieves actually operate, we'll have a better chance both to stop the thief before he strikes, and to limit the damage when he does.

IDENTITY FRAUD 101

So how does a fraudster go about committing identity fraud? I served as a federal prosecutor in Manhattan from 2000 to 2009, where I handled a number of big identity fraud cases, and spearheaded the U.S. attorney's office effort to combat identity fraud. My position led me to spend countless hours debriefing identity thieves and getting to know how they worked.

GETTING IDENTITY DATA

Identity fraud ultimately relies on stolen or fictitious identity information. While some fraudsters personally will steal data, many others will trade for it. The Philip Cummings identity theft case, which I handled as a prosecutor, provides a good example. Cummings didn't personally exploit the approximately 30,000 credit reports he stole; instead, he sold reports to others, who used them for fraud. The scheme's impact was dramatic (leading to losses of as much as $100 million), but the market Cummings created for credit reports was tiny when compared to some of the "carding" forums on the Internet. On websites such as Shadowcrew and Mazafaka, criminals openly traded large quantities of identity data, such as lists of card numbers or Social Security numbers.

Where does all this data come from? Sources of identity data can run the gamut from a complex hacking scheme to simply rooting through a victim's garbage (commonly called "dumpster diving"). Low-tech approaches may be the most common. By stealing mail or a purse, a thief may reap a victim's name, date of birth, and address, and perhaps even her account information and Social Security number. A disadvantage of a low-tech approach, of course, is that it's easy to detect, which means the victim could cancel her cards and the thief will risk getting caught.

Data breaches provide a major source of identity data. Breaches come in different varieties. While hacking catches a lot of news, less sophisticated breaches – which might occur when a laptop is lost or stolen – may well be more prevalent and lead to more damage.

Company insiders often cause the most significant breaches. The BetOnSports case I handled provides a good example. Working with an employee in the credit department of a gambling website, the ring stole customers' private identity information, including names, dates of birth, addresses and credit card information. Hospitals are another favorite target. New York Presbyterian Hospital, for example, suffered a large data breach when a patient admissions representative accessed the records of over 40,000 patients.

Data breaches sometimes rely on plain old trickery. A famous example is the ChoicePoint case, where fraudsters opened at least 50 bogus company accounts with a credit reporting agency in the names of phony debt collectors, insurance agencies or other companies, and then used those accounts to steal identities of 145,000 people. Other approaches involve "phishing," "malware" attacks and "pretexting" schemes. The common thread in these "social engineering" schemes is that a thief seeks to trick a person – perhaps a bank employee – into providing identity information.

"Skimming" involves stealing card information by using a card reading device. Thieves may mount a well-disguised skimming device over an ATM, which records the data of cards inserted into the ATM. To capture PINs, thieves might mount a small camera near the key pad, or may use a "PIN overlay pad," which looks like the original pad, but is equipped to record PINs as victims enter them.

EXPLOITING IDENTITY DATA

What does a fraudster do with stolen data? It depends on the scheme. A skimming scheme, for example, may simply involve loading stolen data onto a blank card and withdrawing cash from an ATM. In other cases, however, fraudsters will go to great lengths to build a façade that they are, in fact, the person they are impersonating.[1] By studying carefully government-issued IDs, fraudsters (or their colleagues) often will create authentic looking documents. The thief also may obtain authentic government-issued IDs, for example, by bribing a DMV employee, or by obtaining her victim's birth certificate, and using it to get additional IDs, such as a driver's license or even a passport.

Establishing a fraud address allows fraudsters to receive mail (including utility bills, which can help in getting a government-issued ID) or packages without alerting their victims. A thief can use a friend's address, a neighbor's apartment or a vacant house. Corrupt real estate agents, and mail receiving agencies also are useful sources for fraud addresses.

A thief's next steps depend on the data she has. A stolen credit report can show where the victim already has accounts. To attack an account, the thief often will send a change-of-address letter to the bank or card company. After a few days, the thief might order new checks, or report a lost card and request a replacement. A fraudster also might apply for a new card or credit line with a new bank.

Once a fraudster gets a new card, she can start reaping the rewards. She might start with a test purchase, buying gas, for example, to see if the card is active, while at the same time allowing for a quick escape. If the card works, the fraudster can attempt cash advances or buy expensive merchandise (such as computers or stereo equipment), which she can resell through a fence. A thief also can obtain convenience checks in one victim's name, deposit them into an account established in another victim's name and withdraw funds.

Fraudsters often gain considerable insight about their victims. The Cummings ring, for example, gathered intelligence about security measures, and focused on banks with weaker security (which they believed were smaller banks and banks in rural areas). Ring members also shared intelligence about which retailers ask for identification for credit card purchases, and would buy from stores with weaker security.

The fraudulent purchases or withdrawals often are surprisingly small. This makes sense. A large withdrawal or purchase is more likely to draw scrutiny than a smaller one. By attacking many victims, each on a relatively small scale, a thief still can make a lot of money, while reducing both the risk of getting caught and the likely penalty.

Not everyone is an easy target. Some may have a lower credit rating or their bank may have strong security. A thief nevertheless can exploit almost anyone's identity. One approach, which I call the "bank account daisy chain" method, involves opening multiple accounts in the names of different victims. Then, a thief may instruct the bank of a wealthy victim to transfer funds to a newly-created account. Once the money lands in the second account, he can withdraw some, and transfer funds to multiple other accounts on the daisy chain, withdrawing money along the way, and making the scheme harder to investigate and stop.

RESPONDING TO THE THREAT

Individuals are the first line of defense. Most of us know not to carry around our Social Security cards or birth certificates, to shred sensitive documents, to carry only the ID and credit cards we actually need, and to take care how we handle sensitive documents. It also helps to monitor account statements. At bottom, the rules are simple: (1) know what identity data you have, (2) make sure it's secured so that (a) the bad guys likely won't be able to get it, and (b) if they do get it, your exposure is limited and your most sensitive material remains safe and (3) stay alert for signs that someone is using your identity. And if you do end up a victim, you should take aggressive steps to correct your credit history, and prevent further attacks.

Many of the ways individuals can protect their data also are useful for businesses, although the difference is that corporations typically possess much more data, including data on their employees and customers. The FTC's free guide, "Protecting Personal Information, A Guide For Business," provides useful advice. In a nutshell, businesses need to guard against both low-tech sorts of attacks and more sophisticated hacking schemes – by locking filing cabinets, disposing of personal data appropriately and establishing robust, up-to-date IT security systems. Strong password protocol and computer firewalls are crucial. To guard against a corrupt insider – such as the next Philip Cummings – companies should limit and track which employees have access to sensitive data, and routinely monitor the data that employees access. It also helps to divide sensitive data into separate components, limiting any single employee's access. To limit the impact of any breach, businesses need to understand fully what data they have, and keep only the material they actually need. Financial institutions also should routinely reevaluate their data security, looking for vulnerabilities and fixing them as they arise. And banks can fight social engineering schemes with employee training, clear and enforced rules articulating the information employees may provide over the telephone or the Internet and monitoring interactions with customers.

How do banks protect the money and other valuables they hold? Knowing how identity thieves actually operate will help. Remember, one of the first things an identity thief often does is change the victim's address. So change-of-address letters can be red flags. Banks can help thwart identity theft by contacting the old email address or phone number, and notifying the victim of the change. Banks also can develop programs to look for unusual moves or purchasing activity. Here's an example from my own life: I'm a lawyer in New York, but a few years ago I found myself in Oklahoma and decided to buy some cowboy boots. My credit card company recognized this as unusual (it was), and immediately called my cell to determine if the transaction was real. Banks also can protect their online customers by recognizing commonly used computers, establishing better password protocols and asking customers non-obvious security questions. Banks also limit the damage from attacks by imposing limits on the withdrawals permitted through vulnerable access points such as ATMs.

Finally, financial institutions need to plan for the worst. Companies hit with a data breach often face a dizzying array of practical and legal issues, ranging from investigating and stopping the breach, to interfacing with law enforcement, complying with victim notification requirements, dealing with the press, and defending civil litigation. Having a plan to address a security breach – such as a plan to change customer passwords, disconnect the IT system from the Internet, and timely notify victims – and taking the time to go through table top "fire drill" type exercises, can go a long way toward helping banks execute an effective response and minimize the impact of any breach. ■

Marcus Asner is a partner at the New York office of Arnold & Porter. Asner is a trial lawyer in the firm's white collar practice group and co-chairs the privacy and data security practice. Asner has extensive experience with data breaches, cybercrime, corporate espionage, money laundering and bank fraud matters. He can be reached at Marcus.Asner@apks.com or (212) 836-7222.

FOOTNOTES

1. The District Court's opinion in the Cummings matter provides a useful description of how one identity theft ring went about exploiting stolen identity data. *United States v. Abiodun*, 442 F. Supp. 2d 88, 90-94 (S.D.N.Y. 2006), aff'd in pertinent part, 536 F.3d 162 (2d Cir. 2008).

Arnold & Porter

December 19, 2017

New York Department of Financial Services Issues Additional Cybersecurity FAQs

Advisory

By David F. Freeman, Jr., Marcus A. Asner, Michael A. Mancusi, Brian C. McCormally, Adam Golodner, Nancy L. Perkins, Anthony Raglani, Kevin M. Toomey

On December 12, 2017, the New York Department of Financial Services (DFS) issued four additional frequently asked questions (FAQs) relating to its new cybersecurity regulation (Part 500).[1] The regulation, which became effective on March 1, 2017 and has garnered widespread attention, requires submission of the first annual certification of compliance to the DFS by February 15, 2018. The four new FAQs supplement an earlier release of FAQs in September 2017.

As previously discussed (here and here), Part 500 requires Covered Entities[2] to adopt and maintain a cybersecurity program and corresponding cybersecurity policies and procedures. Part 500 is believed to be the first state effort of its kind regulating cybersecurity of financial services firms. Although in some ways Part 500 is similar to federal requirements and guidance on cybersecurity for banks and securities firms, it differs in details and imposes substantial reporting obligations. Covered Entities are now required to be in compliance with the majority of the regulation's requirements and, after the submission of certifications for the first time in February 2018, additional requirements of Part 500 phase in between March 1, 2018 and March 1, 2019.

Covered Entities that are implementing measures to comply with Part 500 and preparing certifications for submission will likely find the new FAQs instructive. For example, new FAQ #2 and its response clarifies that Covered Entities may not rely solely on certificates of compliance received from Third Party Service Providers[3] to comply with the requirements of Section 500.11(a)(3). The DFS clarifies that additional due diligence of third parties is required to "assess the risks each Third Party Service Provider poses to [the Covered Entity's] data and systems and effectively address those risks." Although this guidance is consistent with the existing federal expectations for managing risks associated with third-party relationships, it may alter certain Covered Entities' approaches when preparing to submit annual certifications of compliance to the DFS. New FAQ #2 clarifies that reliance on sub-certifications is limited and, on their own, is insufficient to satisfy DFS expectations.

The four new FAQs are reproduced below.

1. Assuming there is no continuous monitoring under 23 NYCRR Section 500.05, does the Department require that a Covered Entity complete a Penetration Test and vulnerability assessments by March 1, 2018?

The Regulation requires Covered Entities to have a plan in place that provides for Penetration Testing to be done as appropriate to address the risks of the Covered Entity. Such plan must encompass Penetration Testing at least annually and bi-annual vulnerability assessments, but the first annual Penetration Testing and first vulnerability assessment need not have been concluded before March 1, 2018 under Section 500.05. The Department expects all institutions with no continuous monitoring to complete robust Penetration Testing and vulnerability assessment in a timely manner as they are a crucial component of a cybersecurity program.

2. If Covered Entity A utilizes Covered Entity B (not related to Covered Entity A) as a Third Party Service Provider, and Covered Entity B provides Covered Entity A with evidence of its Certification of Compliance with NYSDFS Cybersecurity Regulations, could that be considered adequate due diligence under the due diligence process required by Section 500.11(a)(3)?

No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019.

3. Does a Covered Entity need to amend its Notice of Exemption in the event of changes after the initial submission (e.g., name changes or changes to the applicable exemption(s))?

If there are changes, the Covered Entity should submit a new Notice of Exemption, which would not be considered an amendment to the original submission. For example, if a Covered Entity originally submitted a Notice of Exemption stating that it qualified for exemptions under Sections 500.19(b) and 500.19(a)(1), but it now only qualifies for a Section 500.19(a)(1) exemption, then the Covered Entity must submit a new Notice of Exemption with the correct information.

The Department also emphasizes that Notices of Exemption should be filed electronically via the DFS Web Portal http://www.dfs.ny.gov/about/cybersecurity. The Covered Entity should utilize the account that they used to file the original Notice of Exemption or create a new account if an individual filing was previously not made. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

4. Should a Covered Entity send supporting documentation along with the Certification of Compliance?

The Covered Entity must submit the compliance certification to the Department and is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the regulation. The Department also expects that the Covered Entity maintains the documents and records necessary that support the certification, should the Department request such information in the future. Likewise, under 23 NYCRR Section 500.17, to the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity must document such efforts and maintain such schedules and documentation for inspection during the examination process or as otherwise requested by the Department.*4*

* * *

Covered Entities interested in assistance with implementing measures to comply with Part 500 are encouraged to contact any of the authors listed below or your Arnold & Porter Kaye Scholer contact. The firm's financial services team would be pleased to assist with any questions you may have about Part 500, its certification, or cybersecurity compliance more broadly.

1 Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Part 500.

2 New York State-chartered or licensed banks, insurance companies, licensed lenders, check cashers, money transmitters, and their holding companies, and other firms that are licensed by, operating under approval orders of, or otherwise subject to regulation by the DFS are subject to Part 500. Part 500 does not purport to treat federally chartered banks or federal branches of non-US banks licensed by the Office of the Comptroller of the Currency (OCC) as Covered Entities. Part 500 directly regulates Covered Entities that operate under DFS licenses or approvals, and also has an indirect impact on their internal and third-party vendors and service providers, as well as affiliates that support or share data platforms and systems with DFS-regulated firms.

3 "Third Party Service Provider(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii)provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity." 23 N.Y.C.R.R. § 500.01(n).

4 Frequently Asked Questions Regarding 23 NYCRR 500 (Dec. 12, 2017).

Arnold & Porter

February 22, 2017

New York Department of Financial Services Issues Final Cybersecurity Regulations

Advisory

By Marcus A. Asner, David F. Freeman, Jr., Adam Golodner, Michael A. Mancusi, Brian C. McCormally, Nancy L. Perkins, Anthony Raglani, Kevin M. Toomey

On February 16, 2017, the New York Department of Financial Services (DFS) released final cybersecurity regulations to be codified under 23 N.Y.C.R.R. Part 500 (the Final Rule). The Final Rule contains few substantive revisions from the proposed rule issued by the DFS in late December 2016 (the Revised Proposal), which superseded the original proposed rule issued by the DFS in September 2016.

New York State-chartered or licensed banks, insurance companies, licensed lenders, check cashers, money transmitters, and their holding companies, and other firms that are licensed by, operating under approval orders of, or otherwise subject to regulation by the DFS are subject to the Final Rule (Covered Entities). The Final Rule does not purport to treat federally-chartered banks or federal branches of non-US banks licensed by the Office of the Comptroller of the Currency (OCC) as Covered Entities. The Final Rule directly regulates Covered Entities that operate under DFS licenses or approvals, and also has an indirect impact on their internal and third-party vendors and service providers, as well as affiliates that support or share data platforms and systems with DFS-regulated firms.

The Final Rule is believed to be the first state effort of its kind regulating cybersecurity of financial services firms. Although in some ways the Final Rule is similar to federal requirements and guidance on cybersecurity for banks and securities firms, it differs in details and imposes reporting obligations to the DFS.

The Final Rule will become effective on March 1, 2017 and provides for staggered transition periods for compliance with various aspects of the regulations. Covered Entities must comply with most of the requirements of the Final Rule by August 28, 2017. The Final Rule includes longer transition periods for select requirements. Covered Entities are given one year to comply with the Final Rule's requirements relating to penetration testing and vulnerability assessments, periodic risk assessments, multi-factor authentication and certain training and monitoring provisions. The first annual certification of compliance to the DFS is required on February 15, 2018. Covered Entities are given 18 months to comply with requirements relating to an audit trail, application security, data retention, encryption, and certain training and monitoring provisions and two years to comply with third party service provider requirements.

We have also prepared a comparison of the Revised Proposal and the Final Rule.

Substantive Revisions to the Revised Proposal

The Final Rule retains the vast majority of the provisions of the Revised Proposal, which are discussed in detail in our January 9, 2017 client advisory titled New York Department of Financial Services Revised Proposed Cybersecurity Regulations. The most substantive revisions in the Final Rule include new exemptions for certain insurance companies, namely captive insurance companies, out-of-state risk retention groups, and charitable annuity societies.

- Under Section 500.19(e) of the Final Rule, certain captive insurance companies are now exempted from the majority of the Rule's requirements. Specifically, captive insurance companies that are Covered Entities (i.e., those operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York Banking Law, Insurance Law or Financial Services Law) and are not required to access or utilize nonpublic information (NPI), other than information relating to its corporate parent company, are now only required to

conduct a periodic risk assessment (Section 500.09), implement third party service provider security policies and procedures (Section 500.11), maintain policies and procedures governing limitations on data retention (Section 500.13), and comply with notification and certification requirements (Section 500.17).

- Under Section 500.19(f), permitted charitable annuity societies, risk retention groups not chartered or licensed in New York, and accredited reinsurers or certified reinsurers accredited under 11 N.Y.C.R.R. Part 125, each of which must not otherwise qualify as a Covered Entity, are exempt from all of the requirements under the Final Rule.

In addition, the Final Rule relaxes to three years the record retention requirements relating to audit trails designed to detect and respond to cybersecurity events, as described in Section 500.06(a)(2). The record retention period of five years remains unchanged for records relating to systems designed to reconstruct material financial transactions to support normal operations and obligations of the Covered Entity, as described in Section 500.06(a)(1).

Finally, the Final Rule revises certain proposed provisions under Section 500.19(a) to clarify that the quantitative operational standards relating to exemptions for smaller entities are based on the New York operations of the entities, although the New York staffing and revenues of affiliates are included in certain aspects of these *de minimis* exemptions. Specifically, under Section 500.19(a)(2), entities with fewer than 10 New York employees, including New York staff of the Covered Entity, its affiliates and any independent contractors, are subject only to select provisions of the Final Rule (specifically, Sections 500.02, 500.03, 500.07, 500.09, 500.11, 500.13 and 500.17). Under Section 500.19(a)(2), entities with less than $5 million in gross annual revenue (including revenues of the Covered Entity and its affiliates) in each of the last three fiscal years from their New York business operations are granted the same limited exemption from the Final Rule. Smaller entities that are eligible for a limited exemption will therefore remain subject to the Final Rule's core requirements to maintain a cybersecurity program, policies and procedures, and a third-party service provider security policy, and will be required to certify compliance to the DFS. For an entity to avail itself of any exemption under Section 500.19, it must file with the DFS a Notice of Exemption, as provided in Appendix B of the Final Rule, within 30 days of determining that it is exempt.

Considerations

Despite concerns voiced by commenters during the two rounds of notice-and-comment that preceded the Final Rule, certain proposed provisions that created confusion or which may subject firms to significant compliance costs remain unchanged in the Final Rule. For example, regarding key points that we mentioned in our analyses of the proposed regulations:

- It is unclear to what extent firms with multi-state enterprise-wide operations, but with only limited ties to New York state, could be deemed to be Covered Entities. The enterprise-wide activities of such institutions could be made subject to the Final Rule, possibly through affiliated DFS-regulated insurance entities and other financial services firms, even if the activities that occur within the DFS's jurisdiction or involve the NPI of New York residents are minimal.
- Completion of an annual certification of compliance is likely to be costly for Covered Entities and will require senior officer(s) of such Entities to obtain actual, perhaps extensive knowledge of compliance systems and controls. Prior DFS statements in connection with the issuance of the Revised Proposal suggest that a Covered Entity's certifying senior officer(s) and/or directors could be held personally liable for perceived compliance shortcomings.
- Although by its terms the Final Rule does not treat national banks, federal savings banks or federally-licensed branches of non-US banks as Covered Entities, the use of common computer and communications platforms among affiliated financial services firms, their interrelated cybersecurity efforts, and the inclusion of "affiliates" of Covered Entities into the measurement of the *de minimis* exemptions, and certain other aspects of the Final Rule might indirectly, as a practical matter, effectively regulate national banks, federal savings banks, and federally-chartered branches of non-US banks that are affiliated with Covered Entities. However, some aspects of the Final Rule may be preempted by federal law as applied to national banks, and in any event, enforcement of the regulations by the DFS against national banks is likely precluded by federal law, which vests with the OCC exclusive visitorial authority regarding the content and conduct of activities authorized for national banks under federal law.
- Similarly, although the DFS is not the licensing or regulatory authority for broker-dealers or investment advisers in New York and those entities are not directly subject to the Final Rule, the use of common computer and communications platforms among affiliated financial services firms may as a practical matter regulate the operations of broker-dealer and investment adviser firms that are affiliated with Covered Entities. Section 15(i) of the Securities Exchange Act (the Exchange Act) and Section 203A(b) of the Investment Advisers Act (the Advisers Act) limit the application of state laws, which establish certain functional and reporting requirements upon broker-dealers and investment advisers that differ

from or add to requirements established by the Exchange Act, the Advisers Act or regulations issued thereunder by the Securities and Exchange Commission.

- The definition of NPI subject to the Final Rule's cybersecurity provisions and controls remains broad, and Covered Entities need to quickly identify all of the business data and information systems that will fall under the multi-factor authentication, risk-based authentication, and encryption requirements of the Final Rule and create plans for (i) meeting applicable requirements for this data and these networks, and (ii) determining and documenting any choice to use alternative compensating controls.
- Covered Entities may wish to consider various strategic alternatives for managing institutional and personal regulatory risk, including charter conversion (to a new home state or a national bank charter), relocation and reorganization.

In conclusion, the Final Rule provides little relief or clarification for Covered Entities relative to the Revised Proposal. The implementation of compliance systems that conform to the Final Rule likely will be a challenging and costly exercise—and the Final Rule poses ongoing liability risks for firms and their individual officers and direct

Aon Cyber Solutions

2018 Cybersecurity Predictions

A Shift to Managing Cyber as an Enterprise Risk

Published: January 2018

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

Table of Contents

Introduction

Foreword 1
Scorecard 4

Predictions

Prediction 1: Waking up to cyber liability 6
Prediction 2: Managing cyber as an enterprise risk 8
Prediction 3: Regulatory spotlight widens 10
Prediction 4: Criminals attack businesses embracing IoT 12
Prediction 5: Companies implement multi-factor authentication 14
Prediction 6: Bug bounty programs go mainstream 16
Prediction 7: Ransomware attackers get targeted 18
Prediction 8: Insider attacks fly under the radar 20

Contacts 22

References 23

Foreword

Preparing security professionals and business leaders to shift their thinking and manage cyber as an enterprise risk in 2018.

Since issuing our 2017 predictions, we've seen a dramatic rise in the sophistication, scale, and impact of cyber attacks. As companies strive to enrich their customer experiences through a spectrum of endpoints, ranging from mobile devices to automobiles, the attack surface has increased dramatically. With this ever-growing threat landscape comes a proportionate increase in the impact that cyber attacks have on enterprises, and the customers they serve. This report draws on our experience working with boards and C-suites, as well as security and risk professionals to plan for, mitigate, and manage the expanding impact of cyber risk across the enterprise.

Our 2017 Predictions: A year of large-scale cyber attacks with significant impact to organizations across sectors

The swift, public, and pervasive cyber attacks in 2017 demonstrated how cyber risk cannot be effectively managed solely as an information technology (IT) issue. The WannaCry ransomware attack hit over 200,000 computers in 150 countries,[1] taking businesses offline, disrupting sales and operations. Arguably the most significant data breach in U.S. history hit Equifax, exposing the sensitive data of 143 million people,[2] while subjecting the company to legal claims resulting in a dramatic loss of shareholder value and executive resignations.[3]

Additionally, as we predicted, criminals hijacked hundreds of thousands of Internet of Things (IoT) devices around the globe to attack third parties, and also advanced their social engineering and spear-phishing tactics.

Beyond large scale interruptions to global commerce,[4] 2017 witnessed the influence of cyber attackers on politics and policy. Russian hackers attempted to influence election outcomes around the globe, and Chinese hacker groups, known for targeting U.S. defense and aerospace companies, turned their attention to critical infrastructure across Asia.[5]

Data integrity attacks, where criminals seek to sow doubt over the accuracy and reliability of information, became a dominant issue in the public and private spheres as bad actors hit with false media reports and other misinformation campaigns. Major social media and technology companies came under fire as unwilling facilitators of these attacks.

As we anticipated, regulatory pressure for financial services institutions to conduct red-team testing increased in major markets including Hong Kong, the European Union (EU), and others. In our own experience working with clients, while some enterprises have begun to undertake proactive measures to test and remediate exposure, we continue to see a significant shortfall around conducting cybersecurity due diligence, particularly around M&A transactions.

"Today's silo-driven approach to cyber risk management will begin to disintegrate in 2018 in favor of a coordinated C-suite driven approach as leading companies begin to view the impact of cyber risk holistically across all functions of the enterprise."

Our 2018 Predictions: A shift to managing cyber as an enterprise risk

In our 2018 predictions, we examine how these and other dynamics will require companies to shift their approach to cyber risk management. Companies' increasing reliance on technology, regulators' focus on protecting consumer data, and the value of non-physical assets are causing a convergence of cyber exposures that will require security to be integrated into both business culture and risk management frameworks.

Global regulatory pressures will continue to intensify in 2018, with renewed enforcement of compliance and audit certificate requirements, as vanguard regulators pursue their missions to protect against the impact of cyber attacks. Mounting regulatory complexity will provoke calls for harmonizing this landscape.

Whereas past directors and officers (D&O) liability claims over cyber incidents have largely been dismissed, we expect to see more claims successfully brought against D&Os, holding them personally responsible for the handling of cyber incidents. In our predictions, we examine how the events of 2017 shifted this landscape. With cyber events now ranking among the top three triggers for D&O derivative actions,[6] we expect these claims to intensify in 2018. Heightened concern among executives over liability, and the financial and operational impact of cyber risk, will drive changes in the insurance market. As businesses demand more comprehensive cyber coverage, that coverage will reach beyond provisions in other policies, such as property, errors and omissions, and general liability.

We also anticipate 2018 will be a year of increased accountability over cyber attacks. Organizations facing risks from insider threats, IoT security, ransomware attacks and more, will have to demonstrate that they have followed best practices to protect consumers and employees. This will lead to an increased focus on proactive measures, such as better data hygiene, bug bounty programs, and multi-factor authentication (MFA) becoming standard practice for a broader and more diverse set of companies.

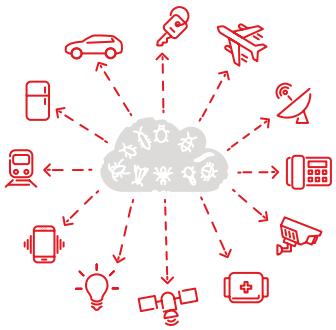
Today's silo-driven approach to cyber risk management will begin to disintegrate in 2018, in favor of a coordinated C-suite driven approach as leading companies begin to view the impact of cyber risk holistically across all functions of the enterprise.

We hope this year's predictions will be a useful launching pad to shift thinking and take action to mitigate and manage cyber risks.

Jason J. Hogg
Chief Executive Officer, Aon Cyber Solutions

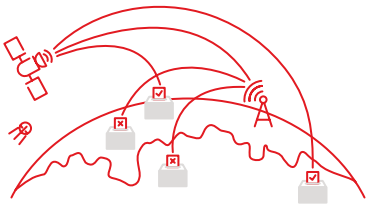
2017 Scorecard

True | Mixed | False



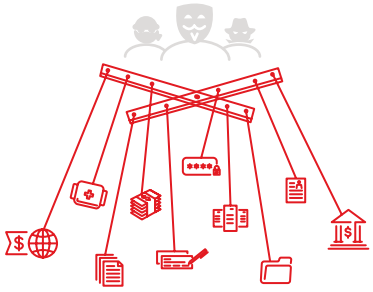
1. Criminals harness IoT devices as botnets to attack infrastructure

Hackers harnessed IoT devices as botnets, causing heightened concern over a potential DDoS attack on critical infrastructure. Security researchers identified new, rapidly growing botnets that hijacked millions of devices, including "Hajime" and "IoT_reaper". North Korea's "Hidden Cobra" operation aimed to use networks of devices to attack U.S. infrastructure.



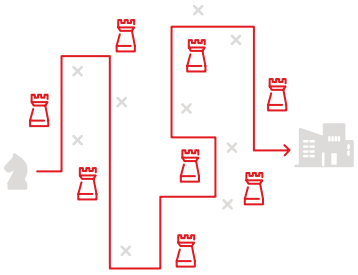
2. Nation state cyber espionage and information war influences global politics and policy

Hackers targeted elections and critical infrastructure, and conducted cyber espionage, impacting domestic politics and international relations. The U.S. investigation into Russian interference in the 2016 election continues. Qatar alleged that Abu Dhabi posted politically motivated fake news on its state news website. The U.S. started a formal probe into Chinese government cyber espionage.



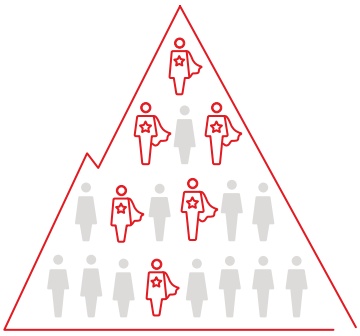
3. Data integrity attacks rise

The spread of misinformation continued; data integrity attacks rose. The spread of inaccurate, unverified information impacted the market value of companies, response to natural disasters, and swayed public opinion. Cyber attackers weaponized tech and media platforms, prompting calls for tech companies to actively address the problem of manipulated postings, bots, and ads.



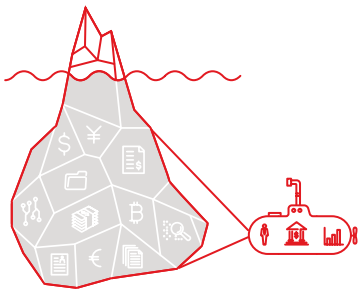
4. Spear-phishing and social engineering tactics become more crafty, more targeted and more advanced

Attackers deployed new spear-phishing tactics against organizations across sectors including major technology companies and government agencies. Hackers tricked employees at international energy companies into opening documents to harvest usernames and passwords, granting access to power switches and computer networks. Fraudsters targeted UK students with an email scam to steal personal and banking details.



5. Regulatory pressures make red teaming the global gold standard with cybersecurity talent development recognized as a key challenge

Global regulators in financial centers worldwide adopted regulation around red team testing, causing security talent shortages. EU financial market infrastructures will undergo testing through an EU red team testing framework. The Hong Kong Monetary Authority enforced the Cybersecurity Fortification Initiative (CFI), including its Intelligence-led Cyber-attack Simulation Testing framework.



6. Industry first-movers embrace pre-M&A cybersecurity due diligence

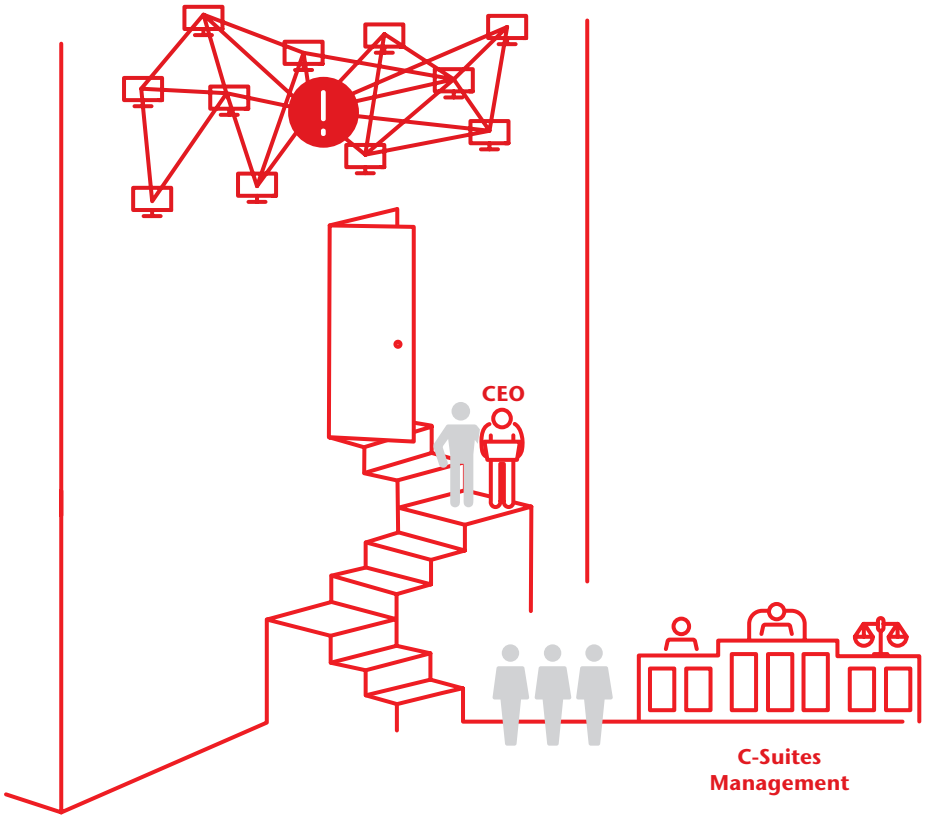
Pre-M&A cybersecurity due diligence is recognized as best practice across industries, but embraced only by first movers. The American Bar Association and others published guidance to help legal and business communities understand key requirements of cybersecurity due diligence that should be part of every M&A transaction.

1. Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.

As boards and executives witness the material impact of cyber attacks, including reduced earnings, operational disruption, and claims brought against directors and officers, businesses will turn to tailored enterprise cyber insurance policies. At the same time, insurers will limit coverage of cyber-related losses in traditional property, casualty, and other business policies.

In 2017, businesses experienced significant material financial impact caused by cyber attacks, with at least six attacks requiring disclosure under U.S. Securities & Exchange Commission guidelines.[7] C-suite executives resigned and market capitalizations dropped following massive thefts of consumer data. Companies faced class-action lawsuits and regulatory investigations over the handling of breaches,[8] with cyber events now ranking among the top three triggers for D&O derivative actions.[9] The WannaCry ransomware and NotPetya malware attacks resulted in companies across industries reporting reduced revenue and profits due to operational problems.[10] These trends have emphasized boards' and executives' liability for ensuring effective cybersecurity controls are in place.

In 2017, C-suite executives resigned following massive data breaches.



In 2018, more companies will disclose severe cyber-related losses in financial reports or analyst calls, as companies face increased scrutiny over their handling of cyber incidents. As cyber attacks drag down earnings, disrupt operations, expose data, and hit share prices, it will no longer satisfy regulators, shareholders, and the public to mandate that a chief executive officer (CEO) or board member step down in the wake of a major compromise. Class-action lawsuits and liability claims will successfully be brought against D&Os, who will be held responsible for failing to uphold their fiduciary responsibility to protect shareholders and consumers from the effects of a breach.

The cyber insurance market will respond to concerns from boards and executives by offering policies reflecting the expanding impact of attacks. A 2017 Ponemon Institute survey found only 24 percent of risk management professionals said their companies had cyber insurance, despite 87 percent viewing cyber liability as one of their top ten business risks.[11] Companies cited inadequate coverage among the top reasons for not purchasing cybersecurity insurance, as well as having property and casualty insurance policies, which often provide limited elements of risk transfer protection from cyber exposures as a "silent" component.

This will change in 2018 as companies demand coverage for the full impact of cyber risk, and insurers explicitly exclude coverage for cyber-related losses in other business policies. As a result, insurers will craft enterprise cyber insurance policies that cover a broad spectrum of cyber-related exposures. Adoption will spread beyond traditional buyers of cyber insurance, such as the retail, financial, and healthcare sectors, to others vulnerable to cyber-related business disruption, particularly as we will see major material cyber incidents caused by system failures and outages impacting airports, airlines, power grids, manufacturing plants, oil and gas, utilities companies and others. Global scale cyber attacks like WannaCry will spur greater adoption, often among first time buyers, in Latin America, Europe, and other geographies outside the U.S., where most coverage is traditionally purchased.[12]

24%

of risk management professionals said their companies had cyber insurance

87%

of risk management professionals view cyber liability as one of their top ten business risks

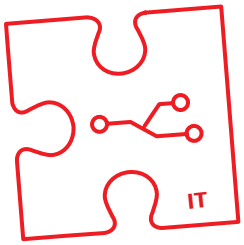
Bottom Line:

In response to the expanding impact of cyber risks on businesses across sectors and geographies and heightened executive concern over liability, the insurance industry will develop new cyber policies while restricting "silent" cyber coverage in other policies. Additionally, both insurers and reinsurers will push for increased scrutiny and improved quantification modeling to better understand potential correlated and systemic cyber perils that could aggregate catastrophic losses across multiple industries and geographies.

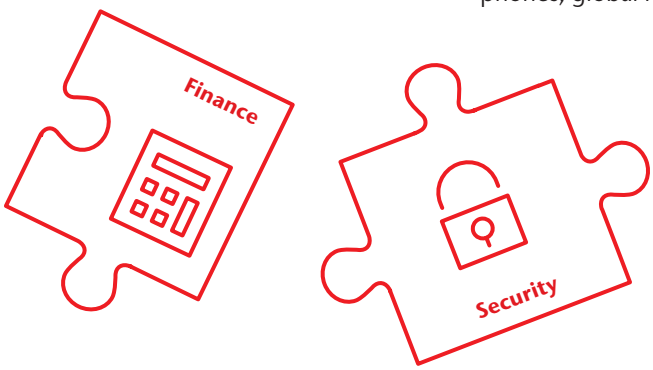
2. As the physical and cyber worlds collide, chief risk officers take center stage to manage cyber as an enterprise risk.

As sophisticated cyber attacks generate real-world consequences that impact business operations at increasing scale, C-suites will be rudely awoken to the enterprise nature of cyber risk. Chief risk officers (CROs) will take center stage, working with information security teams, treasurers, chief financial officers (CFOs), and general counsels (GCs) to improve risk modeling and paint a more holistic picture of the business' exposure.

In 2017, large-scale cyber attacks alerted businesses to the operational impact of technical vulnerabilities, beyond data breaches. Manufacturing companies were taken down; hospitals were extorted by bad actors who held systems for ransom and endangered patient lives; and cyber criminals gained access capable of blacking out U.S. electric power.[13] These attacks and others occurred despite the fact that security spend was up 7 percent in 2017 to $86.4 billion.[14] Despite the impact of cyber risk extending to compliance, technical, finance, human resources, legal and other departments, organizations continued to manage it as if it were only an IT issue. Silos abounded in cybersecurity risk management, and criminals exploited the gaps.



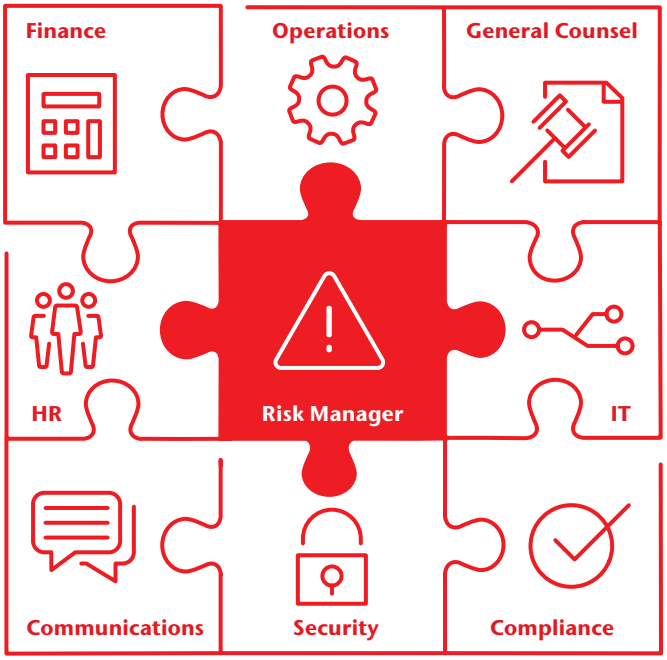
In 2018, C-suites in industries beyond the retail, financial services, and healthcare industries will react to the impact that exploited cyber vulnerabilities can have on their business' ability to operate, weaving cybersecurity into all areas of business risk and breaking down organizational risk management silos. For instance, connected grid systems, infrastructure, supervisory control and data acquisition (SCADA), and industrial control systems, have expanded cyber exposures beyond risks to personally identifiable information (PII) in almost every industry. The C-suites of mature organizations will empower the CRO to enter the cybersecurity spotlight, aligning them closely with information security teams. In 2018, the CROs and chief information security officers (CISOs) will become risk collaborators to better understand their organization's cyber risk exposures and potential "real-world" operational consequences. For example, global logistics companies will gather multidisciplinary teams to anticipate cyber vulnerabilities in applications on drivers' phones; global marketing services firms will look at how cyber vulnerabilities



Silos abounded in cybersecurity risk management, and criminals exploited the gaps.

affect crisis management and business continuity planning; shipping firms will address how cyber impacts operations, such as tankers and goods being remotely diverted. Shipping companies will also continue to assess the potential benefits of smart contracts and block chain technologies with regard to goods and inventory tracking and manifest verification.

As the impact of digital risk and technical vulnerabilities on companies' bottom lines grows through lost sales, business downtime, or product safety concerns, CISOs' visibility into a company's cybersecurity posture will become a major component in how CROs work with CFOs and GCs to assess risk and allocate resources towards insurance solutions. In 2018, CROs will be expected to articulate how digital business operations affect financial exposure. Using the CISO's specialized knowledge of a company's information security posture, alongside sophisticated modeling tools leveraging big data, CROs will improve an organization's ability to model how cyber risk could propagate across the entire enterprise. This will also provide C-suites and boards with a broader picture of the impact of risk on the business as a whole.



Bottom Line:

In 2018, the role of the CRO will be redefined, as they work more closely with CISOs to help company leadership understand the holistic impact of cyber risk on the business. This unique perspective will make the CRO one of the CEO's most valuable assets, as they provide a more meaningful risk story for boards and executive leadership, enabling more effective investment in cybersecurity measures and cyber insurance.

$86.4B

was spent on security in 2017, up 7% from the previous year

3. Regulatory spotlight widens and becomes more complex, provoking calls for harmonization. The EU holds global company to account over GDPR violation; big data aggregators come under scrutiny in the US.

In 2018, regulators at the international, national, and local levels will more strictly enforce existing cybersecurity regulations and increase compliance pressures by introducing new ones. Companies burdened by multiple rules and regulations will mount a campaign to harmonize the complex cybersecurity regulatory landscape.

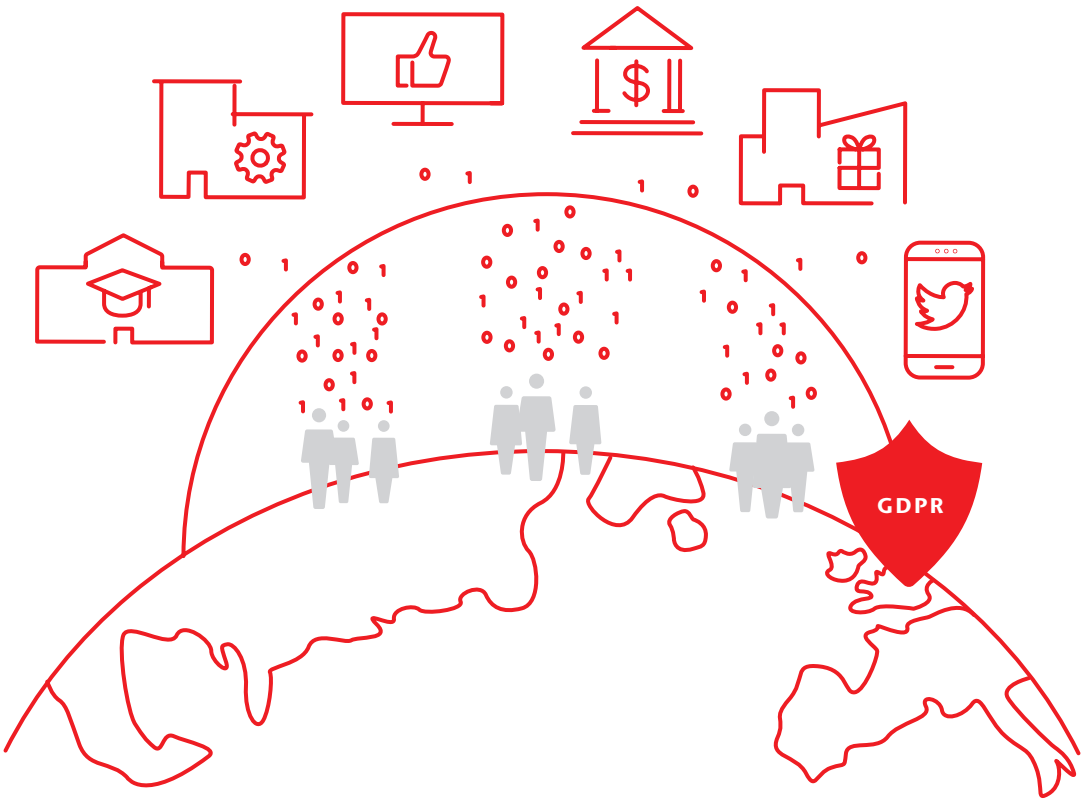
In 2017, new cyber regulations were introduced to address the broad impact of cyber risk across business activities, sectors, and jurisdictions. The EU's focus on setting a universal standard for consumer data privacy now has worldwide significance with the General Data Protection Regulation (GDPR), governing all companies that collect data of EU citizens. Asia-Pacific governments such as Australia, Japan, and South Korea are largely aligned with the EU's approach, albeit with more moderate enforcement and penalties. In the U.S., the New York Department of Financial Services (NYDFS) cybersecurity regulations had major implications for the financial services industry globally.

In 2018, we expect the European Commission will hold major U.S. and global companies to account for GDPR violations, through one or more major enforcement actions demonstrating its seriousness to enforce the regulation internationally, including through fines – a maximum 4 percent of worldwide annual revenue or €20 million (US$23.8 million)[15] – which are uninsurable under most country laws. While there is historically less litigation outside the U.S., consumer businesses in particular could also face the prospect of GDPR-related class action lawsuits, and other impacts such as reputational damages.

In the U.S., while the outcome of the Federal Trade Commission (FTC) versus LabMD litigation will impact whether the scope of the Commission's authority extends to enforcement of cybersecurity standards,[16] in 2018 we will see other regulatory bodies, such as NYDFS, enforcing existing regulations and launching targeted interventions in response to concern over major breaches. For example, big data organizations (aggregators and resellers) will come under renewed scrutiny over how they are collecting, using, and securing data. New regulations will mean that companies in sectors beyond healthcare, financial services, and retail— for example, education—will be forced to address cybersecurity compliance requirements.

Under the burden of significant and ever-increasing regulatory pressures, industry organizations will push back on regulators, calling for the alignment of cyber regulations. Business bodies like the U.S. Chamber of Commerce have already begun lobbying the U.S. government to harmonize regulations with the voluntary framework developed in public-private collaboration under the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).[17] The DigitalEurope trade association has also called for "full consistency" between the GDPR and other legislation in Europe.[18] In general, however, the compliance burden for companies across sectors will get tougher in 2018 before it gets better.

Companies across sectors will therefore need to optimize their compliance programs by leveraging external experts, automation, analytics, and other tools to drive actual, risk-based cybersecurity improvements.



Bottom Line:

As regulators seek to protect against the impact of data breaches and large-scale cyber attacks, with the implementation of GDPR we will see strict enforcement of existing regulation and fines, as well as new rules and guidelines introduced. Companies across sectors, forced to examine the controls in place to comply with multiple regulations, will call for greater alignment to ease the regulatory burden.

4. Criminals look to attack businesses embracing the IoT, in particular targeting a small to mid-sized company providing services to a global organization.

In 2018, global organizations will need to factor into third-party risk management the increased complexities in how their business partners are using the IoT. However, we will not see this happen, and as a result we predict a large company will be brought down by an attack on a small vendor or contractor that targets the IoT as a way into their network. This will be a wake-up call for large organizations to update their approach to third-party risk management, and for small and midsized businesses (SMBs) to implement better security measures or risk losing business.

Enterprises continue to interconnect endpoints, objects, and platforms to their networks, disintegrating traditional network perimeters, converging the digital and the physical worlds, and creating new security challenges. Businesses are expected to have employed 3.1 billion connected things in 2017.[19] Beyond devices, companies are linking more business processes to the Internet to gather data, drive efficiencies, and automate, monitor, and control operations.

This boom in usage could generate up to $11.1 trillion a year in economic value by 2025.[20] Yet, IoT devices are notoriously unsecured and proper patch management programs will continue to be overlooked in 2018. The security vulnerabilities introduced by how businesses are utilizing the IoT therefore present substantial risks, and even if a company's own IoT ecosystem is relatively secure, the impact of how third parties are deploying IoT is neglected. In a 2017 Ponemon study[21], only 25 percent of respondents said the board of directors ask for assurances that IoT risks among third parties are being assessed, managed, and monitored appropriately.

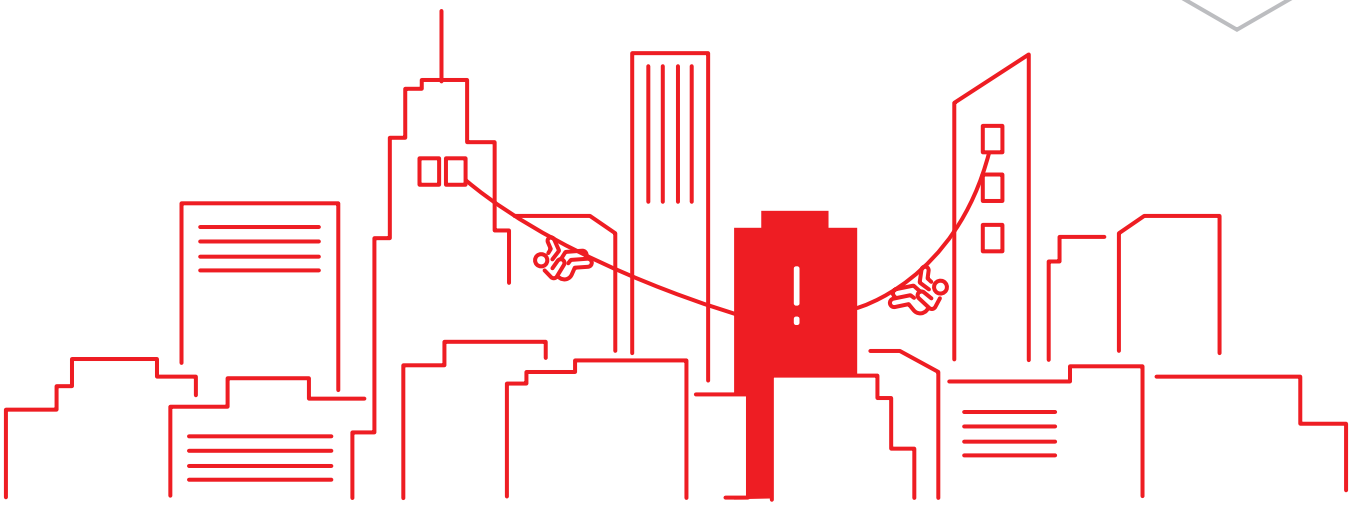
The security vulnerabilities introduced by how businesses are utilizing the IoT present substantial risks. Even if a company's own IoT ecosystem is relatively secure, the impact of how third parties are deploying IoT is neglected.

This is a particular concern for large organizations working with SMBs, given their lower prioritization of cybersecurity. Another recent Ponemon study found that 55 percent of small businesses reported to have been breached in a 12-month period between 2015 and 2016[22], yet a tiny minority said they view it as the most critical issue they face.[23] As enterprises derive more efficiencies from working with SMBs in 2018, hackers will pinpoint smaller businesses that utilize IoT platforms and devices to gain entry into larger businesses. For example, we will see criminals targeting ATM manufacturers and maintenance vendors working with large banks. Additionally, organizations face risks from smaller service providers of printers or copy machines, security camera systems, and other connected endpoints through which client data can be exposed if hacked. As a result, demand for visibility into third-party security will increase and smaller vendors bidding for contracts will have to demonstrate stronger cybersecurity measures around IoT.

55%

of small businesses reported to have been breached in a 12-month period between 2015 and 2016

...yet a tiny minority said they view it as the most critical issue they face.



Bottom Line:

In 2018, we will see an attack on a SMB that has not properly integrated security into its IoT ecosystem, and this attack will extend into the network of a large organization causing exponentially more damage. In response, large organizations will broaden third-party risk management programs and due diligence processes so that they account for weaknesses in vendor IoT security. SMBs bidding to work with them will be forced to improve and document their cybersecurity measures.

5. As passwords continue to be hacked, and attackers circumvent physical biometrics, multi-factor authentication becomes more important than ever before.

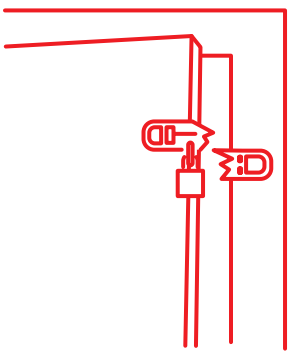
While passwords alone do not provide adequate levels of security, their convenience means that they are still widely deployed. Although they will be phased out as the primary method of authentication on mobile and IoT devices in 2018, they are unlikely to disappear completely. As companies implement biometrics to authenticate identity, criminals will advance their attacks to override these new technologies. In 2018, as more credentials are compromised, and biometrics are hacked, we will see the rise of MFA.

In 2017 we saw companies continue to fall victim to brute force and phishing attacks. A recent study found 81 percent of hacking-related breaches leveraged stolen or weak passwords.[24] As attackers continue to exploit passwords, innovative companies, such as mobile and IoT device manufacturers, are deploying biometrics as an alternative way to authenticate identity. For example, Apple's iPhone X uses facial recognition technology instead of passwords, and banks in financial centers including the UK and Hong Kong are rolling out biometrics in specific situations, such as voice recognition to authenticate customer service calls with high-net-worth individuals.

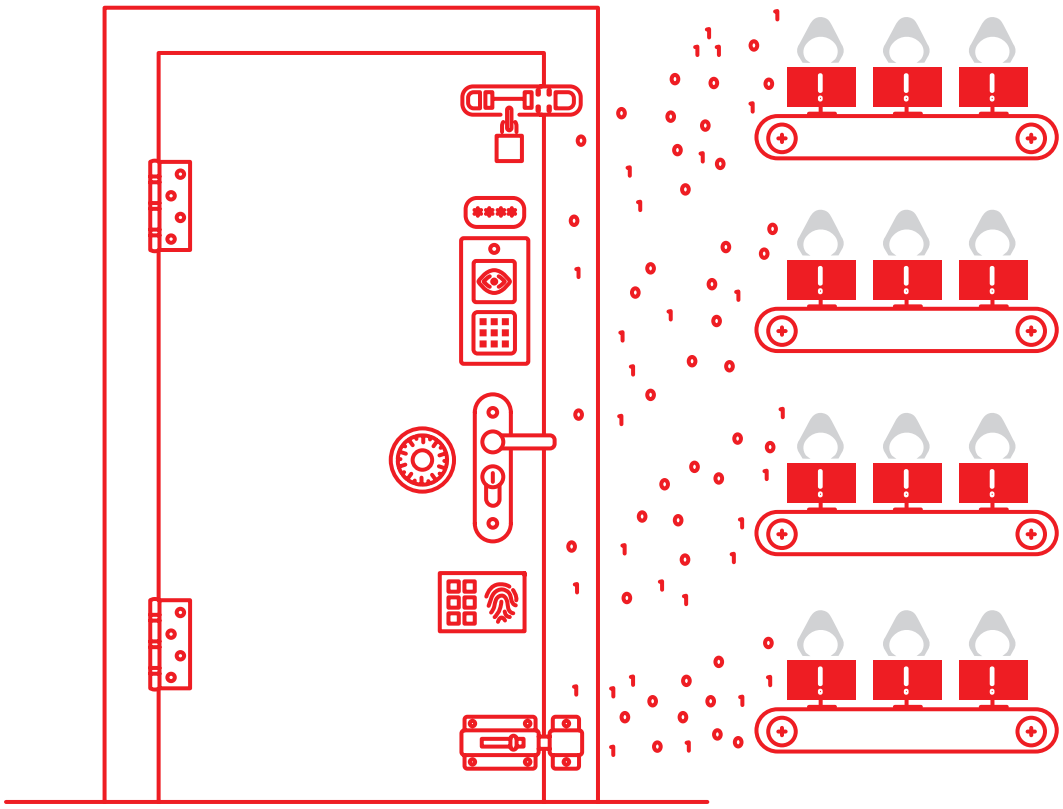
In 2018, these authentication methods, once requisite only for individuals with security clearances, will move mainstream. Physical biometrics, such as facial recognition, iris patterns, or fingerprints will extend beyond mobile devices to everyday usage, for example, replacing access badges to offices. However, even advanced biometrics will not be bulletproof as a single layer of authentication. The hash value behind fingerprints in a device can be stolen and attackers can use forged physical copies of a fingerprint to hack systems. In 2018, we will see a theft of biometrics that creates a lifetime of exposure for consumers, highlighting the challenges inherent in biometrics having no "re-set" process.

To combat the assault on passwords and attacks targeting biometrics, major financial institutions beyond FinTech companies will adopt MFA technologies in earnest, for example using voice recognition plus a PIN or password to authenticate all customer service calls. Individuals will be required to present at least two of the following pieces of evidence to an authentication instrument: knowledge (something they know), possession (something they have), and inherence (something they are). Banks will run behavioral biometrics authentication technologies in the background of online banking websites, continuously collecting information about a user's interactions, like keystroke and mouse movement, to create a unique user template on that device – and asking for more information if the behavior doesn't match the template. Major cloud providers will push for users of their platforms to put MFA into practice.

Even as companies adopt MFA, hackers will devise techniques to penetrate new authentication technologies, just as they devised methods to break two-factor authentication with "SIM swap" attacks. In 2018, we will see new smartphone-based malware targeting MFA applications on mobile phones.



While passwords alone do not provide adequate levels of security, their convenience means that they are still widely deployed.



Bottom Line:

Companies will widely adopt MFA as criminals successfully target single factor authentication, such as usernames and passwords, and biometrics. Even with MFA, companies will need to commit to a proactive, continuous process of testing and improving their defenses, as attackers will continue to evolve their techniques.

81%

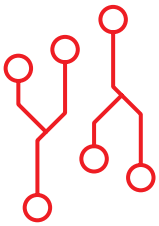
of hacking-related breaches leverage stolen or weak passwords

6. Criminals will target transactions that use points as currency, spurring mainstream adoption of bug bounty programs.

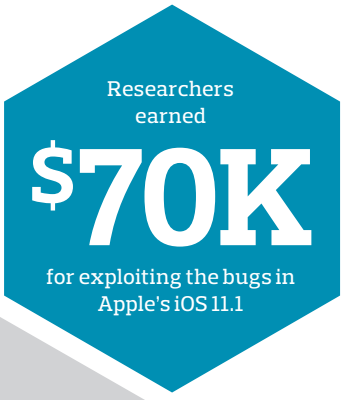
In 2018, companies beyond the technology, government, automotive, and financial services sectors will introduce bug bounty platforms into their security programs. Businesses with loyalty, gift, and rewards programs, such as airlines, retailers, and hospitality providers, will be the next wave of adopters as criminals target transactions that use points as currency.

In 2016 and 2017, we saw organizations in the technology,[25] government,[26] automotive,[27] and the financial services[28] sectors lead the pack in deploying bug bounty programs, crowdsourcing the expertise of skilled security researchers to root out vulnerabilities in exchange for money and recognition. Shortly after Apple's release of iOS 11.1 in 2017, researchers at Tencent Keen Security Lab quickly exploited two bugs,[29] earning $70,000 in rewards — a far lower price than Apple could have paid had the vulnerability been exploited by a malicious attacker.

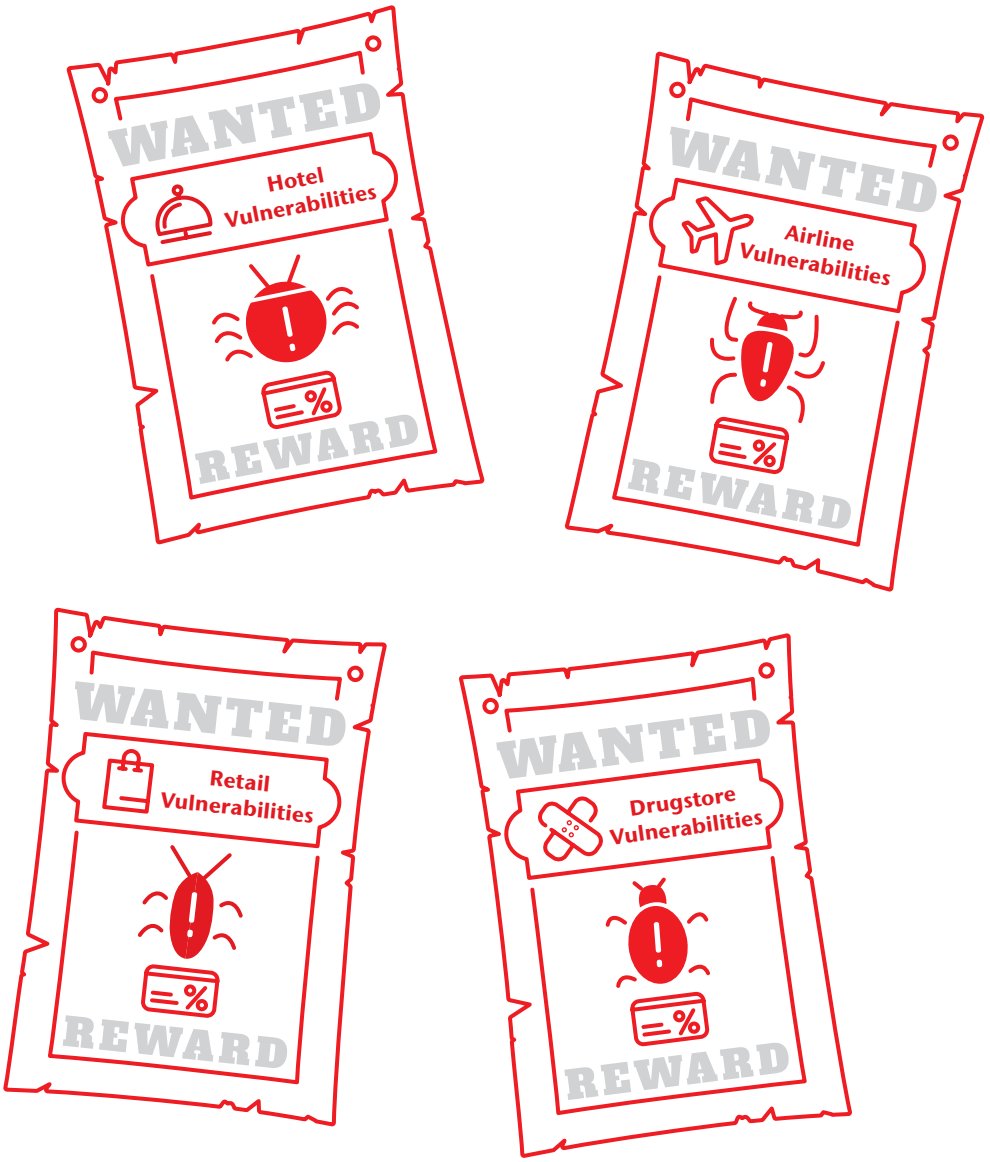
Enterprises with over 5,000 employees accounted for the fastest growth of program launches on the Bugcrowd platform over the past 12 months.[30] In 2018, we will see companies beyond the few early adopters in the airlines industry, as well as retail and hospitality, and other sectors operating rewards programs, adopt bug bounty programs to protect "points as currency". As credit cards become more secure, and criminals target more "card-not-present" transactions like gift cards and rewards points, bug bounty programs will be implemented as an extra layer of defense.



As the threat environment drives broader adoption, bug bounty programs will become part of the standard security lifecycle.



As the threat environment drives broader adoption, bug bounty programs will become part of the standard security lifecycle. Enterprises across industries will be expected to run bug bounty programs to prove they have done everything possible to protect themselves from cyber attacks. As bug bounties go mainstream, more companies will turn to external providers of private bug bounty programs and cybersecurity experts to implement best practices, such as setting up payments, defining the scope of the program, quantifying and remediating vulnerabilities, and managing the program in relation to simultaneous security testing. To meet demand, major cybersecurity and information security service providers will partner with, or acquire, private bug bounty program providers to offer these capabilities.



Bottom Line:

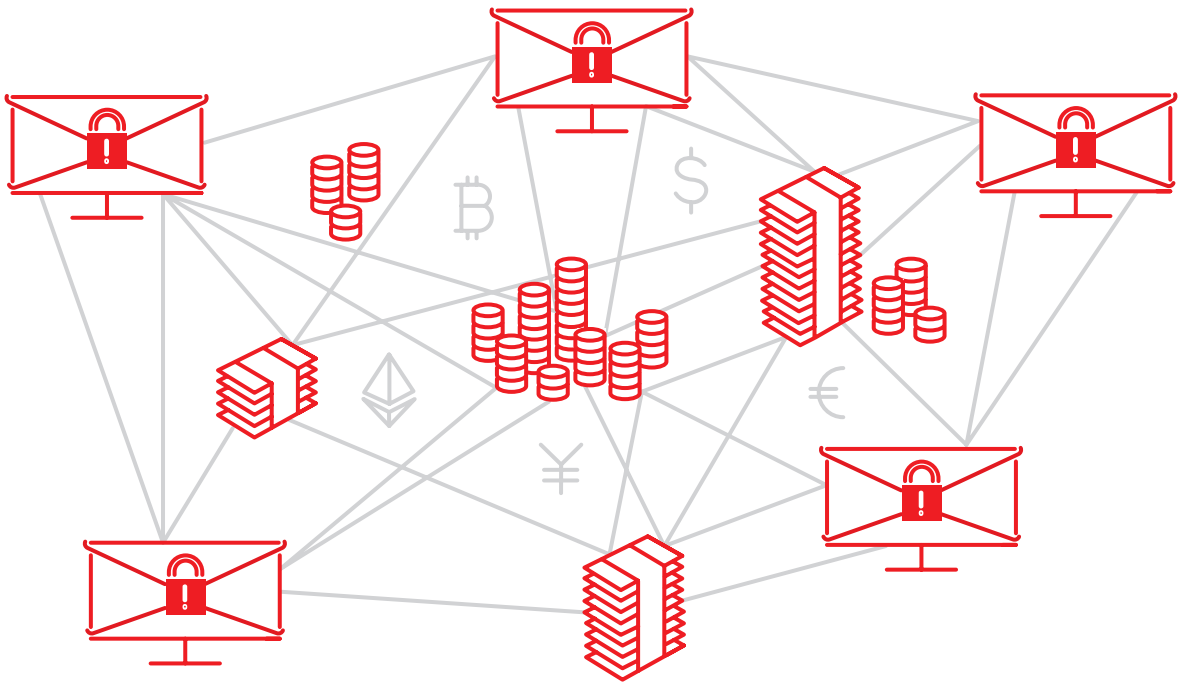
In 2018, bug bounty programs will expand to the wider airline industry, and retail and hospitality sectors, to protect points used as currency. As more organizations embrace bug bounty programs, they will require support from external experts to avoid introducing new risks with improperly configured programs.

7. Ransomware attackers get targeted; cryptocurrencies help ransomware industry flourish.

By the end of 2017, the global cost for organizations of ransomware attacks is estimated to reach $5 billion, up 400 percent from 2016.[31] The WannaCry ransomware attack impacted more than 300,000 people across 150 countries in less than two days. In 2018, criminals will evolve their tactics, including launching well-researched, targeted attacks intended to infect specific high-value assets known to hold critical data.

In the past few years, ransomware attacks relied on infecting systems by taking advantage of vulnerabilities. However, in mid-2017 the perpetrators of the NotPetya ransomware attack changed this landscape. Attackers gained admin credentials which then granted access to infect the non-vulnerable systems of the victim organization, thereby affecting almost all accessible systems in the network. In 2018, we will continue to see large-scale ransomware attacks that target admin credentials to gain access to, and infect, wider networks. With the expected increase in ransomware attacks designed to spread through a network, businesses in 2018 will urgently need to segment their networks. Companies that fail to do so will be impacted by ransomware attacks at a larger scale than necessary.

Attackers will also evolve their tactics in 2018, utilizing forms of benign malware—such as software designed to cause distributed denial-of-service (DDoS) attacks, or launching display ads on thousands of systems— to unleash huge outbreaks of ransomware. Botnet operators will grant ransomware attackers with access to botnet nodes in exchange for payments, allowing them to significantly expand the scope of a ransomware attack.



While attackers will continue to launch scatter-gun-style attacks to disrupt as many systems as possible, we will also see increasing instances of attackers targeting specific companies and demanding ransomware payments proportional to the value of the encrypted assets. To achieve stronger returns in these targeted attacks, criminals will hit environments where access to data and systems is "mission critical," such as hospitals, transportation companies, and manufacturing companies. We also expect to see an increase in the use of ransomware to infect IoT devices, which come with a diminished set of security features by default to facilitate "out of the box functionality", and users tend to maintain these original settings once the devices start functioning. We have already seen the Mirai botnet that harnessed IoT devices to launch DDoS attacks, and anticipate ransomware to infect smart thermostats and other smart devices in 2018.

$5B

is the estimated global cost for organizations of ransomware attacks in 2017 – up 400% from 2016

In addition, cryptocurrencies will continue to support the flourishing ransomware industry overall, despite law enforcement becoming more advanced in their ability to trace attacks, for example, through bitcoin wallets.

To protect themselves in 2018, companies will have to go beyond the vital step of creating backups. Companies will need to utilize systems that can create snapshots in time, or maintain multiple versions of files created over the course of the day, to enable restoration to a specific point in time prior to the backup with minimal loss of productivity. Security professionals will need to routinely test if their backups allow them to restore the data and files in a specific timeframe to ascertain the downtime the company can withstand if a ransomware attack is realized.

In 2018, we will also see more companies recognizing the need to implement the *Principle of Least Privilege*—limiting file access rights for users to the bare minimum permissions they need to perform their work to reduce the number of files that could be encrypted in the event of a ransomware attack. Advanced companies will grant employees only the access needed for the business activities of a specific function, rather than providing automatic access to everything.

Bottom Line:

With perpetrators carrying out wide-scale, profitable, and disruptive attacks in 2016 and 2017, the number of attackers, the volume of ransomware families, and the number of infections increased dramatically. In 2018, we will see attackers continuing to launch large-scale attacks, but also evolve their tactics to implement targeted attacks with demands for greater payments proportional to the value of the assets. This activity will be supported by the continued rise of cryptocurrencies. A company's ability to protect against and recover from ransomware attacks in 2018 will rely on implementing proactive technical measures and business continuity plans.

8. Insider risks plague organizations as they underestimate their critical vulnerability and liability, and major attacks continue to fly under the radar.

Since we predicted the rise of the "insider" in 2016, we have seen organizations severely impacted by actions taken by malicious, careless, negligent, and unaware employees, contractors, leavers, consultants, and others with access to information, systems, and networks. Despite this, in 2017 we saw businesses underinvest in proactive insider risk mitigation strategies and 2018 will be no different. With a continued lack of security training and technical controls, coupled with the changing dynamics of the modern workforce, the full extent of cyber attacks and incidents caused by insiders will not even become fully public.

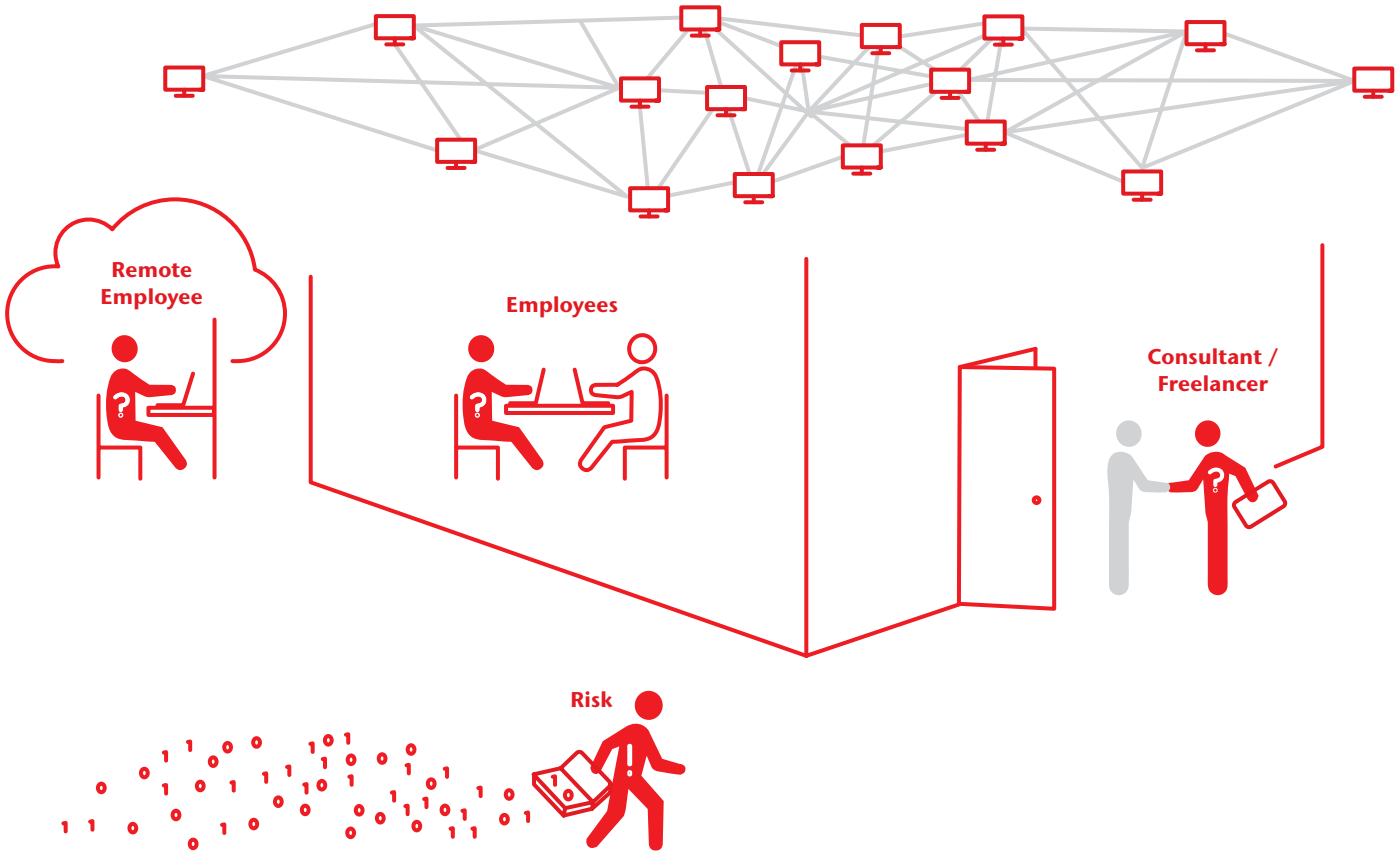
Disruptive technologies and the changing employer-employee relationship is challenging the security of organizations in unprecedented ways. The rise of the gig economy, consulting, and freelancing[32] means the definition of an "insider" has changed, and boundaries between internal and external employees are fluid. Corporations depersonalizing the workforce and creating more virtually connected ecosystems has impacted the level of an employee's psychological investment and engagement in their organization.[33] Media hunger for private documents such as those publicized in the Panama and Paradise Papers attacks is fueling the motivation to expose and leak information from inside sources. These factors contribute to why companies will continue to be impacted by actions—both intentional and unintentional—taken by members of their own workforce next year.

In 2018, too many organizations will continue to manage insider risk reactively, and insiders will cause major cyber incidents such as misappropriating intellectual property (IP), or providing criminals with access to sensitive data and systems to get inside security controls and infiltrate an organization's perimeter. Employees will find workarounds for security policies or unwittingly fall victim to social engineering and phishing attacks. Criminals will target insiders in sophisticated sectors that are required and trusted to ensure information and data remain private, such as professional services, healthcare, financial services, automotive, entertainment, and technology. Bad leavers, many of whom see work products as their own to take, will intentionally misuse access to an organization's network or data.

However, only a fraction of these incidents will be publicly reported, and much of the resulting theft will be difficult to detect—given that many of the most valuable corporate assets today are in the form of IP,[34] trade secrets, research and development, or business strategies—that can be copied without being physically stolen. The dark web, encryption, and virtual currencies will continue to facilitate concealed transactions, communications, and storage of stolen data.

While the full extent of these attacks, and the true cybersecurity cost that insider threats pose, will go underreported, in the proportion of attacks that do become public we will start to see more companies being held legally liable for their poor handling of incidents caused by insiders, as in the landmark 2017 case brought against Morrisons Supermarkets in the High Court in the UK.[35]

In 2018, too many organizations will continue to manage insider risk reactively, and insiders will cause major cyber incidents. However, only a fraction of these incidents will be publicly reported.



Bottom Line:

Companies cannot eliminate the cyber risks caused by even well-intentioned employees, and while it is difficult to measure the full impact of insider risk, they can no longer afford to deprioritize this risk over those they face from external factors. Organizations will need to attend to this vulnerability, and implement effective insider risk programs. If ignored, they could be held liable in 2018 for failing to protect staff and consumers if an incident occurs.

??%

The full extent and the true cybersecurity costs of insider attacks will go underreported

Contacts

Jason J. Hogg
CEO, Aon Cyber Solutions
E: jason.j.hogg@aon.com

Edward Stroz
Co-President
Stroz Friedberg, an Aon company
E: estroz@strozfriedberg.com
T: +1 212 981 6541

Eric Friedberg
Co-President
Stroz Friedberg, an Aon company
E: efriedberg@strozfriedberg.com
T +1 212.981.6536

James M. Aquilina
President, Aon Cyber
Stroz Friedberg, an Aon company
E: jaquilina@strozfriedberg.com
T: +1 310 623 3301

United States

Rocco Grillo
Executive Managing Director
Stroz Friedberg, an Aon company
E: rgrillo@strozfriedberg.com
T: +1 212 981 2674

Kevin Kalinich
Global Practice Leader,
Cyber/Network Risk
Aon Professional Risk Solutions
E: Kevin.Kalinich@aon.com
T: +1 312 381 4203

CJ Dietzman
Vice President, Security Advisory
Practice Leader
Stroz Friedberg, an Aon company
E: cdietzman@strozfriedberg.com
T:+1 347.283.4861

Christian E. Hoffman
Aon Risk Solutions, Financial Services
Group, Professional Risk Solutions,
National Practice Leader
E: christian.hoffman@aon.com
T: +1 484 343 3740

Jibran Ilyas
Managing Director, Incident Response
Stroz Friedberg, an Aon company
E: jilyas@strozfriedberg.com
T:+1 312.216.8107

Stephanie Snyder
National Sales Leader, Cyber Insurance
Aon Professional Risk Solutions
T: +1 312 402 6038

United Kingdom

Justin Clarke-Salt
Co-Founder, Gotham Digital Science,
A Stroz Friedberg Company
E: justin@gdssecurity.com
T: +44 330 660 0720

Alex Carte
Managing Director,
Engagement Management
Stroz Friedberg, an Aon company
E: acarte@strozfriedberg.co.uk
T: +44 20.7061.2302

References

1. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX
2. https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html?utm_term=.7eba7c991ffd
3. https://investor.equifax.com/news-and-events/news/2017/09-26-2017-140531280
4. https://www.programbusiness.com/News/Shipping-Giant-Maersk-Could-Lose-Nearly-450M-Due-to-Recent-Cyber-Attack
5. https://www.ft.com/content/c8e634fa-2a31-11e7-9ec8-168383da43b7
6. http://riskandinsurance.com/ponemon-go/
7. Securities and Exchange Commission, Cybersecurity Disclosure Guidance, October 13, 2011.
8. The Washington Post, Equifax faces hundreds of class-action lawsuits and an SEC subpoena over the way it handled its data breach, November 9, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach
9. http://riskandinsurance.com/ponemon-go/
10. Infosecurity Magazine, Pharma Giant Merck Sees Petya Profit Hit for Rest of 2017, https://www.infosecurity-magazine.com/news/pharma-giant-merck-petya-profits/
11. Ponemon Institute, 2017 Global Cyber Risk Transfer Comparison Report, April 2017. http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp
12. http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp
13. Wired, Hackers Gain Direct Access to US Power Grid Controls, September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
14. Techcrunch, Global cybersecurity spending to grow 7% to $86.4BN in 2017, says Gartner, August 16, 2017 https://techcrunch.com/2017/08/16/global-cybersecurity-sending-to-grow-7-to-86-4bn-in-2017-says-gartner/
15. "Questions and Answers – Data Protection Reform Package," European Commission; http://europa.eu/rapid/press-release_MEMO-17-1441_en.html
16. https://www.bna.com/oral-argument-labmd-n73014453538/
17. "2017 Cybersecurity Policy Priorities," U.S. Chamber of Commerce; https://www.uschamber.com/2017cyberpriorities
18. "DigitalEurope urges MEPs to Bring ePrivacy Closer to Digital Reality," DigitalEurope; http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2549&language=en-US&PortalId=0&TabId=353
19. https://www.gartner.com/newsroom/id/3598917
20. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
21. www.ponemon.org/library/the-internet-of-things-iot-a-new-era-of-third-party-risk
22. Ponemon Institute, "2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)," June 2016, https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/.
23. CNBC Small Business Survey, April 2017. https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html
24. 2017 Data Breach Investigations Report (DBIR), Verizon, July 2017. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
25. https://www.facebook.com/whitehat
26. https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration/
27. https://bugcrowd.com/tesla
28. 2017 State of Bug Bounty Report, June 2017, Bugcrowd. https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/
29. ios11 Hacked by Security Researchers Day After Release, Zach Whittaker, Zero Day, November 2, 2017, ZDNet. http://www.zdnet.com/article/ios-11-hacked-by-security-researchers-day-after-release/?utm_source=hs_email&utm_medium=email&utm_content=2&_hsenc=p2ANqtz-88NIeQpAvpVDiDqbehjhWYOuq-
30. 2017 State of Bug Bounty Report, June 2017, Bugcrowd. https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/
31. https://go.druva.com/2017-Survey-Ransomware-Report-SEM.html?utm_medium=cpc&utm_source=paid-search&utm_campaign=US-inSyncRansomware-Ransomware&utm_content=&utm_adgroup=General&utm_term=ransomware&gclid=Cj0KCQjwsZHPBRCIARIsAC-VMPD9UVi_IC780BzYjlBAYk
32. https://s3.amazonaws.com/fuwt-prod-storage/content/FreelancingInAmericaReport-2017.pdf
33. http://www.aon.com/unitedkingdom/attachments/trp/2017-Trends-in-Global-Employee-Engagement.pdf
34. http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp
35. http://www.telegraph.co.uk/business/2017/12/01/victory-morrisons-workers-data-leak-compensation-claim/

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

About Stroz Friedberg

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. A global leader in the field of cybersecurity, with leading experts in digital forensics, incident response, proactive security, investigations, intellectual property, and eDiscovery, Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong. Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com/.

www.aon.com | www.strozfriedberg.com

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

Arnold & Porter

Tab 5: Speaker Biographies

Arnold & Porter

Marcus A. Asner

Partner

marcus.asner@arnoldporter.com
tel: +1 212.836.7222

250 West 55th Street
New York, NY 10019-9710
United States

Areas of Focus

- Anti-Corruption
- Litigation
- Privacy and Data Security
- Financial Services
- White Collar Defense

Education

- JD, University of Michigan Law School, 1992, *cum laude*
- MS, Mathematics, University of Michigan Rackham Graduate School, 1987
- AB, Physics, University of Chicago, 1985, *with honors*

Admissions

- New York
- US Court of Appeals for the Second Circuit
- US Court of Appeals for the Third Circuit
- US District Court for the Eastern District of Michigan
- US District Court for the Southern District of New York

Marcus Asner is a partner in the white collar criminal defense practice group. Among other areas, Marcus has significant expertise in the areas of data breaches, cyber crime, identity theft and credit card bust-out schemes.

Prior to joining Arnold & Porter, Marcus served as an Assistant United States Attorney for the Southern District of New York (2000-2009), where he was Chief of the Major Crimes and Computer Hacking/Intellectual Property unit (now known as Complex Frauds unit) for two years (2007 to 2009). Marcus was instrumental in coordinating computer crime investigations and prosecutions in the SDNY. He also served as the Identity Theft Coordinator and as Chair of the SDNY Identity Theft Working Group, coordinating identity theft prosecutions and investigations for the United States Attorney's Office.

Experience

Marcus has handled some of the most significant data breach/identity theft and cyber crime cases in the country. These include:

- *Large retail book company* in investigation into major data breach, including coordinating matter with law enforcement and leading to arrest of defendant.
- *Fortune 25 high technology company* with corporate espionage investigation involving trade secrets stolen by former employees, who then took stolen intellectual property to competitor. Successfully assisted company in coordinating with law enforcement, which led to conviction of employee and restitution to client.
- *Former in-house counsel for large internet company* in a high-profile, ongoing investigation related to decision not to disclose massive data breach involving approximately 500 million accounts.
- *Large media company* with investigation into ongoing “dedicated denial of service” (DDOS) cyber-attack of popular online gaming system.
- *Large media company* with investigation into pre-release theft of upcoming film.
- Successfully advised individual victim of hacking incident which occurred in connection with unrelated employment litigation.
- Served as expert witness on behalf of credit reporting agency in a civil case brought in federal court.
- *Internet gambling companies* on matters concerning US criminal law and enforcement.

- *Large US company* in connection with theft of employee benefits data.
- *United States v. David Copeland Reed (OSGold/OSOpps Ponzi scheme)*. Prosecuted international, Internet-based Ponzi scheme arising out of "OSGold," a company which held itself out as an online "bank" that could provide customers with Internet banking services purportedly backed by gold bullion reserves. Defendant arrested in February 2009 and charged with conspiracy to commit money laundering and wire fraud. Case pending.
- *The Philip Cummings Identity Theft Investigation.* Led investigation and prosecutions of fraud ring involved in stealing identities of approximately 30,000 known victims, resulting in estimated losses of over US$100 million. Investigation led to 21 convictions, with last defendant pleading guilty on the morning of trial. Engaged in lengthy evidentiary hearing addressed to sentencing. Successfully defended sentencing and convictions on appeal, leading to noted opinion bearing on myriad sentencing issues. *United States v. Abiodun*, 536 F.3d 162 (2d Cir. 2008).
- *The BetOnSports Identity Theft Investigation*. Led investigation and prosecutions of international identity theft ring engaged in stealing identity and credit information. Investigation led to arrest and conviction of six ring members, including insider who stole the identity information through work at the credit department of BetOnSports.com in Costa Rica.
- *The New York-Presbyterian Hospital Identity Theft Investigation*. Supervised a team of Assistant US Attorneys and agents in an investigation and prosecution of alleged theft and sale of approximately 49,000 patient records.
- *The Bank of Ethiopia Citibank Breach*. Led the investigation into a recent account takeover which led to the theft of approximately US$27 million from a Citibank account belonging to the National Bank of Ethiopia. (See Benjamin Weiser, "Nigerian Accused in Scheme to Swindle Citibank," *New York Times*, Feb. 20, 2009).

Professional and Community Activities

- Member, New York City Bar Association
- Advisory Council to the Presidential Task Force on Wildlife Trafficking (2013-16)
- Advisory Council, Wildlife Justice Commission

Government / Military Service

- Chief, Major Crimes and Computer Hacking/Intellectual Property Unit, US Attorney's Office, Southern District of New York
- Assistant US Attorney for the Southern District of New York

Arnold & Porter

Michael A. Mancusi

Partner

michael.mancusi@arnoldporter.com
tel: +1 202.942.5302

601 Massachusetts Ave, NW
Washington, DC 20001-3743

Areas of Focus

- Financial Services
- Privacy and Data Security

Education

- JD, University of Richmond School of Law, 1997
- MBA, University of Richmond Reynolds Graduate School of Business, 1997
- BS, University of Virginia, 1994

Admissions

- District of Columbia
- Maryland
- Virginia

Michael Mancusi represents domestic and foreign banks, credit unions, and other financial services clients in a wide range of state and federal regulatory, compliance, and enforcement matters. He also has substantial experience representing clients in government and corporate internal investigations, including entities subject to anti-money laundering requirements.

Mr. Mancusi counsels clients facing complex corporate governance and structural issues and represents clients before key state and federal bank regulatory agencies, including the Office of the Comptroller of the Currency, the Federal Reserve, the FDIC, the National Credit Union Administration, the Financial Crimes Enforcement Network, the Consumer Financial Protection Bureau, and the Office of Foreign Assets Control.

Mr. Mancusi counsels clients on compliance with privacy and data security requirements, including financial privacy under the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act, and the federal E-Sign Act. In addition, Mr. Mancusi advises clients regarding developing and implementing data breach response programs, including compliance with notification requirements at the federal and state levels.

Recognized by *Chambers USA* as "a key player in the enforcement arena," Mr. Mancusi served in the Enforcement Division of the Office of the Comptroller of the Currency, where he handled its banking law enforcement actions. He is currently Vice Chair of the ABA's Banking Law Committee, and served on the Executive Council of the Federal Bar Association's Banking Committee. In addition, Mr. Mancusi teaches a training program through the Institute for International Bankers on the US anti-money laundering and sanctions program issues that are most relevant to international banks.

Experience

Financial Services

- *Financial institution* in joint DOJ/CFPB fair lending investigation.
- *Major participants in the secondary mortgage market* on the effect of an FDIC receivership or conservatorship on mortgage servicing and the related obligations of the failed banks.
- *Federal branch of a foreign bank* in an enforcement proceeding under the Bank Secrecy Act brought by the Office of the Comptroller of the Currency and the Financial

Crimes Enforcement Network and in implementing the terms of a cease and desist order requiring a reduction in business operations in the United States.

- *Pro bono client* in successfully challenging the Department of Veterans Affairs to reinstate disability compensation and benefits for a low income veteran with 25 years of service.

Recognition

- *Chambers USA*
  Financial Services Regulation: Banking – Enforcement & Investigations (Nationwide) (2014-2018)
- *Washington, DC Super Lawyers*
  Banking, Consumer Law, Business/Corporate (2014-2018)
- *Best Lawyers*
  Banking and Finance Law (2016-2018)
- *The Legal 500 US*
  Financial Services: Regulatory (2015-2017)
- *The Legal 500 Latin America*
  Banking and Finance

Professional and Community Activities

- Former Chair, District of Columbia Bar, Financial Institution Committee
- Executive Council, Federal Bar Association, Banking Committee
- Vice Chair, American Bar Association, Banking Law Committee
- BSA/AML/OFAC Training Series, Institute for International Bankers

Arnold & Porter

Nancy L. Perkins

Counsel

nancy.perkins@arnoldporter.com
tel: +1 202.942.5065

601 Massachusetts Ave, NW
Washington, DC 20001-3743

Areas of Focus

- Privacy and Data Security
- National Security
- Legislative and Public Policy
- Financial Services
- Governments/Sovereigns

Education

- AB, Harvard College, 1979
- JD, Harvard Law School, 1987
- MPP, Harvard University, John F. Kennedy School of Government, 1987

Admissions

- District of Columbia
- Supreme Court of the United States
- US Court of Appeals for the District of Columbia Circuit
- US Court of Appeals for the Eleventh Circuit
- US Court of Appeals for the Federal Circuit
- US Court of Appeals for the Fifth Circuit
- US Court of Appeals for the Ninth Circuit
- US Court of Appeals for the Sixth Circuit

Nancy Perkins, counsel in the Washington, DC office, focuses her practice on litigation, regulatory compliance, and consulting on emerging policy issues, with a principal focus on data privacy and security. She regularly advises clients on compliance with a wide range of data protection requirements at the federal and state levels, including rules applicable to online communications and transactions as well as all types of uses and disclosures of medical, financial, and other sensitive personal information. She assists clients in structuring their activities, online service offerings and privacy policies to comply with applicable laws and best practices, taking into account technological and intellectual property issues associated with the expansion of electronic commerce and Internet activities. Among other laws, Ms. Perkins frequently provides counsel on the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act (as amended by the Fair and Accurate Credit Transactions Act), the federal E-Sign Act, the Children's Online Privacy Protection Act, and the Video Privacy Protection Act, - as well as state privacy, security, data breach notification, and electronic signature laws. She also has a deep background in international law and advises clients on the US-EU Safe Harbor relating to the EU Data Protection Directive, as well as broader issues arising under the rapidly developing framework for global legal protection of personal information.

Ms. Perkins served as a law clerk to Judge Eugene H. Nickerson of the US District Court for the Eastern District of New York from 1987 to 1988. She is a 1987 graduate of Harvard Law School, where she was an editor of the *Harvard Law Review* and the *Harvard International Law Journal*. She is a member of the American Law Institute and serves on the Executive Council of the American Society of International Law and the Steering Committee of the International Law Section of the District of Columbia Bar.

She also has a deep background in international law and advises clients on the US-EU Safe Harbor relating to the EU Data Protection Directive, as well as broader issues arising under the rapidly developing framework for global legal protection of personal information.

Ms. Perkins served as a law clerk to Judge Eugene H. Nickerson of the US District Court for the Eastern District of New York from 1987 to 1988. She is a 1987 graduate of Harvard Law School, where she was an editor of the *Harvard Law Review* and

- US District Court for the District of Columbia

the *Harvard International Law Journal*. She is a member of the American Law Institute and serves on the Executive Council of the American Society of International Law and the Steering Committee of the International Law Section of the District of Columbia Bar.

Professional and Community Activities

- Treasurer and Executive Council Member, American Society of International Law (ASIL)
- Editorial Advisory Committee Member, *International Legal Materials*, an ASIL publication
- Member, American Law Institute
- Leadership Committee Member, International Law Section of the DC Bar

STROZ FRIEDBERG
an Aon company

PROFILE

Edward M. Stroz

Co-President

New York, NY

E estroz@strozfriedberg.com

T +1 212.981.6541

F +1 212.981.6545

linkedin.com/in/linkedin.com/in/edstroz

Education

B.S., Fordham University

Ed Stroz is the founder and Co-President of Stroz Friedberg, an Aon company and global leader in investigations, intelligence and risk management. Ed oversees the firm's growth and client development, while ensuring the maintenance of its distinctive culture. He also provides hands on strategic consulting in investigations, intelligence and due diligence, plus cyber and physical security. Before starting the firm, Ed was a Special Agent with the FBI where he formed their computer crime squad in New York.

Trained as a Certified Public Accountant, Ed has extensive experience in investigations of white-collar crime including bank fraud and securities fraud, and has testified in court numerous times as an expert witness.

Ed is a trustee of Fordham University, his alma mater, and serves as an advisor to the Center on Law and Information Policy (CLIP) at Fordham Law School. Ed sits on the Board of Directors of the Crime Commission of New York City, an independent non-profit organization focused on criminal justice and public safety policies and practices, and is a member of the Association of Former Intelligence Officers (AFIO). He served on the New York State Courts System E-Discovery Working Group, established to provide ongoing support and expertise to the New York State Judiciary in the area of e-discovery.

As a member of the National Association of Corporate Directors (NACD), in 2017 he earned the CERT Certificate in Cybersecurity Oversight from Carnegie Mellon University.

Arnold & Porter

Kevin M. Toomey

Associate

kevin.toomey@arnoldporter.com
tel: +1 202.942.5874

601 Massachusetts Ave, NW
Washington, DC 20001-3743

Areas of Focus

- Financial Services
- Privacy and Data Security
- Corporate and Finance

Education

- JD, Syracuse University College of Law, 2012
- BA, Colgate University, 2007

Admissions

- District of Columbia
- Maryland

Kevin Toomey represents banks and nonbank financial services companies, along with their boards of directors, executives, and senior management, in a wide range of enforcement, regulatory, compliance, and governance matters before the federal and state banking agencies, Department of Justice, CFPB, FinCEN, and OFAC. Mr. Toomey regularly represents clients in investigative proceedings, including navigating internal and government investigations, and advises clients on issues relating to the Bank Secrecy Act and anti-money laundering requirements, consumer protection, the Dodd-Frank Wall Street Reform and Consumer Protection Act, and state and federal banking laws and regulations.

Mr. Toomey also has significant experience counseling financial institutions on an array of corporate, securities, and transactional matters, including mergers and acquisitions, public and private securities offerings, and corporate reorganizations.

While attending law school, Mr. Toomey worked in the Enforcement Section of the FDIC, the Executive Office for US Attorneys at DOJ, and the US Attorney's Office for the District of Columbia.

Experience

Enforcement and Investigations

- *National bank* in an investigation under the Bank Secrecy Act brought by the Office of the Comptroller of the Currency, the Financial Crimes Enforcement Network, and the Department of Justice.
- *Large nonbank financial institution*, before the DOJ, SEC and FDIC, in an investigation of alleged violations of securities laws.
- *Nonbank financial institutions* in internal investigations relating to BSA/AML requirements.
- *Board of directors* on corporate governance matters and enforcement proceeding brought by the New York Department of Financial Services.
- *Outside directors* of a state-member bank's board in enforcement proceeding brought by the FDIC relating to BSA/AML matters.

Regulatory

- *Numerous financial institutions* with respect to banking agency and CFPB examination issues.
- *Online lender* on permissibility and structure of securitized loans.
- *Numerous financial institutions* with development of policies and procedures relating to consumer protection, UDAAP, Regulation O, Regulation W, and BSA/AML.

Corporate

- *Numerous financial institutions* in connection with a variety of mergers and acquisitions, including public company mergers.
- *Financial institutions* in registering public and offerings of debt and equity securities and private placements of securities.
- *Onex Corporation* in the sale of USI Insurance Services to an affiliate of KKR & Co. L.P. and Caisse de dépôt et placement du Québec for an enterprise value of $4.3 billion.

Recognition

- *Washington, DC Super Lawyers*
  "Rising Star" – Banking (2017-2018)

Professional and Community Activities

- Member, American Bar Association, Banking Law Committee
- Member, American Bar Association, Consumer Financial Services Committee
- Member, District of Columbia Bar, Financial Institutions Committee
- Instructor, BSA/AML/OFAC Training Series, Institute for International Bankers

Government / Military Service

- Enforcement Section, Federal Deposit Insurance Corporation

Notes

Notes

Notes

Notes

BRUSSELS
1, Rue du Marquis -
Markiesstraat, 1
Brussels
BELGIUM

CHICAGO
70 West Madison Street
Chicago, IL 60602-4231

DENVER
Suite 4400
370 Seventeenth Street
Denver, CO 80202-1370

FRANKFURT
Bockenheimer Landstrasse 25
60325 Frankfurt
GERMANY

HOUSTON
Suite 1600
700 Louisiana Street
Houston, TX 77002-2755

LONDON
Tower 42
25 Old Broad Street
EC2N 1HQ
UNITED KINGDOM

LOS ANGELES
44th Floor
777 South Figueroa Street
Los Angeles, CA 90017-5844

NEW YORK
250 West 55th Street
New York, NY 10019-9710

SAN FRANCISCO
10th Floor
Three Embarcadero Center
San Francisco, CA 94111-4024

SHANGHAI
Suites 3808-3811, CITIC Square
Shanghai 200041
People's Republic of China

SILICON VALLEY
3000 El Camino Real
Five Palo Alto Square, Suite 500
Palo Alto, CA 94306-3807

WASHINGTON, DC
601 Massachusetts Ave, NW
Washington, DC 20001

WEST PALM BEACH
Phillips Point, East Tower
Suite 1000
West Palm Beach, FL
33401-6152