Morgan Lewis

Morgan Lewis and Alvarez & Marsal present

CYBERSECURITY:

LEGAL, REGULATORY, AND PRACTICAL CHALLENGES FACING THE INSURANCE INDUSTRY

TUESDAY, MAY 19, 2015

Panelists:

- **Hon. Katharine Wade**
  Connecticut Insurance Commissioner
- **Matthew Fitzsimmons**
  State of Connecticut Assistant Attorney General
- **Art Ehuan**
  Alvarez & Marsal Global Forensic & Dispute Services
  Cyber Practice
- **Scott Harrison**
  Alvarez & Marsal Insurance Risk & Advisory Services
- **Mark Krotoski**
  Privacy and Cybersecurity Partner, Morgan Lewis
- **Daniel Savrin**
  Privacy and Cybersecurity Partner, Morgan Lewis

Cybersecurity: Legal, Regulatory, and Practical Challenges Facing the Insurance Industry

Reference Materials

TAB 1

CYBER RISK TO THE INSURANCE INDUSTRY

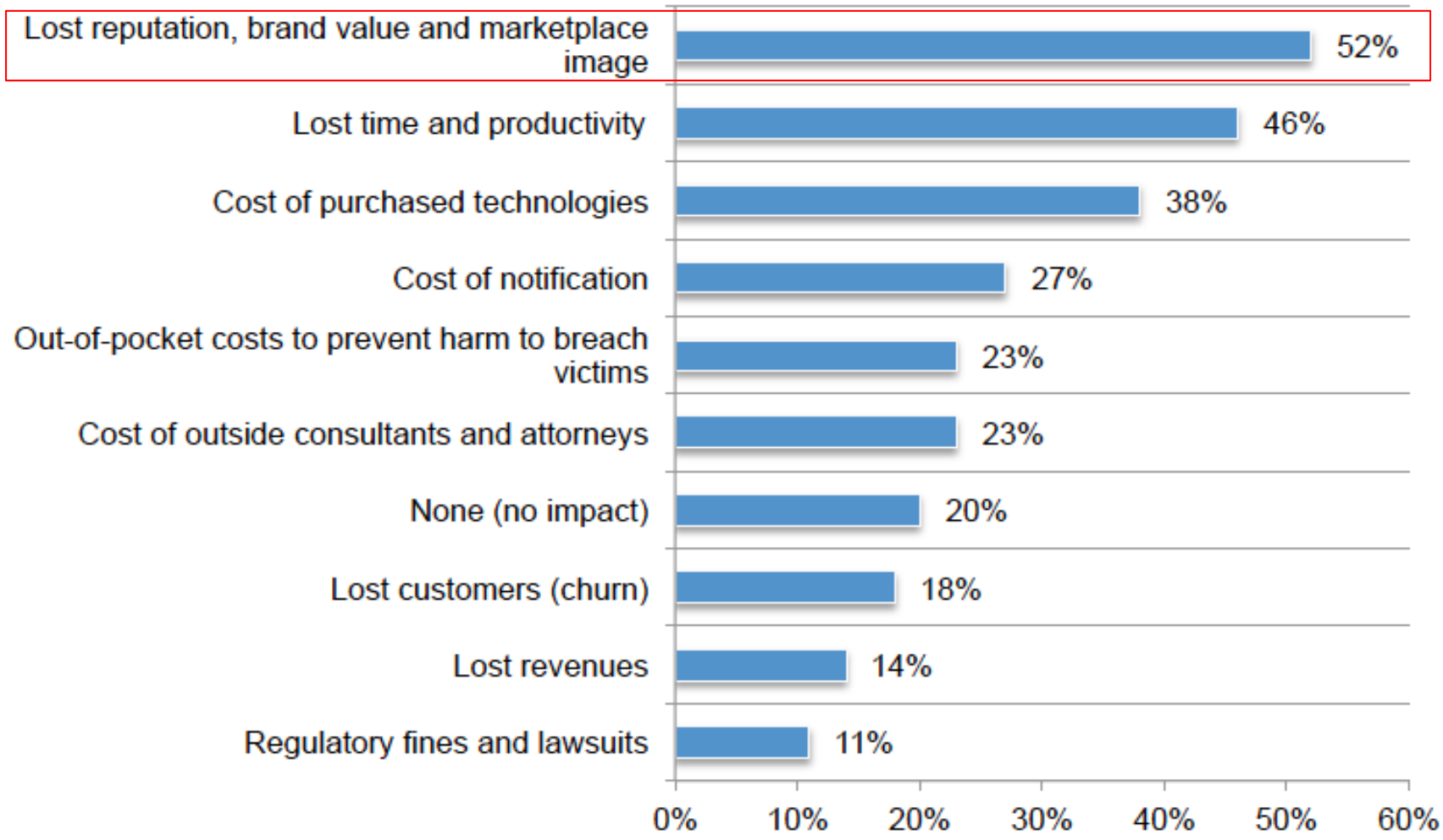
ALVAREZ & MARSAL

Protection of corporate assets (data/information) is the responsibility of all employees. The Board and C-Level have a critical governance responsibility.

Protection of information/data in the cyber age is a responsibility for the Board, Management and Staff.

CYBER THREAT RISK TO INCREASE

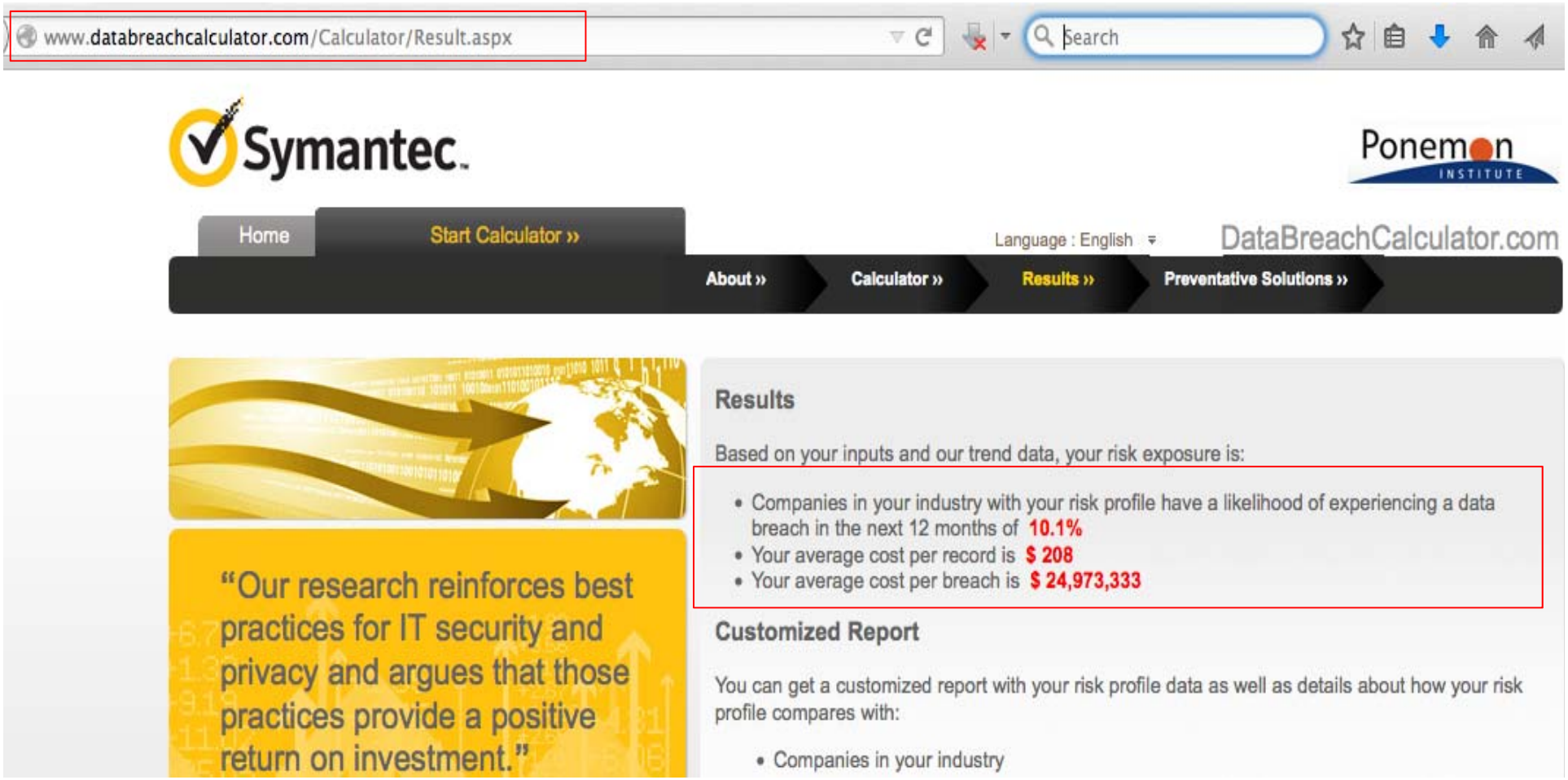
The cyber threat landscape continues to increase and impact corporations' market brand, financials, etc.



Ponemon Institute, 2014 A Year of Mega Breaches

FINANCIAL SERVICES INDUSTRY TARGETING

Estimated costs of a breach for a medium sized insurance company.



1

INSURANCE SERVICES INDUSTRY TARGETING

Why is the insurance services industry targeted?

- Executive Communications (Email, Calendar, Voicemail, etc.)
- Intellectual Property (Insurance Policy Modeling, etc.)
- Employee Human Resource (HR) Data (SSN, DOB, etc.)
- Customer, Partner, Vendor, & Consumer Information
- Patient Information/Data

Here's What Chinese Hackers Actually Stole From U.S. Companies

A run-down of exactly what "trade secrets" Chinese hackers are accused of stealing from U.S. metals and solar power companies, and a labor union

Five Chinese military hackers employed by the Chinese government were accused yesterday of infiltrating American companies and stealing trade secrets. By charging the men with economic espionage and identity theft, among other crimes, the Department of Justice has set the stage for a tense standoff with the Chinese government.

CYBER THREAT ACTORS

Cyber threat actors include Hackers, Organized Crime Groups, and Nation-States

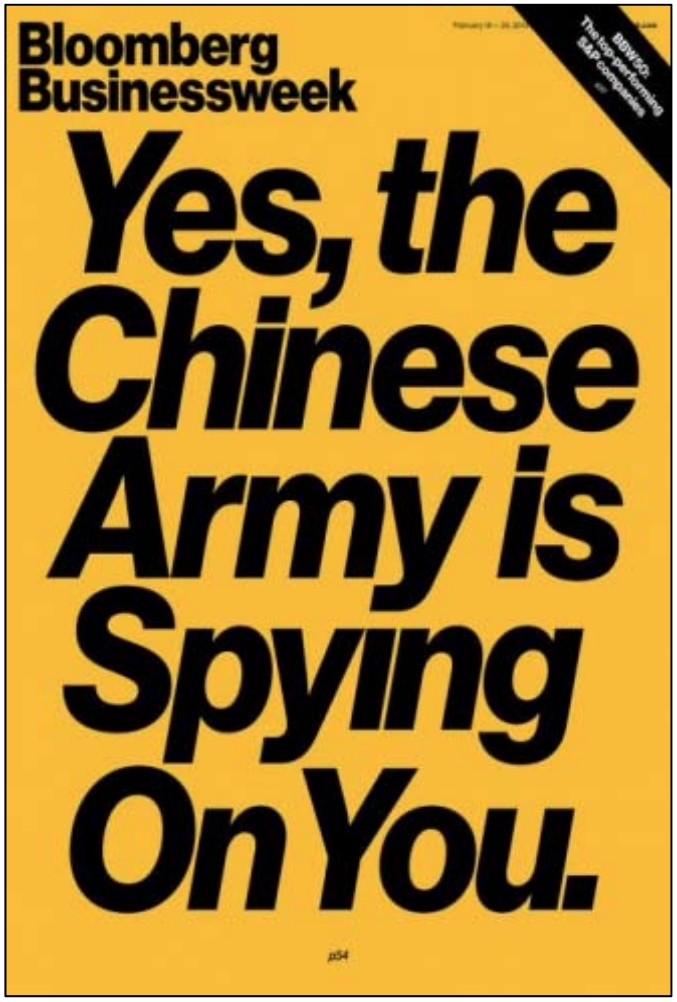
Hackers

Organized Crime

MOSCOW – When it comes to finding original ways of virtually stealing real money, Russian criminals are in a class of their own. With an estimated annual turnover of more than $2 billion a year, the Russian cybercrime industry is the source of at least a third of all viruses, Trojans and other malicious software, or malware, sent around the world.

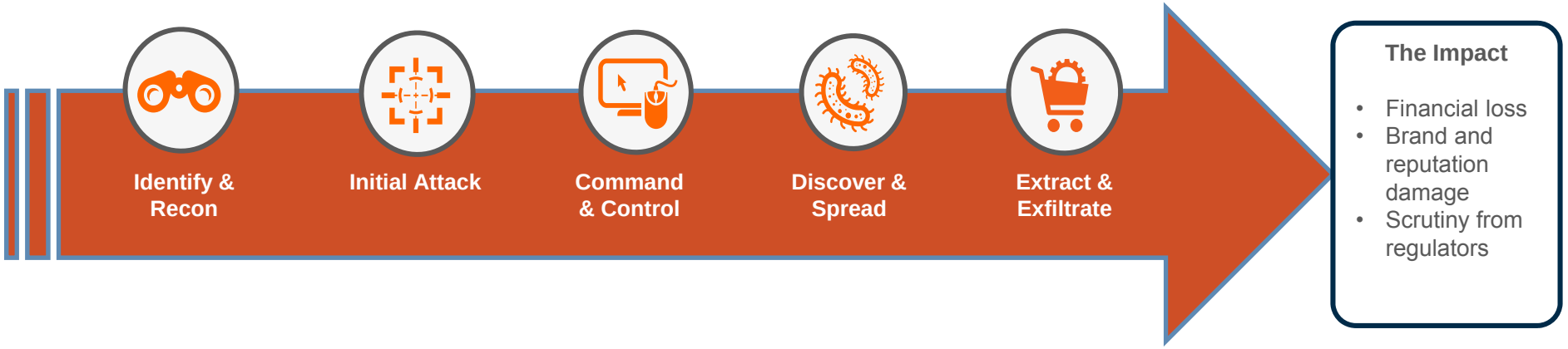
"In terms of sophisticated types of malware, Russia leads the way," according to Kyle Wilhoit, an American cyber-security expert.

Nation-State



CYBER THREAT ACTORS

Cyber threats are complex and most companies find it difficult to identify breaches



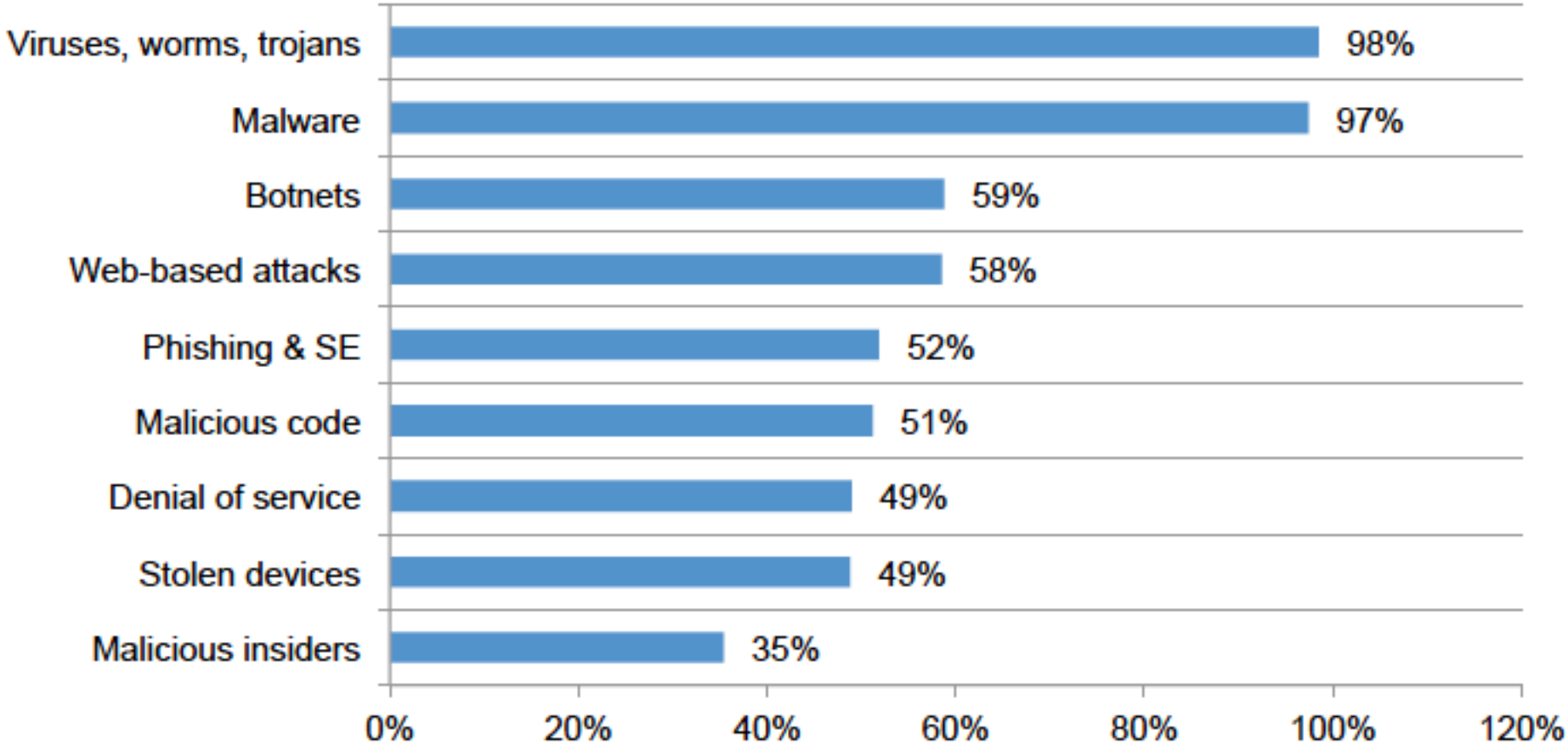
- **Cyber Attacks are multi-stage, using multiple threat vectors**
- **Organizations often don't identify that they have been compromised for months after the event[1]**
  - 229 days on average before detection of compromise
- **Over two-thirds of organizations find out from a 3rd party when they have been compromised[2]**

1 – IDC Worldwide Security and Vulnerability Management 2014–2018 Forecast
2 – 2014 mTrends Threat Report

HOW ARE CORPORATIONS BEING COMPROMISED

Cyber threat actors compromise corporations using various methodologies and tactics.

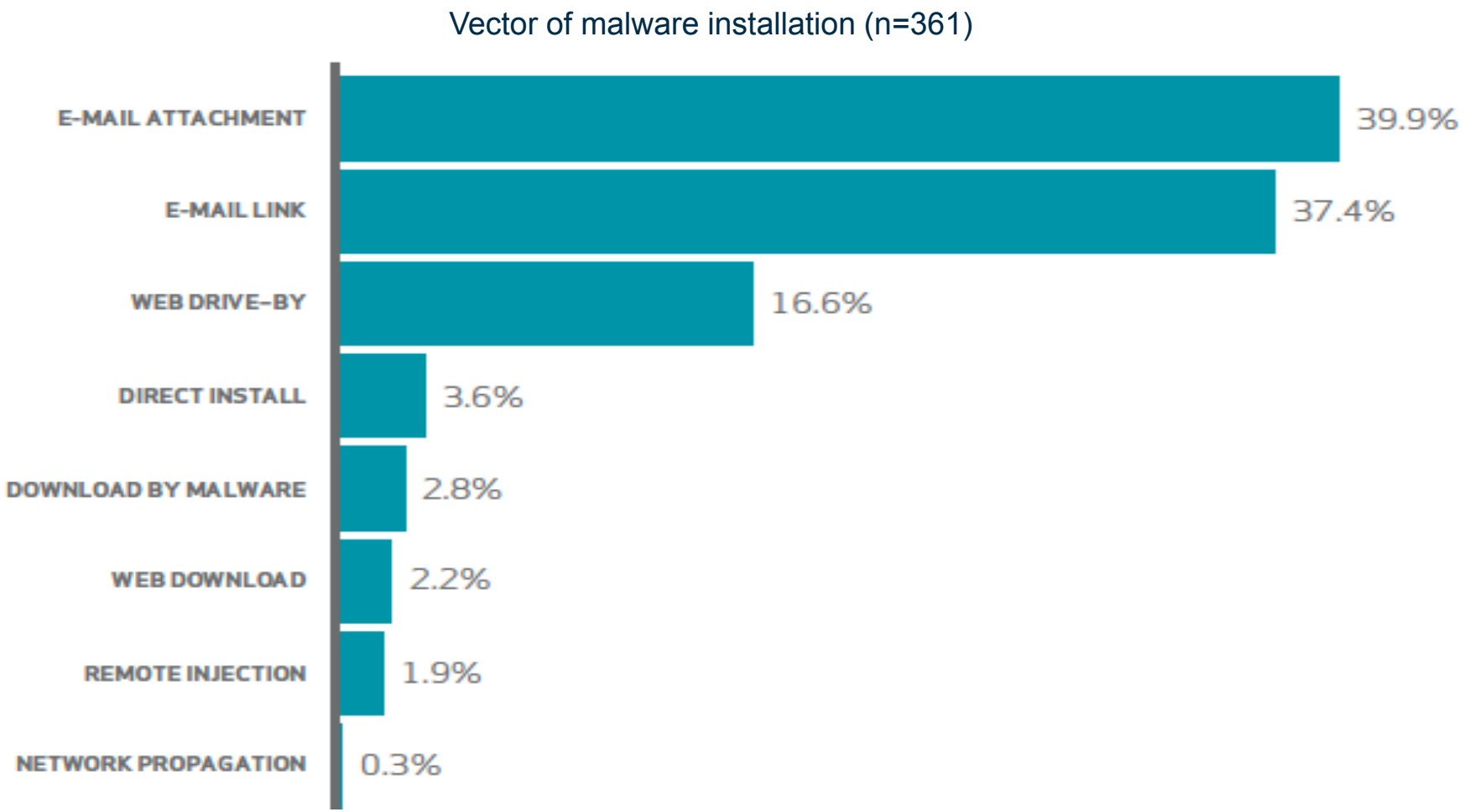
Types of cyber attacks experienced by 257 benchmarked companies (consolidated view, n=257 separate companies)



Source: Ponemon Institute, 2014 Global Report on Cost of Cyber Crime

HOW ARE CORPORATIONS BEING COMPROMISED

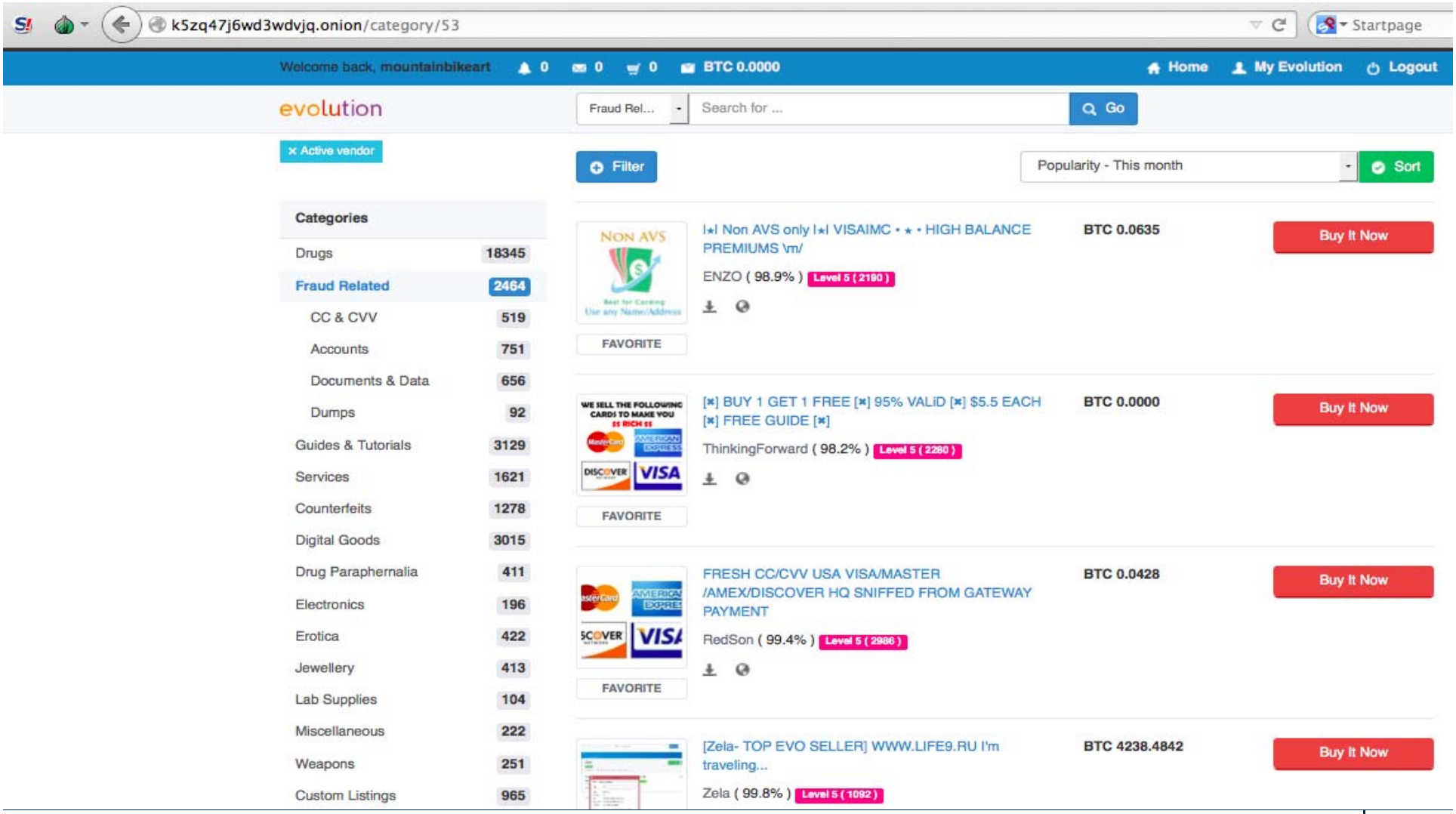
Cyber threat actors compromise corporations using various methodologies and tactics.



Source: Verizon, 2015 Data Breach Investigations Report

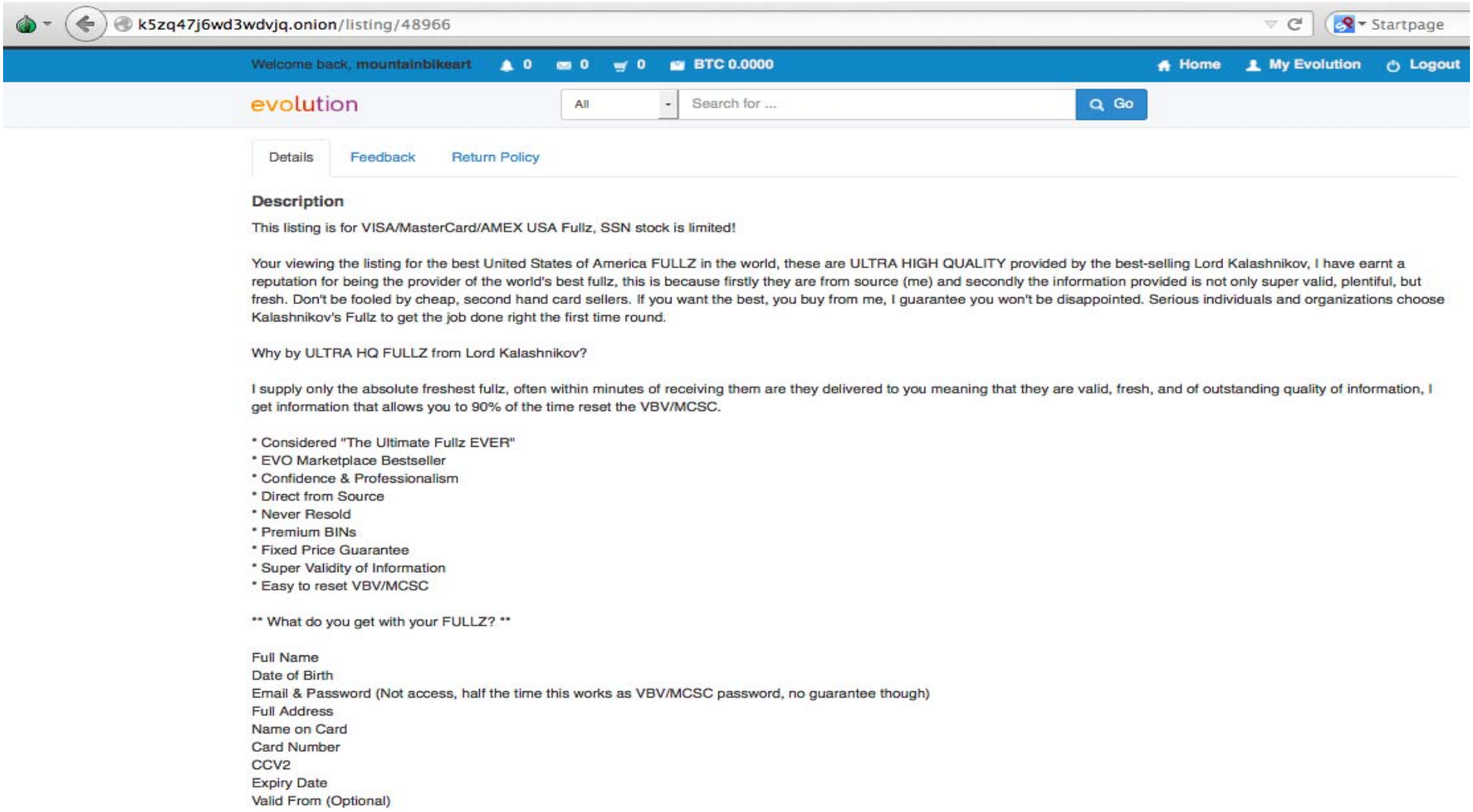
WHERE DOES STOLEN INFORMATION GO?

Many threat actors sell stolen information online using untraceable currencies in hard to track communities.



WHERE DOES STOLEN INFORMATION GO?

Many threat actors sell stolen information online using untraceable currencies in hard to track communities.



WHAT HAPPENED TO THE SECURITY PERIMETER?

The permeable perimeter keeps increasing in scope.

Cloud Services

Corporate Perimeter

Mobile Devices

Remote Workers

Advanced Malware

COST EFFECTIVE CYBER PROTECTION

NORTH AMERICA EUROPE MIDDLE EAST LATIN AMERICA ASIA

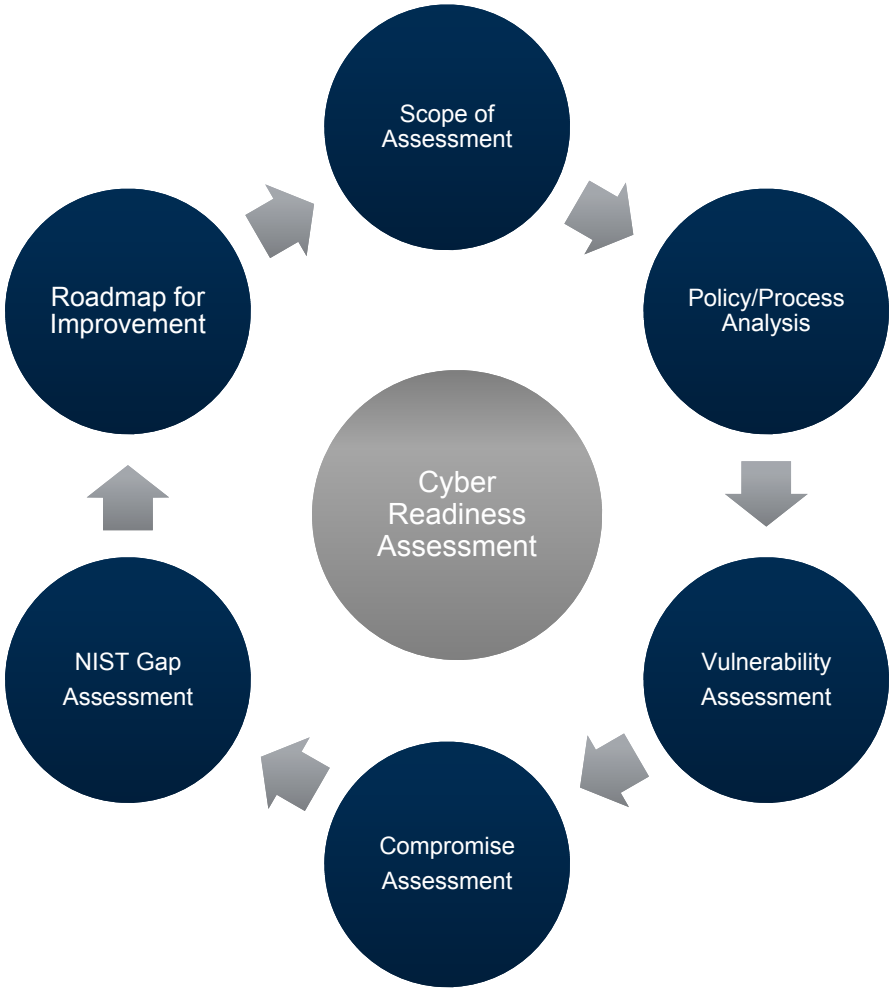
EFFECTIVE CYBER SECURITY NEED NOT BE EXPENSIVE

The protection of a corporation's information/assets can be managed in a cost effective manner if the basic requirements are met.

Cost effective cyber security starts with the basics, which most corporations are not doing…

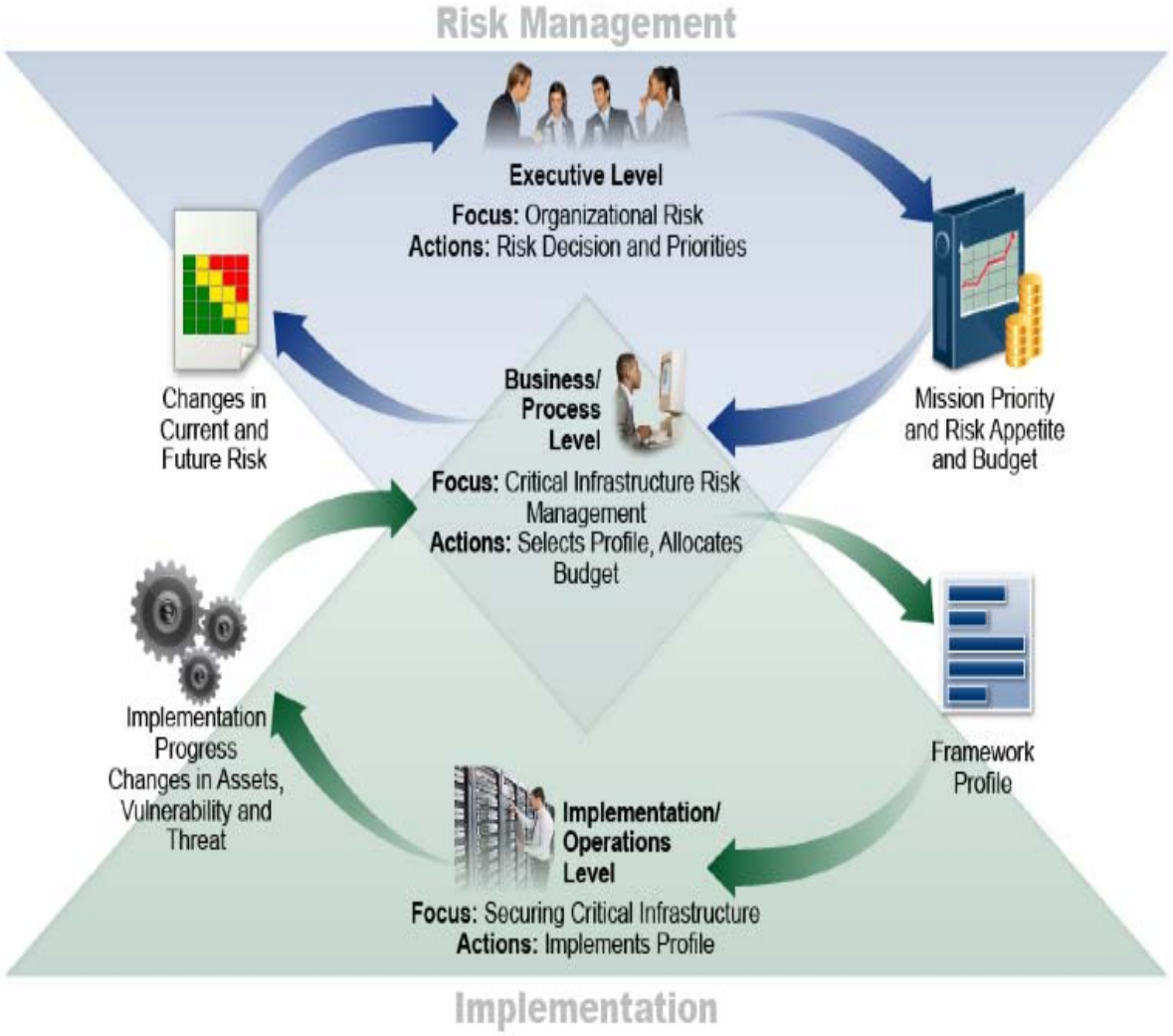
Cyber Readiness Assessment to Identify Risk

- A cyber readiness assessment is utilized to identify the existing security profile of a company.
- The assessment will identify vulnerabilities, threats, and risks to information.
- The assessment will determine the effectiveness of:
  - Cyber Security Framework/Strategy
    - Cyber Security Policies
    - Network Topology
    - Incident Response
    - Acquisition Due Diligence
    - Data Classification
    - Remote Worker
    - Vulnerability Management
    - Log Analysis
- Used to calibrate your spend and effectiveness (KPI's) of budget.



Implement the NIST CyberSecurity Framework

- The NIST CyberSecurity Framework consists of a set of standards and best practices for organizations to manage cyber risk.
- The NIST Framework assists an organization in aligning cyber security activities with business requirements, risk tolerance and available resources.
- The NIST Framework can utilize the ISO or NIST standards for its implementation.



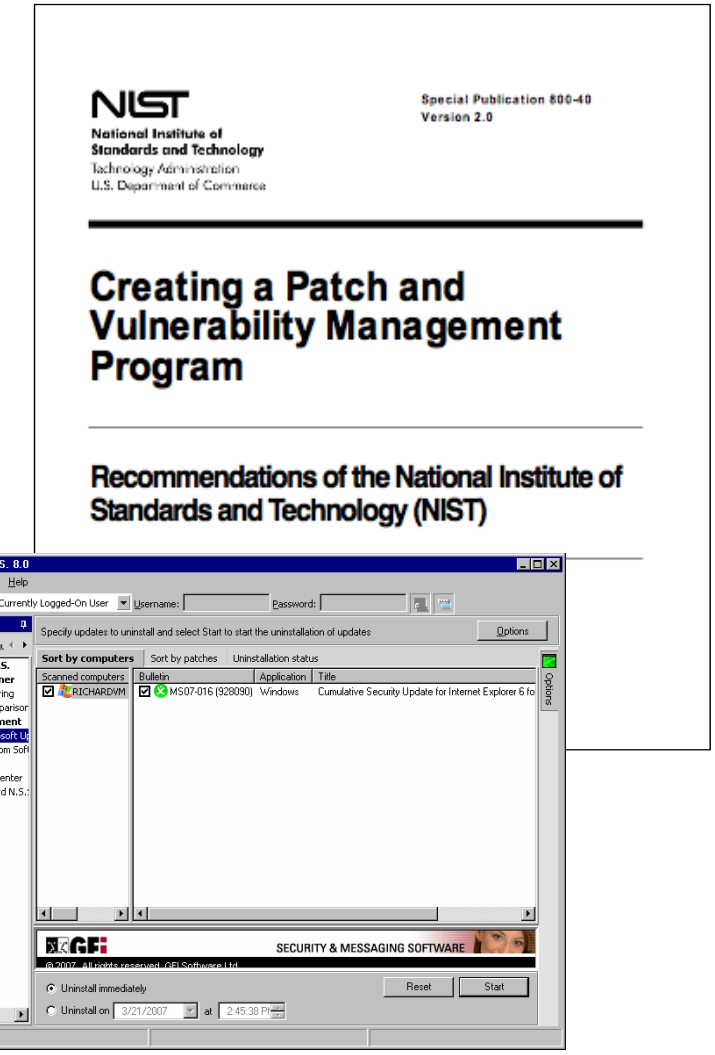
Cyber Threat Identification Management

- A fundamental component in today's business environment, supported by a comprehensive methodology.
- Identifying cyber threats to your corporate information is crucial.
- A threat intelligence program is designed to provide a proactive approach to information protection (similar to a radar screen).
- Threat intelligence provides information on the malicious actors that are interested in the company.
- The threat intelligence is used to secure systems and protect critical data.

This should not be your company's cyber threat notification process…….

Vulnerability Management Program

- An effective Vulnerability Management Program is one of the most underappreciated facets of information security.
- Proper patch management can provide a significant reduction in a corporation's risk profile by eliminating known vulnerabilities to the organization.
- A process-driven configuration management should be established and adhered to in strict fashion to reduce risk.



Secure the Supply Chain & Acquisitions

- Suppliers and vendors that have access to the corporate network must be continuously vetted to ensure they comply with cyber security standards and to ensure they cannot access your data without authorization.
- Require thorough contractual language that requires suppliers/vendors to protect your data.
- Audit or access suppliers/vendors to verify that data is being protected.
- Ensure that cyber risk is minimized before adding new company to portfolio.

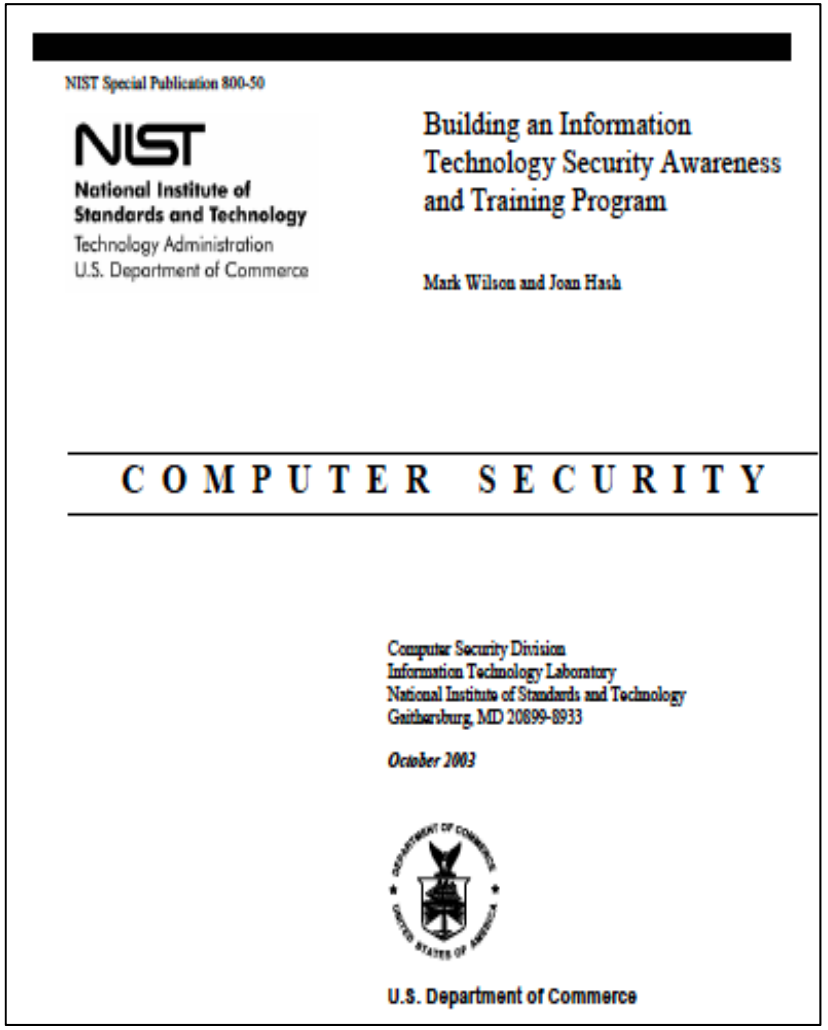
Target Nears Settlement With MasterCard Over Data Breach

Settlement of $20 million would reimburse banks for costs; talks with Visa continue

Target is close to reaching a $20 million settlement with MasterCard to reimburse financial institutions for costs they incurred from the retailer's massive data breach in 2013. *PHOTO: GETTY IMAGES*

Security Awareness Program

- The weakest link in any cyber security program is the human element.
- Executives and staff must all be cyber-aware in the dynamic business environment.
- Cyber security should enable the business and take into account the corporate culture.


NIST Special Publication 800-50

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Building an Information Technology Security Awareness and Training Program

Mark Wilson and Joan Hash

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

October 2003

U.S. Department of Commerce

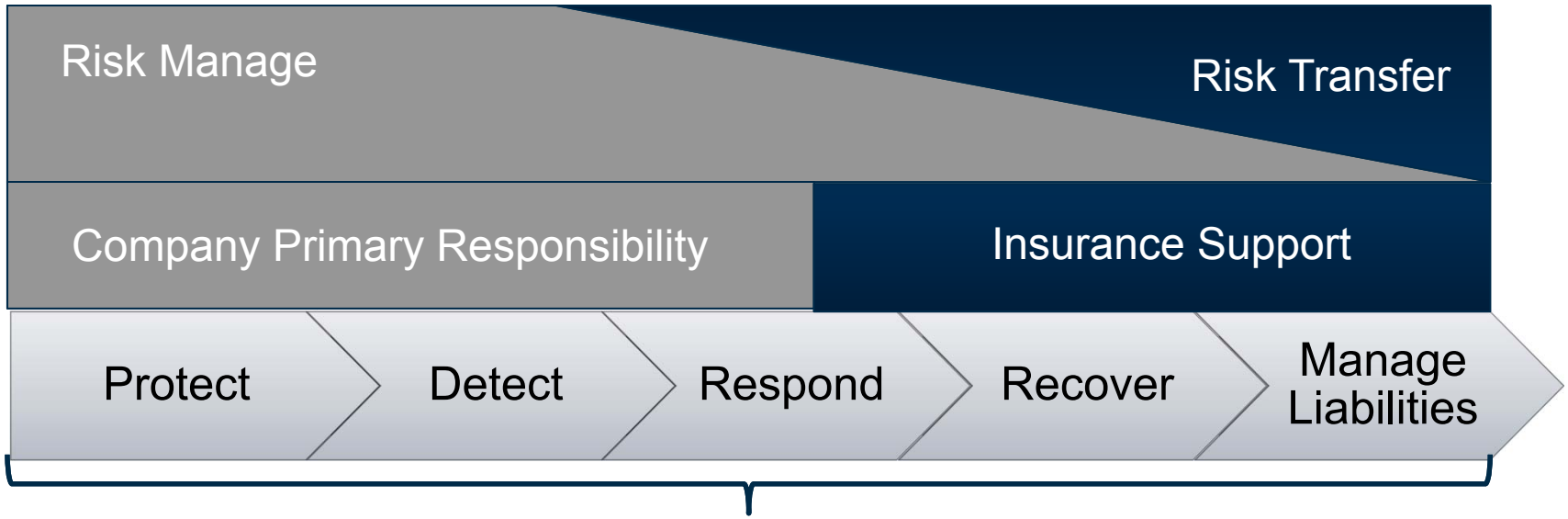
SECURING THE CORPORATION

7 Questions for the Board and Executives

1	Who is ultimately responsible for cyber risk in the corporation?
2	What and where are the most critical assets that could be attacked? What is their value?
3	Has a cyber attack simulation been performed in the corporation to test the incident response plan?
4	Has a cyber readiness assessment been conducted to identify gaps in information security defenses?
5	How many times has the corporation suffered a cyber breach in the last year? How do you know? Is there monitoring and reporting of cyber risk incidents (24/7?)
6	Is cyber risk covered in contracts with third parties vendors, etc.? How is compliance verified?
7	Is the Board aware of the risk exposure of the corporation?

WHERE DOES CYBER INSURANCE FIT IN ENTERPRISE CYBER RISK MANAGEMENT STRATEGY?

A trade-off exists between the amount a firm should invest in protecting against security breaches and the amount it should spend on cyber risk insurance.



Cyber Risk Management Lifecycle

An enterprise primarily focuses its traditional cyber security spend to develop suitable risk management measures to put in place the right protection, detection, and basic response measure. Cyber insurance is used to provide response, recovery, and liability management support, which forms the residual risk.

FEDERAL/STATE INSURANCE SERVICES FIRM CYBER REGULATION

Insurance services firms are increasingly subject to Federal and State regulatory requirements.

Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Commissioner Luis A. Aguilar

"Cyber Risks and the Boardroom" Conference
New York Stock Exchange
New York, NY

June 10, 2014

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk[25] — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.[26]

NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Benjamin M. Lawsky
Superintendent

March 26, 2015

Dear Chief Executive Officer, General Counsel, and Chief Information Officer:

In an effort to promote greater cyber security across the financial services industry, the New York State Department of Financial Services (the "Department") has expanded its information technology ("IT") examination procedures to focus more attention on cyber security. The Department encourages all institutions to view cyber security as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology. To that end, the Department intends to incorporate new questions and topics into the existing IT examination framework.

In particular, IT/cyber security examinations will now include, but not be limited to, the following topics:

- Corporate governance, including organization and reporting structure for cyber security-related issues;
- Management of cyber security issues, including the interaction between information security and core business functions, written information security policies and procedures, and the periodic reevaluation of such policies and procedures in light of changing risks;
- Resources devoted to information security and overall risk management;
- The risks posed by shared infrastructure;
- Protections against intrusion, including multi-factor or adaptive authentication and server and database configurations;
- Information security testing and monitoring, including penetration testing;
- Incident detection and response processes, including monitoring;
- Training of information security professionals as well as all other personnel;
- Management of third-party service providers;
- Integration of information security into business continuity and disaster recovery policies and procedures; and
- Cyber security insurance coverage and other third-party protections.

A&M TEAM BIO

Art Ehuan

Managing Director

aehuan@alvarezandmarsal.com
571-331-7763

- Art Ehuan has extensive industry and law enforcement experience in the field of cyber and risk advisory services. He has a specialization in strategic risk advisory services, including incident response, vulnerability assessments and cyber program development for corporate and government agencies. Mr. Ehuan also serves as a lecturer on cyber crime/terrorism for the U.S. State Department, Diplomatic Security Service, Anti-Terrorism Assistance Program. In this capacity he has lectured on cyber threat to nation-state critical infrastructure to include Advanced Persistent Threat (ATP), Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS).
- Prior to joining A&M, Mr. Ehuan was Managing Director at Forward Discovery, a boutique cyber security firm. Mr. Ehuan also served as Assistant VP and Director of the Corporate Information Security Department for USAA, a Fortune 200 financial/insurance services company. He was responsible for worldwide enterprise and strategic/risk guidance on the protection of USAA information from external/internal threats.
- Among Mr. Ehuan's high-profile corporate positions was Deputy Chief Information Security Officer for the Northrop Grumman Corporation. He was responsible for protecting data from internal and external cyber threats, developing and managing security operations and implementing a corporate digital investigative unit. Mr. Ehuan was also a Federal Information Security Team Manager for BearingPoint (formerly KPMG Consulting), where he established information security initiatives and solutions for government and corporate organizations, as well as developing BearingPoint's corporate incident response and digital forensic services. In addition, Mr. Ehuan served as the Program Manager for Cisco Systems Information Security, where he was responsible for securing corporate networks, managing risk assessments, protecting source code and developing Cisco's worldwide digital forensic capability.
- As a law enforcement officer, Mr. Ehuan has worldwide experience working on cases involving computer crimes. His extensive background conducting and managing computer intrusion and forensic investigations with the Federal Bureau of Investigation (FBI) led to his assignment as a Supervisory Special Agent assigned to the Computer Crimes Investigations Program at FBI Headquarters in Washington, D.C. In addition, he served as a Computer Analysis Response Team Certified Examiner, where he developed and conducted training for law enforcement globally. Mr. Ehuan served as a computer crime Special Agent for the Air Force Office of Special Investigations (AFOSI), where he investigated cyber crime against the network systems of the U.S. Department of Defense. Mr. Ehuan has also testified in Federal, State and Military courts in cases involving digital forensics.
- Mr. Ehuan has received industry credentials including: EnCase® Certified Examiner (EnCE®), Certified Information Systems Security Professional (CISSP) He also maintains the Information Assessment Methodology (IAM) credentials with the National Security Agency (NSA).
- Mr. Ehuan was previously an Adjunct Professor/Lecturer at George Washington University, Georgetown University and Duke University where he taught courses on cyber crime, incident response, digital investigations and computer forensics. He is a contributing author of Techno-Security's Guide to E-Discovery and Digital Forensics from Elsevier Publishing.

Scott Harrison

Managing Director

Washington DC

Phone: (202-)360-0586
E-mail Address:
srharrison@alvarezandmarsal.com

- Scott Harrison is a Managing Director with Alvarez & Marsal Insurance and Risk Advisory Services. He serves as a trusted advisor to insurance companies and their strategic partners seeking regulatory, compliance and corporate governance solutions.
- For nearly 30 years, Scott has helped companies improve operations, manage their businesses and mitigate risk in a rapidly changing regulatory environment. He provides counsel on business and public affairs strategies, issue advocacy, corporate governance, the development of regulatory and legislative policy and market regulation/compliance. National insurance companies, banks and trade associations are among Scott's key clients.
- Scott serves as Executive Director for the Affordable Life Insurance Alliance (ALIA), an independent insurance trade association with the mission to fundamentally reform state laws and regulations governing life insurance reserves.
- He has also represented a group of life insurance companies on complex reserve valuation issues before states and the National Association of Insurance Commissioners. This initiative resulted in the ongoing effort to replace the current valuation system with a principles-based approach.
- Scott has worked as Deputy Superintendent of the New York State Insurance Department and as Deputy Commissioner of the Delaware Insurance Department.
- Additionally, Scott served as interim Chief Compliance Officer for a Fortune 500 life and health insurance company and as partner at KPMG LLP where he managed the firm's national insurance regulatory practice. He was on the Board of Directors of a New York life insurance company as a member of its Audit and Investment committees.
- Scott holds a J.D. from Suffolk University Law School and a B.A. in Political Science from Gordon College. He is admitted before the Supreme Court of the United States and is licensed to practice law in the District of Columbia and in the state and federal courts of Delaware, Massachusetts and Pennsylvania.
- Scott is a frequent speaker before insurance groups and associations on compliance, privacy and the emerging issues concerning the financial services industry.

ALVAREZ & MARSAL

TAB 2

CT Information Security Laws

General Statutes § 42-470 - Restriction on posting, display, transmission and use of SSN's

A. Protect SSN's by Prohibiting:

A. Publicly displaying someone's SSN

B. Printing an SSN on any ID card

C. Requiring an SSN over unencrypted web connection

D. Require an SSN to access a website without also requiring a password

B. Penalties for Violations:

A. Non-Civil:

- 1st offense: $100 per willful violation
- Second offense: $500 per willful violation
- Third and subsequent offenses: $1,000 and/or 6 months imprisonment

B. Civil Penalty: $500 per willful violation, to a maximum of $500,000 for any single event.

****Civil penalties shall be deposited into the CT privacy protection guaranty & enforcement account.****

CT Information Security Laws

General Statutes § 42-471 - Safeguarding of personal information

A. Safeguards for "Personal Information" (defined broader than in breach statute):

1. Must safeguard data, computer files and documents containing the personal information of another person from misuse by third parties; and
2. Shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.

B. Safeguards for SSN's:

1. Any person who collects SSN's in the course of business shall create a privacy protection policy which shall be published or publicly displayed (e.g., on internet web page);
2. Such policy shall:

a) Protect the confidentiality of Social Security numbers;

b) prohibit unlawful disclosure of Social Security numbers; and

c) limit access to Social Security numbers.

C. Penalties for violations:

1. Civil Penalty: $500 per willful violation, to a maximum $500,000 for any single event.

****Civil penalties shall be deposited into the CT privacy protection guaranty & enforcement account.****

CT Information Security Laws

General Statutes § 36a-701b - Breach of Security Re Computerized Data Containing Personal Information

- Unauthorized access to or acquisition of data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable

- **"personal information"** means first name or first initial and last name in combination with one or more of the following: (1) SSN; (2) driver's license number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

- Notice must be made without unreasonable delay to consumers **and AG**.

- Notification not required if "after an appropriate investigation ***and consultation with relevant federal, state and local agencies responsible for law enforcement***, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."

TAB 3

Morgan Lewis

CYBERSECURITY: LEGAL, REGULATORY, AND PRACTICAL CHALLENGES FACING THE INSURANCE INDUSTRY

Mark Krotoski and Daniel Savrin

May 19, 2015

Overview

- Increasing Cyber Threats with Increased Sophistication
- Multiple Government Agencies with Oversight and Enforcement Authority
- Considering the Tension – Issues Raised in Cooperating with the Government
- The Severity of Government Remedial Action is Often Proportionate to the Extent of Pre-Existing Efforts to Protect Cyber Assets
- Private Litigation – Often Involving Credit Card Data – Has Faced Pleading and Class Certification Challenges
- Settlements Have Often Been More Measured Due to These Considerations
- Litigation Considerations and Settlements Are Likely to Vary Based on Nature of Data at Issue
- Be Prepared = Best Motto for Both Protection and Mitigation of Government and Private Litigation Exposure

Increasing Cyber Threats with Increased Sophistication

- International hacking groups
- Cyber-espionage
- State-sponsored intrusions
- Cyber fraud
- Hacktivists
- Insider threat
- Greater sophistication
- Malware
- Targeting More Detailed Customer Data and Valuable Corporate Information

New Executive Order Acknowledges Threat and Need for Responsive Action

- "Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit. From now on, we have the **power to freeze their assets, make it harder for them to do business with U.S. companies, and limit their ability to profit from their misdeeds**."

BRIEFING ROOM | ISSUES | THE ADMINISTRATION | PARTICIPATE | 1600

Home • Briefing Room • Presidential Actions • Executive Orders

The White House
Office of the Press Secretary

E-Mail | Tweet | Share | +

For Immediate Release

April 01, 2015

Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"

EXECUTIVE ORDER

BLOCKING THE PROPERTY OF CERTAIN PERSONS ENGAGING IN

SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.

The Challenge of the Multi-Pronged Approach to Government Enforcement

The Multitude of Government Enforcement Agencies Create Compliance Issues and May Engender Tensions for Corporate Actors

There are multiple potential government enforcement authorities including:

- Secret Service
- FBI
- FTC
- FCC
- Office of Civil Rights (OCR) at Dep't of Health and Human Services
- SEC
- CFPB
- FINRA
- State Attorneys General
- State Consumer Protection Agencies
- State Insurance and other Industry Regulators
- State Police




Managing the multiple enforcement agencies - - or simply determining who may assert enforcement authority - - can present a genuine challenge

The Multitude of Government Enforcement Agencies Create Compliance Issues and May Engender Tensions for Corporate Actors

There are multiple state and federal agencies that assert regulatory authority or oversight with respect to cybersecurity issues. The scope of their authority may very depending upon the nature of the insurance company operations and the data involved. Federal law does not pre-empt state law--as a result, while there is significant overlap, standards may differ between the various agencies.

State insurance commissioners will have direct authority over all insurance companies' practices.

Other agencies will have general authority of cybersecurity and privacy practices including:

- Federal Trade Commission which has asserted authority over such matters and issued generalized guidance
- State attorney generals and consumer protection agencies per state statutes and regulations that generally govern privacy and data breach matters

The Multitude of Government Enforcement Agencies Create Compliance Issues and May Engender Tensions for Corporate Actors

Other agencies have authority based on the nature of the business or information:

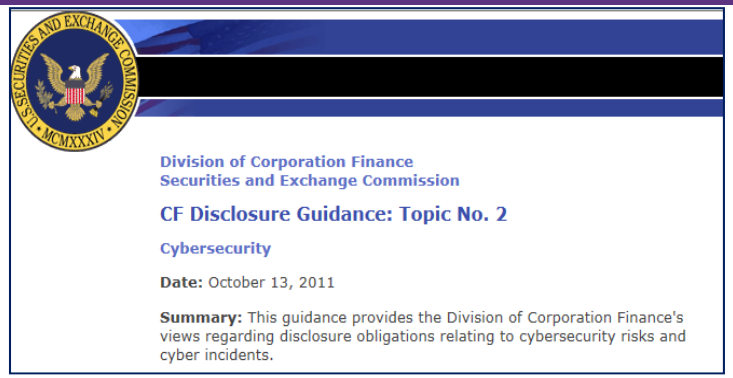
- Security and Exchange Commission (regulations and guidance relative to publicly traded companies)
- Office of Civil Rights (OCR) and Department of Health and Human Services (statute, regulations and guidance relative to health care information)
- CFPB (statutes, regulations and guidance for consumer facing finance businesses)

Other agencies or self-regulatory bodies have provided guidance and standards on cybersecurity matters:

- U.S. Department of Justice (Guidance)
- FINRA – guidance and standards for financial firms
- NIST – guidance templates of general application

In formulating their cybersecurity policies and plans, insurance companies need to be mindful of all the potentially applicable regulations, guidance and standards.

SEC Cybersecurity Disclosures



Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

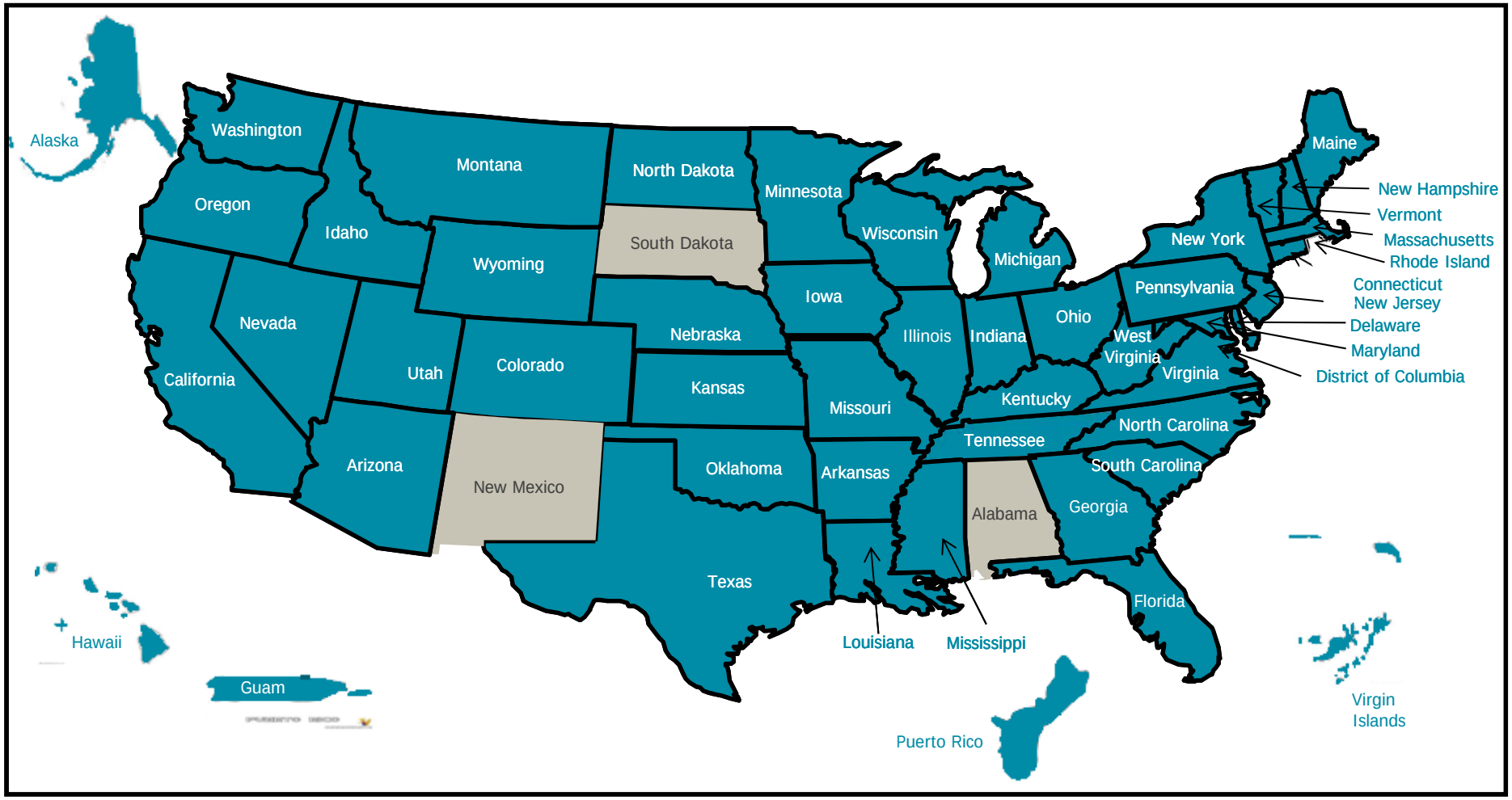
Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents

The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.[2] Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.[3] Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

The following sections provide an overview of specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.

http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

47 Breach Notification States



Morgan Lewis

Differing State Notification Standards

- Vary by state and circumstances of the breach

  - ❖ Definition of “personal information”
  - ❖ Notification trigger
  - ❖ Notification to AG or other state agency
  - ❖ Manner of notification
  - ❖ Data format: hard copy files vs. electronic only
  - ❖ Safe harbor for encryption

NAIC Principles May Lead to a Further Level of Regulations and Enforcement

Principles for Effective Cybersecurity: Insurance Regulatory Guidance[1]

Due to ever-increasing cybersecurity issues, it has become clear that it is vital for state insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to aid in the identification of uniform standards, to promote accountability across the entire insurance sector, and to provide access to essential information. State insurance regulators look to the insurance industry to join forces in identifying risks and offering practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers.

Principle 1: State insurance regulators have a responsibility to ensure that personally identifiable consumer information held by insurers, producers and other regulated entities is protected from cybersecurity risks. Additionally, state insurance regulators should mandate that these entities have systems in place to alert consumers in a timely manner in the event of a cybersecurity breach. State insurance regulators should collaborate with insurers, insurance producers and the federal government to achieve a consistent, coordinated approach.

Principle 2: Confidential and/or personally identifiable consumer information data that is collected, stored and transferred inside or outside of an insurer's, insurance producer's or other regulated entity's network should be appropriately safeguarded.

Principle 3: State insurance regulators have a responsibility to protect information that is collected, stored and transferred inside or outside of an insurance department or at the NAIC. This information includes insurers' or insurance producers' confidential information, as well as personally identifiable consumer information. In the event of a breach, those affected should be alerted in a timely manner.

Principle 4: Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework.

---

[1]These principles have been derived from the Securities Industry and Financial Markets Association's (SIFMA) "Principles for Effective Cybersecurity Regulatory Guidance."

NAIC Principles May Lead to a Further Level of Regulations and Enforcement

Principle 5: Regulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations.

Principle 6: State insurance regulators should provide appropriate regulatory oversight, which includes, but is not limited to, conducting risk-based financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident response by insurers, insurance producers, other regulated entities and state insurance regulators is an essential component to an effective cybersecurity program.

Principle 8: Insurers, insurance producers, other regulated entities and state insurance regulators should take appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.

Principle 9: Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

Principle 10: Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer's board of directors or appropriate committee thereof.

NAIC Principles May Lead to a Further Level of Regulations and Enforcement

Principle 11: It is essential for insurers and insurance producers to use an information-sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

Principle 12: Periodic and timely training, paired with an assessment, for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity issues is essential.

Considering the Tension – Issues Raised in Cooperating with the Government

- Whether and when to cooperate with law enforcement?
- Tensions are presented on the timing and consequences
- Consider the ability of law enforcement to protect the interests of the company as a victim of cybercrime

- Benefits
  - Investigative resources
  - International investigation
  - Prosecution, prison, restitution
  - Victim rights requirements and issues

- Tradeoffs
  - Lose control over timing
  - Potential adverse publicity
  - Reputational harm
  - Long process
  - Representing the interests of the company
  - Litigation consequences

State and Federal Government Enforcement

State and Federal Enforcement Agencies Have Broad and Comprehensive Authority to Pursue Sanctions and Remedial Measures

- State and federal laws enable significant per violation sanctions (e.g., $5,000 per individual violation)
- State and federal laws enable recovery of additional sums (e.g., attorneys' fees, restitution)
- State and federal laws also authorize pursuit of injunctive relief

Government Response Generally Commensurate with Corporate Actor's Safeguard Measures

- Many Statutory Frameworks Provide for Voluntary Resolutions - - the Usual Course for Privacy and Security Investigations
- Sanctions and Fines Tend to Vary Based on the Sense of Responsibility - - Whether the Breach was the result of a Hack, Lax Oversight or the Enabling of Access (Inadvertent or Otherwise) Often Matters
- Fines and Remedial Measures are Often More Measured When the Breach is the Result of Outside Actors and Reasonable Measures Were in Place to Protect Data

Government Response Generally Commensurate with Corporate Actor's Safeguard Measures

- Examples of the Varied Approach to Enforcement:
- FCC **$25 Million Fine** of AT&T for Privacy Breach - - Allegations that AT&T Call Center Employees Had Access to and Sold Customer Information
- **$4.8 million HIPAA Settlement** with Two New York Hospitals - - Allegations that Absence of Technical Safeguards Enabled Access to ePHI by Internet Search Engines (New York and Presbyterian and Columbia)
- Multi-state Attorney General Settlements from victim of hacking attack that disclosed millions of consumer records instituted additional security measures and paid approximately **$100,000** (Zappos)
- **$850,000** multi-state Attorney General Settlement over Data Breach involving approximately 260,000 customers records where the breach allegedly occurred through the loss of unencrypted data back-up files (TD Bank)
- FTC Settlements Involving Comprehensive Information Security Programs (limited authority to pursue fines)

Private Litigation

Class Action Litigation Generally Follows in the Wake of an Announced Data Breach or Enforcement Action

- Class Litigation Often Follows Within Days, if not, Hours of Data Breach News or Announcements
- There Are Few Private Rights of Action with Respect to Privacy Breaches: Cases Generally Proceed Under Unfair and Deceptive Trade Practices Statues or Common Law Contract and/or Tort Theories
- Under the Class Action Fairness Act, Cases Generally Proceed in Federal Court As Consolidated Multi-District Litigation
- These Cases Engender Considerable Motions Practice - - Often Surrounding Pleading of Injury and Damage
- These Cases Have Often Settled For What Appear to be Relatively Modest Sums

Cybersecurity Breaches Are Pursued Under Many Different Causes of Action

- Consumer Protection Laws
- Breach of contract
- Failure to provide notice or disclose material fact
  - Data Breach notifications
  - SEC or other required notifications
- Negligence-type claims
  - Failure to maintain adequate computer systems and date security practices
- Injunctive Relief
- Statutory Claims
  - Where applicable - - few statutes create private rights of action

Cybersecurity Breach Claims May Be Brought by A Variety of Potential Plaintiffs

- Consumers and customers
  - Owners of the Personally Identifiable Information (PII)
- Financial institutions
  - Credit card companies
- Company constituents
  - Shareholder derivative actions
  - Vendors

Private Cybersecurity Litigations Often Engenders Significant Motions Practice

- Motions Practice Involving Injury In Fact and Standing Have Largely Arisen in the Context of data breaches involving credit card information . The circuits are split on the standards. For example:
- The Third Circuit has held that the threat of future injury was insufficient to confer Article III standing because the alleged injury was too conjectural and speculative. The court also noted that the purchase of credit monitoring services to prevent potential harm was equally insufficient to establish standing because plaintiffs had not incurred such expenses as a result of any actual injury. *Reilly v. Ceridian, Corp* 664 F.3d 38 (3d Cir. 2011)
- The Seventh, Ninth, and Tenth Circuits have taken a different position finding a lower threshold for alleging injury-in-fact. *Pisciotta v. Old Nat'l Bancorp,* 499 F.3d 629, 634 (7th Cir. 2007) (concluding that the threat of future harm satisfied the injury-in-fact requirement); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141-42 (9th Cir. 2010) (ruling that "generalized anxiety and stress" is sufficient to confer Article III standing); *Ruiz v. Gap*, 380 Fed. Appx. 689, 690-91 (10th Cir. 2010) (holding that the increased risk of identity theft was sufficient for Article III standing, but acknowledging that it falls short of establishing damages for negligence purposes)
- The First Circuit, concluding that it was foreseeable that a customer would mitigate damages by replacing the compromised card and purchasing insurance, held that injury-in-fact was sufficiently alleged, particularly where card owners suffered actual financial losses from subsequent identity theft and card misuse, and were not exposed merely to an increased risk of injury. *Anderson v. Hannaford Brothers Co.* 659 F.3d 151 (1st Cir. 2011) (class certification later denied because need to prove individualized damages defeated predominance)

Private Cybersecurity Litigation Often Engenders Significant Motions Practice

- Watch this Space: New Supreme Court Case Next Term

  Spokeo, Inc. v. Thomas Robins (No. 13-1339)

- **Question Presented**
  - Whether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a statute.

- **Impact**
  - Will the Supreme Court's opinion have far-reaching consequences for private cybersecurity litigation?

Standing and Damages Issues Will Likely Differ Based Information Disclosed and Its Perceived Potential to Injure Individuals

- It is expected that Plaintiffs will Vigorously Assert That Injury-In -Fact and Damages Will Be Easy to Allege and Prove in Other Contexts
- It is Anticipated that Credit Card Information is Tightly Controlled with Limits on Individual Exposure Whereas Disclosure of Information that May Concern Finances or Behavioral Characteristics are More Likely to Cause Justiciable Injury
- Expect Class Certification to Continue to Present a Challenge to Class Certification

Privacy Settlements Often Reflect the Legal Challenges Facing Privacy Litigation and the Associated Expenses

- Some examples of recent settlements:
- In *In re Countrywide Financial Corp.* Countrywide agreed to pay **$6.5 million** to settle privacy and identity theft related claims arising from a 2008 data breach affecting over 2.4 million subprime borrowers. 2010 WL 3341200 *(W.D. Ky. 2010).*
- *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation*, the court approved a **$3 million settlement** of claims arising from a 2009 data breach involving over 130 million credit card accounts. 851 F. Supp. 2d 1040 (S.D. Tex. 2012). (Only 290 claims were filed—of which only 11 were valid—in a potential class of 130 million. Only **$1,925** was paid out to class members, and the remainder was distributed through cy pres, to plaintiff's attorneys' or to the notice administrator)
- In *Sterling v. Strategic Forecasting Inc.*, a global security analysis company agreed to settle charges that it failed to adequately protect class members' credit card information after a hacker stole a large amount of client data. Under the terms of the settlement, Strategic Forecasting provided class members with one free month of service, a free copy of an e-book published by the company called "The Blue Book," one year of credit monitoring service, and turn over all insurance proceeds from the data theft. No. 2:12-cv-00297 (E.D.N.Y. Nov. 15, 2012).

Data Breaches Also Often Engender Litigation Brought By Affected Commercial Actors - - This Is a Growing Area of Litigation with Heightened Associated Risk

- Compare Preliminarily Approved **$10 Million Target Consumer Settlement** with Reported Up to **$19 Million Settlement** with Master Card which is the Subject of On-Going Challenges From Member Banks
- Shareholder Actions Were Also Filed Against Target
- Derivative Actions Have Also Been Pursued in Cybersecurity Matters
- Litigation Has Often Followed Against Vendors or Third Party Service Providers
- Coverage Litigation Often Also Follows With Respect to Both Private Litigation and Enforcement and Compliance Expenses

What Can You Do To Protect Against Cybersecurity Litigation Risks

Are You Prepared?

- How prepared are you?

- Consider two scenarios:
  - Companies that have been breached
  - Companies about to be breached

- Who is responsible in your company to assist in preparing for and responding to a data breach?

Protective and Mitigation Measures Help Minimize Both Risk and Exposure

(1) Identify what information has the greatest value or is at risk

- Identify and protect the “crown jewels”
- Including company trade secrets as well as the company and its customers confidential information

(2) Identify key risks in protecting the data

- Avoid any weak links
- As part of Data and Trade Secret Action Plans, institute physical, administrative and technical safeguards and make sure third party vendors and service providers do so as well

(3) Have a current, tested incident response plan

- Conduct gap analyses and constantly monitor and test your systems
- Develop and enhance your action plans

(4) Who is responsible for managing cyber risk in the organization?

- Who reports to the board -- critical to setting agenda with the company and, as need be, demonstrating its importance to others

Be Prepared

- Establish multi-disciplinary and comprehensive Data Breach and Trade Secret Theft Action Plans
- Run drills on the action plans to test and improve the plan
- Include outside counsel and key consultants in plan development (covered by the attorney client privilege), refinement and testing to make sure that they are equipped to, and capable of, responding immediately should matters go awry
- Immediate mitigation is key to control both the disclosure risks and the litigation risks
- Failure to mitigate or implement plans properly can have dire consequences

Questions

Daniel S. Savrin
Boston, Massachusetts
tel. +1.617.951.8674
fax. +1.617.428.6310
Daniel.savrin@morganlewis.com

Mark L. Krotoski
Silicon Valley, California
tel. +1.650.843.7212
fax. +1.650.843.4001
mkrotoski@morganlewis.com

THANK YOU

ASIA

Almaty
Astana
Beijing
Singapore
Tokyo

EUROPE

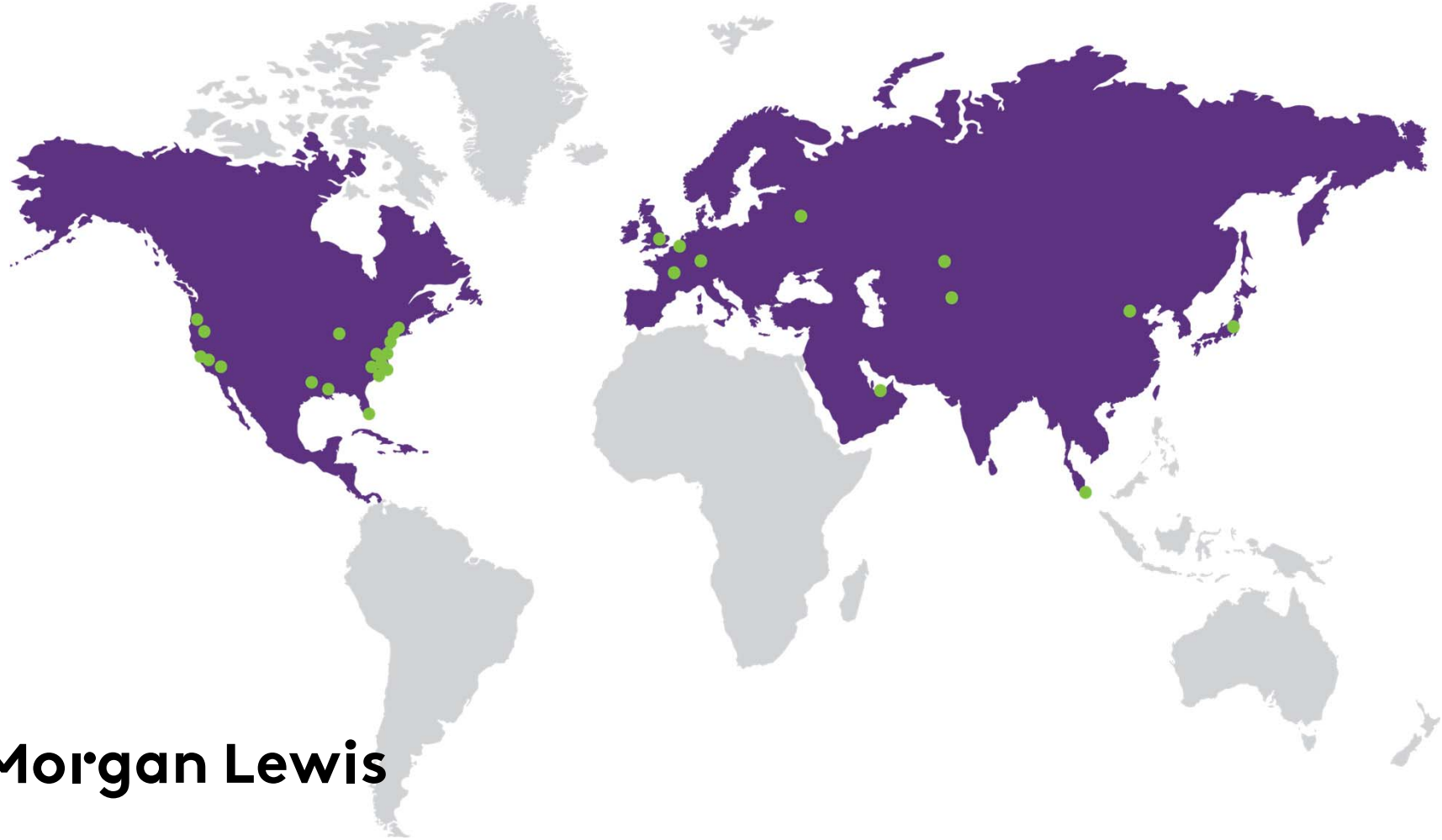
Brussels
Frankfurt
London
Moscow
Paris

MIDDLE EAST

Dubai

NORTH AMERICA

Boston
Chicago
Dallas
Harrisburg
Hartford
Houston
Los Angeles
Miami
New York
Orange County
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Washington, DC
Wilmington



Morgan Lewis

TAB 4

THE NATIONAL LAW JOURNAL
FEBRUARY 19, 2015
An ALM Publication

THE PRACTICE | Column

Five Key Cybercrime and Cybersecurity Issues To Consider

BY MARK L. KROTOSKI


CREDIT: BOYGOVIDEO/ISTOCKPHOTO.COM

On Jan. 20, during his State of the Union Address, President Barack Obama highlighted the need to enact cybersecurity legislation in the near term. As he framed the issue:

> "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyberthreats, just as we have done to combat terrorism. And tonight, I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyberattacks, combat identity theft and protect our children's information. If we don't act, we'll leave our nation and our economy vulnerable. If we do, we can continue to protect the technologies that have unleashed untold opportunities for people around the globe."

The White House later previewed some of its cybersecurity strategy and legislative proposals. More details will be coming soon. Additionally, FBI Director James Comey highlighted " a five-point strategy" to address cybersecurity. On Feb. 10, a new Cyber Threat Intelligence Integration Center was announced by White House officials as part of an effort to strengthen our national cyber defenses. On Feb. 13, Stanford hosted the White House Cybersecurity Summit, which focused on a host of cybersecurity issues.

There are many facets to cybersecurity. This article highlights five key issues for consideration.

1. National notification standards. Data breach notification has become unnecessarily complicated, confusing and costly. Clearly defined uniform standards would promote the objectives of notification.

Nearly 13 years ago, the first data security-breach notification law was enacted in California. Since then, 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have adopted breach notification laws. Many states are adding and enacting notification requirements or considering new ones.

The original objective—to inform consumers about data breaches involving their personal and financial information—has turned into a notification maze and nightmare. Given the many notification standards, conflicts have emerged including over what triggers notification and when and how to provide notice. It should not be as complicated and confusing as it has become for a company to provide notice to consumers. The failure to satisfy the notification standards may subject the company to lawsuits even though the company has tried in good faith to comply.

The states are unlikely to adopt uniform notification standards, given the myriad of state laws and standards that have been adopted and new ones being advanced. Eventually, Congress can establish national notification standards. Delay in doing so will permit the status quo to persist, resulting in an unnecessarily complicated, confusing and costly mix of standards undermining the notification purposes and compliance.

2. Restore effectiveness to the Computer Fraud and Abuse Act. The primary federal computer crime statute is the Computer Fraud and Abuse Act (CFAA), originally enacted in 1984 and amended through the years. A civil private right of action may also be permitted under the law. The effectiveness of this statute has been questioned in recent years. The act should be updated to address current computer crime issues. A couple of examples are noted.

Courts are divided about whether the

CFAA covers insiders initially granted access to computers but who then use that access to harm the company or owners of the computer data. Let's say you just learned that a long-term, trusted employee had used company computers to download, steal and transfer confidential business information either to start his own company or provide it to a competitor.

Would this theft of company information be a crime under federal law? Under existing law, it depends on the jurisdiction in which the theft occurred. The federal courts are divided as to whether the company's prior authorization of its computers disallows a later violation under the CFAA.

The courts have found the statutory terms concerning computer access "without authorization" or "exceed[ing] authorized access" difficult to apply. The statute does not define the terms "without authorization." However, the terms "exceeds authorized access" mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

The division in the courts over the application of the statute has persisted for several years and should be clarified. Insider theft of computer information should be a crime covered under the statute. This type of conduct should not be subject to varying interpretations by the courts.

Other ambiguities persist. For example, since 2008 the CFAA has included a conspiracy provision. However, the statute does not specify what penalties apply to conspiracy convictions.

3. Trade-secret remedies and protection. Trade secrets continue to provide a key source of innovation and value to the economy. As a result of their significant value, trade secrets are targeted for theft and cyber-espionage. Some have estimated the cost of trade-secret theft to range from 1 percent to 3 percent of the gross domestic product of the United States and other advanced industrial economies.

In his recent speech, the president made clear that neither foreign nations nor hackers should be allowed to "steal our trade secrets." Congress should enact legislation that would create a federal private right of action for the theft of trade secrets for the first time. Under the Economic Espionage Act of 1996, the Department of Justice could prosecute the misappropriation of trade secrets. However, few trade-secret thefts require or criminal prosecution.

Generally, state trade-secret laws are effective at addressing local theft. When trade secrets are removed from the state or country, trade-secret owners confront a cumbersome process in seeking effective remedies. Trade-secret owners should be able to remedy theft in federal court. Trade secrets are the only form of intellectual property that lacks a federal private right of action.

Companies should have the option of seeking relief in either state or federal court. The new federal law would also provide more effective protection for trade secrets than under existing state law and encourage innovation and trade-secret development.

4. Sharing of cyberthreat information. New avenues should be established to effectively share government and private industry information about cyberthreats to avoid and mitigate further harm. Information sharing takes places on many levels. The government has information about cyberthreats that it can share with private industry. Private industry obtains information that it can provide to others in the private sector and to government.

The National Institute of Standards and Technology recently issued a draft report for public comment to highlight information-sharing best practices. As summarized by the report:

> "When an organization identifies and successfully responds to a cyberattack, it acquires information that can be used by other organizations that face the same or similar threats. When information is shared, threatened organizations have access to threat intelligence provided by peer organizations and are able to rapidly deploy effective countermeasures and detect intrusion attempts. As a result, the impact of a successful cyberattack can be reduced."

Presently, there is a chilling effect on sharing cyberthreat information that may help others based on liability concerns. Some companies fear that the disclosure of information would result in regulatory action or lawsuits. Congress has been considering this problem and legislation has twice passed in the House of Representatives only to stall in the Senate. Until the liability problems can be addressed, key threat information will not be disseminated to those who can use it.

5. Promoting understanding and restoring public trust. Without public trust, law enforcement is constrained in investigating crime and protecting society.

On Dec. 4, Assistant Attorney General Leslie Caldwell announced the creation of a DOJ cybersecurity unit to "address cyberthreats on multiple fronts, with both a robust enforcement strategy as well as a broad prevention strategy." In her speech, she appropriately noted "a growing public distrust of law enforcement surveillance and high-tech investigative techniques" that "can hamper investigations" which may be based on "misconceptions about the technical abilities of the law enforcement tools and the manners in which they are used."

She is correct. Restoring public trust is a top priority. Without it, the ability to address cybercrime will be less effective. Steps should be taken to promote a better public understanding of how law enforcement solves cybercrimes and addresses privacy concerns. An important part of this debate is learning about what judicial showing is required for law enforcement to obtain data and the steps necessary to address cybercrime today.

There are many aspects to providing effective cybersecurity. These five issues, among others, will advance cybersecurity efforts. The time is ripe for meaningful legislation.

MARK L. KROTOSKI *is a partner in the privacy and cybersecurity, antitrust and litigation groups at Morgan, Lewis & Bockius. He previously served as a prosecutor in computer hacking and intellectual property crime units in the Northern and Eastern Districts of California and as coordinator of the DOJ's national program. The views expressed are his own and not necessarily those of the firm or any clients.*

TAB 5

Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity

Views on Cyberthreat Information Sharing From Mark L. Krotoski of Morgan Lewis

As hacking attacks on U.S. businesses grow in intensity, the call for stronger private sector cybersecurity risk data sharing with the government has grown louder.

Bloomberg BNA Privacy & Security Law Report Senior Legal Editor Donald G. Aplin posed a series of questions to Mark L. Krotoski, a partner at Morgan Lewis & Bockius LLP in Palo Alto, Calif., about cyberthreat data sharing. Krotoski has nearly 20 years of experience as a federal prosecutor, including serving as national coordinator for the Computer Hacking and Intellectual Property Program in the Department of Justice's Criminal Division.

BLOOMBERG BNA: What are the primary concerns for companies in terms of partnering with the government to address cybersecurity issues generally and to respond to specific cyberattack threats and investigations?

Krotoski: The sharing of cyberthreat information is generally recognized as one key facet of an effective cybersecurity sharing strategy. Once information about a cyberthreat becomes known, the sharing of that information can prevent and mitigate other significant losses for others. Notwithstanding the substantial benefits that may result, presently there is a chilling effect on the sharing of cyberthreat information. Some of the primary obstacles include:

- What civil or criminal liability may result from information sharing?

- How will the government use information that is shared? For example, will the information be given to

 ISSN 1538-3423

regulators who may open an investigation on the reporting company? Will the National Security Agency use the shared information for intelligence purposes?

■ On privacy concerns, how can personal information or information identifying a particular individual be protected in sharing cyberthreat information?

■ Will shared information with the government be subject to later disclosure based on Freedom of Information Act requests?

■ What other regulatory issues are raised by information sharing? For example, when competitors in an industry share cyberthreat information, how are antitrust issues addressed?

An analogy helps explain the present challenges. Assume you live in a neighborhood where each residence has a strong security system. For some unknown reason, a few residences are burglarized without detection. If one neighbor learns how the security system is bypassed, he could share it with others. Armed with this information, the neighbors could protect themselves by addressing the security vulnerability. Law enforcement may use the information to catch the burglar. However, the neighbor may refrain from sharing the information based on fears about the consequences from the disclosure.

We need to incentive the neighbor to share the cyberthreat information without fear of the potential consequences. Until these obstacles are addressed, those who can benefit most from the cyberthreat information will not receive it.

BLOOMBERG BNA: Do you think President Barack Obama's February executive order directing the Department of Homeland Security to identify voluntary standards or guidelines for the creation industry-led information sharing and analysis organizations (ISAOs) (14 PVLR 324, 2/23/15) set the right tone for addressing those concerns and encouraging private sector participation?

The executive order is an administrative step to promote cybersecurity sharing, but it cannot be a substitute for necessary legislation that is required to accomplish the goal of meaningful information sharing.

Krotoski: The executive order is an administrative step to promote cybersecurity sharing, but it cannot be a substitute for necessary legislation that is required to accomplish the goal of meaningful information sharing. The White House recognizes the distinction since it has offered its own separate legislative proposal for information sharing that contains other substantive provisions.

While the executive order seeks to encourage voluntary information sharing, a number of unanswered questions are raised. First, it does not—and cannot—effectively address the core obstacles to information sharing. The DHS secretary is tasked to ''strongly encourage'' the development of ISAOs. However, it is questionable whether many private organizations will conclude there are strong enough incentives to participate in the absence of legislation (which would include liability and FOIA protections, among others).

Second, the order directs agencies to ensure ''appropriate protections for privacy and civil liberties'' are developed. However, the sufficiency of these protections remains to be seen.

Third, another unanswered question concerns what limitations there are on what the government will do with the information it obtains from the private sector.

Fourth, the executive order creates a new bureaucracy and new lines of authority, and it is not clear that all of them may be necessary in light of existing functions handled by others.

Further, it remains to be seen how the new structure will be implemented. Similar organizations already are used for some sectors (such as aviation, defense industrial base, financial, electricity). How will these existing information sharing entities operate with the new ISAOs? Another goal of the ISAOs is to establish best practices on information sharing. Yet, the National Institute of Standards and Technology recently published a draft guide on these issues (13 PVLR 1979, 11/17/14). In 2013, the White House directed NIST to establish a cybersecurity framework, which was issued Feb. 12, 2014 (13 PVLR 281, 2/17/14). It remains to be seen what role NIST will serve on these issues.

Ultimately, legislation will be required to provide meaningful incentives to the private sector to share cyberthreat information with sufficient privacy and liability protections and limits on the government's use of the information.

BLOOMBERG BNA: Was the executive order consistent with Obama's January legislative proposal (14 PVLR 108, 1/19/15) to grant companies liability protection when they shared cyberthreat information with the DHS National Cybersecurity and Communications Integration Center?

Krotoski: The executive order is essentially an administrative complement to the White House legislative proposal, notwithstanding some language differences. For example, both rely on the establishment of ISAOs. Both direct that an ''open and competitive process'' be used to identify a private entity to establish standards or guidelines for private information sharing. Of course, the legislation contains substantive standards that the executive order does not, such as limitations on liability and an exemption from disclosure for FOIA requests.

BLOOMBERG BNA: Does the data-sharing bill (S. 754) moved by the Senate Intelligence Committee (14 PVLR 447, 3/16/15)—that it hopes will clear Congress and be on the president's desk sometime in May (14 PVLR 597, 4/6/15)—provide any meaningful improvements or differences from Obama's proposal?

Krotoski: Bipartisan legislative momentum is building on this issue in both the Senate and House. In addition to S. 754, two other congressional committees have reported out information sharing legislation based on strong bipartisan votes.

On March 26, the House Permanent Select Committee on Intelligence reported out H.R. 1560, the Protect-

  PVLR ISSN 1538-3423

ing Cyber Networks Act, on a voice vote, to the full House (14 PVLR 546, 3/30/15).

On April 14, the House Homeland Security Committee unanimously passed H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (*see related report*).

There are some key features in these measures that are not in the White House proposal. For example, the Senate bill would authorize ''defensive measures'' to be taken ''to protect the rights or property of the private entity'' or upon consent of''an information system of another entity.'' The Senate bill has express provisions for the sharing of information by the federal government, and the White House proposal does not. The Senate bill has an antitrust exemption provision that would allow for the exchange of cyberthreat indicators or assist in mitigating threats for cybersecurity purposes. There are some differences among the proposals on defining ''cyber threat indicator.'' Another question is which entity would receive the cyberthreat information. The White House and the House Homeland Security Committee measures would assign this function to the DHS National Cybersecurity and Communications Integration Center. The Senate bill would lead to a ''capability and process within the Department of Homeland Security,'' or ''portal,'' to receive cyberthreat information by electronic means.

It is still early in the legislative process since these measures have yet to be considered in the House or Senate. However, given the strong bipartisan, committee support, a consensus is forming on key aspects of meaningful legislation to encourage information sharing. In the past few years, information sharing legislation passed the House by a strong margin, only to die in the Senate. Now strong legislative interest is building on these issues.

BLOOMBERG BNA: Do you think the new April 1 executive order that authorized the Department of Treasury to impose sanctions on foreign individuals or entities that engage in malicious cyberattacks that threaten the economy or knowingly receive or use trade secrets stolen in such attacks (14 PVLR 578, 4/6/15) might sway private sector companies into greater information sharing with the government?

Krotoski: The order declaring a ''national emergency'' based on recent cyber espionage and malicious cyberattacks and authorizing sanctions in appropriate cases of ''malicious cyber-enabled activities''—including for ''causing a significant misappropriation'' of trade secrets—provides another tool of deterrence in appropriate cases for malicious cyberattacks. The sanctions may include the freezing of assets, denial of visas to identified hackers and barring U.S. companies from engaging in business with hackers. While it remains to be seen how frequently this new sanctions tool will be used, it provides more options to the government.

The new cyberattack sanctions executive order allows companies to conclude that by sharing cyberthreat information, the government may use a variety of tools to prosecute cybercrimals.

Significantly, the new order follows the imposition of sanctions against a country for the first time. On Jan. 2, economic sanctions against North Korea were increased based on its role in the ''destructive, coercive cyber-related actions during November and December 2014'' after the FBI announced that it had attributed to the North Korean government cyberattacks on Sony Pictures Entertainment Inc. (14 PVLR 67, 1/12/15).

Companies can conclude that by sharing cyberthreat information, the government may use a variety of tools to prosecute individuals for committing cybercrime and in appropriate cases issue sanctions. For example, where individuals cannot be extradited to the U.S., the sanctions may impose other significant penalties on those responsible for malicious cyberattacks.

BLOOMBERG BNA: Is robust pursuit of criminal prosecution of hackers by the federal government an important part of the dynamic for engendering private sector trust in a voluntary data-sharing program?

Krotoski: In our increasingly interconnected world, effectively combating cybercrime remains a key component of any national cybersecurity strategy. Law enforcement successes in combating cybercrime promote deterrence and confidence in our criminal justice system.

When private industry sees these criminal justice results, it reinforces the need to provide critical cyberthreat information to law enforcement. Private industry can contribute by providing cyberthreat information to the government with the sufficient protections we have noted

Today's cyberthreats come from many sources including state-sponsored groups engaged in cyber espionage, organized cyber syndicates, cyber terrorists and others. Cybercrime is being committed with greater sophistication than in the past. Many of the cyberattacks originate outside the U.S., making coordination with international law enforcement officials necessary.

Private industry certainly cannot address these challenges. A strong, effective ability to investigate and prosecute cybercrime remains essential. The Department of Justice Computer Hacking and Intellectual Property (CHIP) network consists of around 270 federal prosecutors around the nation. For several years, I was privileged to be a part of this network and appreciated the chance to work with many talented prosecutors around the country on interesting cases and cutting edge legal and technical issues. The CHIP network is strong and effective in addressing cybercrime issues.

TAB 6

Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

In the second installment of a series of articles covering legal issues related to trade secrets, the author identifies best practices for and a series of steps in the development of a company's trade secret protection plan.

Do You Know Whether Your Trade Secrets Are Adequately Protected? Highlighting Key Questions and Issues to Consider Before Any Misappropriation Occurs

BY MARK L. KROTOSKI

Trade secrets can be among the most valuable assets a company has. According to one study, ''Two-thirds of enterprises' information portfolio value comes from the secrets they create.''[1] One trade secret can lead to many products. As a unique form of intellectual property, trade secrets can be vital not only to a company and its employees, but also to other jobs, investments, an industry, the economy and, depending on the trade secrets, even national security.

Two Key Questions for Trade Secret Owners

Given the importance of trade secrets, trade secret owners should ask two key questions:

(1) How many trade secrets do you have?

(2) Are your trade secrets adequately protected?

The answers to these two questions may help mitigate the risk of theft or loss. If necessary, the protective measures used may determine whether there is any legal protection available under trade secret law if the trade secrets are later stolen or misappropriated.

The first question is important because different types of trade secrets require tailored forms of protection. For example, a secret recipe can be stored in a locked safe but electronic information will require passwords and other steps to restrict access on a computer network. The second question is essential as any legal protection may be forfeited if the trade secret owner did not employ reasonable steps to protect the trade secret.

Surprisingly, large and small companies holding significant trade secrets regularly fail to protect these key assets adequately. This article reviews the requirement that trade secret owners have to reasonably protect their trade secrets and highlights steps that companies can take to safeguard their trade secrets.

Trade Secret Definition: Three Aspects

A trade secret has three essential parts. First, it consists of commercial information, such as ''financial,

[1] Forrester Consulting, The Value of Corporate Secrets, at 4-5 (Mar. 2010), http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf.

Mark Krotoski is a Partner in the Litigation, Privacy and Cybersecurity, and Antitrust Practice Groups of Morgan, Lewis & Bockius, resident in the Washington, D.C., office. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice and as an instructor on economic espionage and trade secret cases and other law enforcement issues at the DOJ National Advocacy Center.

business, scientific, technical, economic, or engineering information.''[2] Illustratively, the information can include prototypes, plans, processes, codes, designs, methods and techniques. Common trade secret examples may include the Coca Cola formula or the Google algorithm.

Second, the information derives economic value from being secret; that is, from not being generally known or readily ascertainable. Third, the trade secret owner must take ''reasonable measures to keep such information secret.'' This article focuses on the role and significance of the third part of the trade secret definition, the adequacy of the steps taken by the trade secret owner to safeguard them.

Dealing With the Shock of Trade Secret Misappropriation

In working with large and small companies on trade secrets cases, I have witnessed many times that one of the greatest shocks that a company may experience is learning that key trade secrets have been stolen or misappropriated. Further, a trade secret misappropriation never happens at a good time.

Once a company learns its trade secrets were misappropriated, the company often begins a valiant chase and effort to recover the trade secrets. Regrettably, the trade secrets may never be fully recovered. Within a day or so, the trade secrets may be in another state or half way around the world in a competitor's hands. Or the trade secret may have been delivered to a foreign government.

Trade secret misappropriations are usually highly reactive events.[3] The employee who took the trade secrets may have already left and be bound for another destination when the discovery occurs. Hackers may have obtained access to the network through other servers that are hard to trace. The company's investigation will try to gather as much information as possible about the misappropriation, chasing the facts of the case.

The company will usually consider what legal remedies are available. Presently, 47 states and the District of Columbia, Puerto Rico and the U.S. Virgin Islands have enacted some form of the Uniform Trade Secret Act (UTSA).[4] In some cases, a criminal case may be opened, such as under the federal Economic Espionage Act.[5]

As past cases have shown, when any legal action occurs, the measures used by the trade secret owner will likely be called into question by defense attorneys and scrutinized in court. To be prepared for this moment, if it cannot be avoided, the steps to protect the trade secrets should be taken long before the unanticipated misappropriation.

Reasonable Measures Standard

Under trade secret law, the trade secret owner holds the obligation to use reasonable measures to protect its trade secrets.[6] As explained in the House Committee Report for the federal criminal trade secret statute:

> The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it. It is important to note, however, that an owner of this type of information need only take 'reasonable' measures to protect this information. While it will be up to the court in each case to determine whether the owner's efforts to protect the information in question were reasonable under the circumstances, it is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.[7]

Avoiding Forfeiture of a Legal Remedy Based On a Failure to Reasonably Protect Trade Secrets

The consequences of a trade secret owner failing to employ reasonable measures to protect trade secrets can be fatal. As Seventh Circuit Judge Richard Posner stated, the failure to use reasonable steps to protect a trade secret will ''forfeit protection'' under trade secret law. As he explained:

> Failure to take such steps is persuasive evidence that the secret has no real value. Courts are entitled, moreover, to economize on their scarce resources of time and effort by refusing to help a secret holder who failed to take minimum steps to protect his secret before running to court. Failure to take protective steps also sets a trap, since a company that ferrets out information that the originator does not think special enough to be worth incurring any costs to conceal will have no reason to believe that it is a trade secret.[8]

The courts will dismiss trade secret claims based on a failure to use reasonable steps to protect the trade secret.[9]

---

[2] *See, e.g.,* Economic Espionage Act, 18 U.S.C. § 1839(3) (defining trade secret); *see also* Uniform Trade Secret Act § 1(4) (same), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[3] *See, e.g.*, M. Krotoski, Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases, 57 UNITED STATES ATTORNEYS' BULLETIN 1, 13-14 (Nov. 2009) (highlighting case examples showing the reactive nature of many trade secret cases) [hereinafter Common Issues and Challenges], http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[4] Only New York, North Carolina and Massachusetts have not enacted some version of the UTSA. For a list of the jurisdictions adopting the UTSA, *see* http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade Secrets Act. The UTSA was completed in 1979 by the Uniform Law Commissioners and amended in 1985. *See* http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act. For the UTSA as amended in 1985, *see* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[5] *See* 18 U.S.C. §§ 1831-1839.

[6] *See, e.g.*, *ClearOne Communications, Inc. v. Bowers*, 643 F.3d 735, 767-68, 2011 BL 169413 (10th Cir. 2011) (jury instruction noting the trade secret owner's burden and providing factors to the jury on the issue of reasonable measures).

[7] H.R. Rep. No. 788, 104th Cong., 2d Sess. 7 (1996).

[8] *BondPro Corp. v. Siemens Power Generation*, 463 F. 3d 702, 708, 80 U.S.P.Q.2d 1207 (7th Cir. 2006); *see also* Common Issues and Challenges, *supra* note 4, at 17 (noting the importance of ''work[ing] closely with the trade secret owner to ensure that the reasonable measures in place are properly identified before charges are filed'').

[9] *See, e.g.*, *Incase Inc. v. Timex Corp.*, 488 F. 3d 46, 53, 83 U.S.P.Q.2d 1032 (1st Cir. 2007) (74 PTCJ 147, 6/1/07) (affirming judgment as a matter of law based on a failure to establish trade secret claim at trial; ''The fact that Incase kept its work for Timex private from the world is not sufficient; discretion is a normal feature of a business relationship. Instead, there must be affirmative steps to preserve the secrecy of the information as against the party against whom the misappropriation claim is made.''); *see also Fail-Safe, LLC v. AO Smith Corp.*, 674 F.

  PTCJ ISSN 0148-7965

Reasonable Protection Need Not Be Absolute

So what steps should a trade secret owner take to safeguard its trade secrets? Under trade secret law, the protective measures must be reasonable under the circumstances.

The reasonableness standard reinforces the innovation objectives of the trade secret law. If the costs of maintaining secrecy are too high, innovation will be discouraged. The protective measures should be sufficient to safeguard the trade secrets and encourage innovation.

As Judge Posner aptly framed the issue, ''If trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention.''[10] For good reason, trade secret law does not require the best or most costly standards of security. The law only requires reasonable measures to protect the trade secret.

Key Focus: Are the Protective Steps Reasonable When Considered as a Whole?

Trade secret law focuses on the protective measures used when viewed as a whole. The law disregards other steps that may have been taken.

Consider an example. One common step that a trade secret owner may take to protect a trade secret is to simply lock it up to exclude others from access. As a general matter, this approach is not a costly security measure. Does the failure to take this step adversely affect the determination on whether the trade secret was reasonably protected? This question came up in a case involving some sensitive trade secrets involving restricted technology and trade secrets related to the space shuttle program and Delta IV rocket.

In *United States v. Chung*, the defendant, a former Boeing engineer, was convicted at a bench trial on foreign economic espionage and related charges for misappropriating trade secrets with the intent to benefit the government of the People's Republic of China. The trade secrets included ''four documents about a phased array antenna for the space shuttle and two documents about the Delta IV Rocket.''[11] On appeal, he challenged the sufficiency of the evidence to support the economic espionage counts because Boeing had failed to lock up some of the trade secrets. In other words, he argued that the trade secret owner could not show reasonable measures were taken and therefore the economic espionage counts should be dismissed. The Ninth Circuit court of appeals rejected this argument by considering the collective steps taken to protect the trade secrets. As the court explained:

> Although none of the documents was kept under lock and key, Boeing implemented general physical security measures for its entire plant. Security guards required employees to show identification before entering the building, and Boeing reserved the right to search all employees' belongings and cars. Boeing also held training sessions instructing employees not to share documents with outside parties, and it required employees, including Defendant, to sign confidentiality agreements. Further, two of the four phased array documents (underlying counts 3 and 5) were marked as proprietary. Thus, there was sufficient evidence to support the conclusion that Boeing took reasonable measures to keep all four phased array antenna documents secret.[12]

Other cases have reached a similar result. For example, the Sixth Circuit concluded that a company had collectively taken ''reasonable measures to keep the design of its tire-assembly machines secret'' even though the company did ''not secure its tire-manufacturing machines under lock and key within its'' plant.[13] In affirming the convictions of two employees of a competitor that gained access to and took photographs of the trade secret, the court concluded that other measures were reasonable when considered as a whole. These other measures included surrounding the plant with a fence, a requirement that visitors ''pass through a security checkpoint,'' advance permission to enter into the plant, the signing of confidentiality agreements which included terms the signers ''would not use or disclose that information for ten years,'' an agreement not to take photographs (which the defendants violated), and a requirement that suppliers agree to maintain the company information secret.[14] Taken as a whole, these measures were reasonable and other measures, such as a lock and key, were not required.

Consider one more example. One common security measure is a confidentiality agreement that governs the terms of access to the trade secret and imposes obligations to return the confidential information. If a confidentiality agreement is not used, will it undermine the reasonableness of the protections surrounding the trade secret? Well, it depends on what other measures are used. When this issue arose in a trade secret case, the Seventh Circuit concluded the failure to use a confidentiality agreement with subcontractors did not matter in light of other steps that were taken. As the court noted:

> None of [trade secret owner] RAPCO's subcontractors receives full copies of the [trade secret] schematics; by dividing the work among vendors, RAPCO ensures that none can replicate the product. This makes it irrelevant that RAPCO does not require vendors to sign confidentiality agreements; it relies on *deeds* (the splitting of tasks) rather than *promises* to maintain confidentiality.[15]

In trade secret cases, it is not uncommon for the defense to nitpick what other steps may have been taken by the company to protect the trade secret, often with the benefit of hindsight. Trade secret law is clear that the focus is not on what steps could have been taken, but rather whether the protective steps considered as a whole were reasonable. For example, as the Tenth Circuit noted on this issue, ''there always are more security

---

3d 889, 892, 2012 BL 77648 (7th Cir. 2012) (affirming district court determination that the company ''failed to take reasonable precautions to protect its trade secrets'' which ''vitiates FS's claim of misappropriation''); *Tax Track Systems Corp. v. New Investor World, Inc.*, 478 F.3d 783, 785 (7th Cir. 2007) (''Typically, whether a party took reasonable steps to protect its confidential information is a fact question for the jury, but here no reasonable jury could conclude that Tax Track's meager and inconsistent protective measures were sufficient to protect its information.'').

[10] *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179-80, 17 U.S.P.Q.2d 1780 (7th Cir. 1991).

[11] *United States v. Chung*, 659 F.3d 815, 823, 2011 BL 244585 (9th Cir. 2011).

[12] *Id.* at 827.

[13] *United States v. Howley*, 707 F.3d 575, 579, 105 U.S.P.Q.2d 1886 (6th Cir. 2013) (85 PTCJ 472, 2/8/13).

[14] *Id.* at 578, 579.

[15] *United States v. Lange*, 312 F.3d 263, 266, 72 U.S.P.Q.2d 1671 (7th Cir. 2002) (emphasis in original).

precautions that can be taken. Just because there is something else that [the trade secret owner] . . . could have done does not mean that their efforts were unreasonable under the circumstances.''[16]

With regard to the federal trade secret statute, the Economic Espionage Act, Congress was clear that all possible steps are not required to protect the trade secret, only reasonable ones:

> The fact that the owner did not exhaust every conceivable means by which the information could be kept secure does not mean that the information does not satisfy this requirement. Rather, a determination of the 'reasonableness' of the steps taken by the owner to keep the information secret will vary from case to case and be dependent upon the nature of the information in question.[17]

In sum, these cases highlight a couple of useful lessons. First, the test in court is whether the measures protecting a trade secret were reasonable when considered together. Second, the focus is on the reasonableness of the steps used, not those that could have been used.

Recommended Steps: An Objective, Early Assessment of Protective Measures

The primary goal is to safeguard the trade secrets. Sufficient measures can protect the trade secrets for many years. Ideally, the company will never experience the shock that comes from learning that its trade secrets were misappropriated or stolen. In that event, the efforts of the company will be redirected to recover the trade secrets and protect the reputation and brand of the company.

Given the importance of the trade secrets to most companies, support from the top is central. Company executives and leaders can establish and underscore a culture and system of protection within the company.

The protections need to be tailored to the individual trade secret. Different trade secrets will require distinct measures of protection.

Layered Levels of Security Protection

Generally a layered approach works not only reasonably but effectively. The layers limit access to the trade secrets on a need to know basis and mitigate potential threats of misappropriation from several sources.

The security layers will typically include physical, policies and practices, technology and contractual aspects in addition to objective legal guidance from experienced counsel. For example, on the first level, some **physical safeguards** may include a fence, security guards and key cards to limit and record access.[18] A locked safe or room can be used to store the trade secrets. Identification systems can be used to record who has accessed the trade secrets.[19] Sign-in sheets and escorts may be used for visitors.

Another layer of protection will be based on **company policies and practices**.[20] One essential policy is to require an exit interview for departing employees. The interview can reinforce the obligations to return company property, usually reflected in a confidentiality agreement. It can also provide an opportunity to learn if any trade secrets are outside of the company. Another company practice may include education and training that underscores the company culture of protecting trade secrets. Loyal employees will be reminded about the importance of protecting company assets and reporting unusual activity. Trade secret material may be marked as confidential.

Most likely **technology protections** will provide another layer of security, particularly if the trade secret is in electronic form or touches a computer network.[21] Restrictions can be used to limit access to the network. Password policies can ensure that passwords are sufficiently strong and changed at appropriate times. Encryption practices should be required. Network logs may confirm who has accessed the business information.

As another layer of protection, **contractual agreements** can be used with employees and subcontractors with access to the trade secret information.[22] Depending on the jurisdiction, confidentiality, non-disclosure

---

[16] *Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1113, 91 U.S.P.Q.2d 1801 (10th Cir. 2009) (78 PTCJ 513, 8/21/09).

[17] H.R. Rep. No. 788, 104th Cong., 2d Sess. 12-13 (1996); *see also id*. at 7 (''[A]n owner of this type of information need only take 'reasonable' measures to protect this information. . . . [I]t is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.''); *Surgidev Corp. v. Eye Tech., Inc.*, 828 F.2d 452, 455, 4 U.S.P.Q.2d 1090 (8th Cir. 1987) (''Only reasonable efforts, not all conceivable efforts, are required to protect the confidentiality of putative trade secrets.'').

[18] *Chung*, 659 F.3d at 825 (''Security measures, such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as confidentiality agreements and document labeling, are often considered reasonable measures.''); *see also United States v. Shanshan Du*, No. 13-01606, slip op. at *12 (6th Cir. June 26, 2014) (unpublished) (noting ''physical security measures'' included ''a locked facility monitored at all times by security guards, who required employees to show a photo identification to enter'' and who ''checked all bags and computer devices carried out of the building, patrolled the facility after hours, and escorted visitors within the facility'').

[19] *See, e.g.*, *Chung*, 659 F.3d at 825–26 (noting that ''limiting access to a trade secret on a 'need to know basis' and controlling plant access'' may constitute reasonable measures).

[20] *Du*, No. 13-01606, slip op. at *12-13 (noting the use of ''formal policies and practices governing confidentiality and information security'' which ''included non-disclosure agreements signed by employees and an information security policy requiring employees to protect the company's proprietary information and limiting their access to this information on a 'need to know basis' ''). For a discussion on the use of electronic evidence to investigate trade secret cases, *see* M. Krotoski, Identifying And Using Electronic Evidence Early To Investigate And Prosecute Trade Secret And Economic Espionage Act Cases, 57 UNITED STATES ATTORNEYS' BULLETIN 42-51 (Nov. 2009), http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[21] *Du*, No. 13-01606, slip op. at *12 (noting ''the digital equivalent of'' the ''physical security checkpoints'' were used ''on its computer network'' including multiple levels of password requirements to limit access ''from unauthorized users outside the facility'' and ''within the network'' and ''to particular folders on the server containing information about the hybrid vehicle development'' and a requirement for ''permission from a manager, who authorized access only if an employee needed the files for work'').

[22] *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521, 26 U.S.P.Q.2d 1458 (9th Cir. 1993) (noting the role of requiring ''employees to sign confidentiality agreements respecting [company] trade secrets'' as a reasonable measure); *see also Chung*, 659 F.3d at 825 (noting the role of ''confidentiality

  PTCJ ISSN 0148-7965

and invention assignment agreements can be used to restrict access and impose an obligation to return trade secret information. If third parties have access to the trade secrets, confidentiality agreements are important to limit their use of the trade secrets.

As part of a company's **Trade Secret Protection Plan**, to mitigate the harm from trade secret theft, a trade secret misappropriation incident response plan can be established. For the recovery of trade secrets, minutes and hours can make a difference

Finally, **legal guidance** from experienced counsel can provide a useful role in protecting a company's trade secrets. A trade secret audit can assist in assessing the reasonableness of the trade secret protections. Experienced legal counsel can provide an objective assessment of the protections and layers of security. An individualized assessment should be made for each trade secret. Significantly, communications with experienced counsel are protected under the attorney client privilege and work product doctrines, allowing for candid discussions about the reasonableness of the measures safeguarding the trade secrets.[23]

procedures, such as confidentiality agreements and document labeling,'' as ''reasonable measures'').

[23] *See generally Upjohn Co. v. United States*, 449 U.S. 383 (1981) (reviewing the scope of the corporate attorney-client privilege).

Conclusion

Many companies have trade secrets which can generate substantial value for the company. Regrettably, experience has shown that large and small companies have not taken the steps necessary to protect them. When the unexpected misappropriation occurs, it is clearly too late.

A culture of protection can establish the tone within the company to safeguard the trade secrets. A layered approach to security has proven effective in past cases to mitigate any misappropriation and to establish the reasonableness of the security measures. An objective assessment of the measures safeguarding the trade secrets can assist in determining the reasonableness under trade secret law. Most importantly, companies should develop a trade secret protection plan in advance of any misappropriation.

So, as a trade secret owner, how do you answer the two questions? How confident are you that your trade secrets are reasonably protected and will survive court scrutiny if that ever becomes necessary?

TAB 7

Commissioner Katharine L. Wade

Katharine L. Wade was appointed as Connecticut's Insurance Commissioner by Gov. Dannel P. Malloy on March 20, 2015. A former Cigna executive, Commissioner Wade has more than 20 years of industry experience and oversees a regulatory agency with jurisdiction over one of the largest insurance industries in the United States.

Her tenure with the Connecticut-based Cigna (1992-2013) is highlighted by an extensive background in leadership, regulatory compliance and consumer outreach.

As Vice President of Public Policy, Government Affairs and U.S. Compliance for Cigna, Commissioner Wade led a 130-member national team responsible for federal and state governmental affairs for Cigna's health, group life and disability businesses. Her responsibilities included oversight for statutory compliance of product and rate filings, regulatory reporting, market conduct examinations and producer licensing.

During the implementation of the federal Affordable Care Act, Commissioner Wade oversaw Cigna's compliance with all ACA's laws and regulations. She directed the team responsible for the creation of Cigna's award-winning ACA outreach campaign – *InformedOnReform* – that delivered timely and accurate information on the federal law to customers, brokers and other key stakeholders.

She oversaw the global health insurer's comprehensive international regulatory review during Supervisory Colleges, a multi-jurisdictional proceeding of U.S. and international insurance regulators. Commissioner Wade also developed the company's public policy structure to deal with its global business units.

As Health Policy Director for Cigna from 1996-2000, her tenure was marked by consumer-focused health care and the creation of an Advocacy Outreach Program. That program served as a resource for a number of constituency groups, including the National Partnership for Women and Families National Woman's Law Center, Bazelon Center for Mental Health Law and the Ovarian Cancer National Alliance.

Commissioner Wade served as the Cigna's liaison to the National Association of Insurance Commissioners. She has held leadership roles with America's Health Insurance Plans (AHIP) and AHIP's State Government Relations Committee, the Connecticut Association of Health Plans and the Association of California Health and Life Insurance Companies.

She earned a Bachelor's of Arts in History from Simmons College in Boston. Commissioner Wade resides in Simsbury with her husband, Mike, and three children.

Matthew Fitzsimmons

Matthew Fitzsimmons is an Assistant Attorney General in Connecticut, heading that Office's Privacy and Data Proteciton Department. He serves as the lead attorney in the Office on all matters involving data security and privacy, most often in relation to data breaches. Most notably, AAG Fitzsimmons served as the lead attorney and negotiator for a thirty-nine state investigation of a top technology company's WiFi data collection, which matter was settled in early 2013. AAG Fitzsimmons has also served in a lead role investigating and negotiating multistate matters with other top internet and technology companies, including the two leading social networking websites. He also served as co-lead counsel in the first-ever state enforcement action (under the HITECH Act of 2009) for alleged violations of HIPAA. During his career as an Assistant Attorney General, AAG Fitzsimmons has litigated an array of complex matters involving violations of the Connecticut Unfair Trade Practices Act in state and federal court, and has also argued on behalf of the State in numerous bankruptcy cases in several states where consumer protection laws and policies are implicated.

In 2011, Attorney General Jepsen appointed AAG Fitzsimmons to lead a multidisciplinary Privacy Task Force to educate the public about data protection and to focus the office's response to Internet privacy concerns and data breaches that affect consumers.

In March 2015, Attorney General George Jepsen created a dedicated and permanent Privacy and Data Security Department within the Connecticut Attorney General's Office and appointed AAG Fitzsimmons as its Department Head. The formation of an official Department was in part to ensure that the privacy and data security work of the office maintains the high level of excellence and cutting edge commitment it receives today by dedicating staff to work exclusively on privacy-related matters. Like the Task Force before it, the new Department will be responsible for all investigations involving consumer privacy and data security. It will also help to educate the public and business community about their responsibilities, which include protecting personally identifiable and sensitive data and promptly notifying affected individuals and the Office of the Attorney General when breaches do occur.

AAG Fitzsimmons is a frequent guest speaker and panelist at industry and continuing legal education events on the topic of data privacy and security, and has contributed to panel discussions in the United States and Canada. Recently, AAG Fitzsimmons was named one of Connecticut Magazine's "Forty under 40" and Connecticut Law Tribune's "New Leaders in the Law" for 2012.

AAG Fitzsimmons also serves as Adjunct Professor at the University of Connecticut School of Law, where he teaches oral advocacy and brief writing as part of the school's Moot Court program. AAG Fitzsimmons received his B.A., *magna cum laude*, from the University of Hartford and his J.D., *with honors*, from the University of Connecticut School of Law.

A&M TEAM BIO

Art Ehuan

Managing Director

aehuan@alvarezandmarsal.com
571-331-7763

- Art Ehuan has extensive industry and law enforcement experience in the field of cyber and risk advisory services. He has a specialization in strategic risk advisory services, including incident response, vulnerability assessments and cyber program development for corporate and government agencies. Mr. Ehuan also serves as a lecturer on cyber crime/terrorism for the U.S. State Department, Diplomatic Security Service, Anti-Terrorism Assistance Program. In this capacity he has lectured on cyber threat to nation-state critical infrastructure to include Advanced Persistent Threat (ATP), Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS).
- Prior to joining A&M, Mr. Ehuan was Managing Director at Forward Discovery, a boutique cyber security firm. Mr. Ehuan also served as Assistant VP and Director of the Corporate Information Security Department for USAA, a Fortune 200 financial/insurance services company. He was responsible for worldwide enterprise and strategic/risk guidance on the protection of USAA information from external/internal threats.
- Among Mr. Ehuan's high-profile corporate positions was Deputy Chief Information Security Officer for the Northrop Grumman Corporation. He was responsible for protecting data from internal and external cyber threats, developing and managing security operations and implementing a corporate digital investigative unit. Mr. Ehuan was also a Federal Information Security Team Manager for BearingPoint (formerly KPMG Consulting), where he established information security initiatives and solutions for government and corporate organizations, as well as developing BearingPoint's corporate incident response and digital forensic services. In addition, Mr. Ehuan served as the Program Manager for Cisco Systems Information Security, where he was responsible for securing corporate networks, managing risk assessments, protecting source code and developing Cisco's worldwide digital forensic capability.
- As a law enforcement officer, Mr. Ehuan has worldwide experience working on cases involving computer crimes. His extensive background conducting and managing computer intrusion and forensic investigations with the Federal Bureau of Investigation (FBI) led to his assignment as a Supervisory Special Agent assigned to the Computer Crimes Investigations Program at FBI Headquarters in Washington, D.C. In addition, he served as a Computer Analysis Response Team Certified Examiner, where he developed and conducted training for law enforcement globally. Mr. Ehuan served as a computer crime Special Agent for the Air Force Office of Special Investigations (AFOSI), where he investigated cyber crime against the network systems of the U.S. Department of Defense. Mr. Ehuan has also testified in Federal, State and Military courts in cases involving digital forensics.
- Mr. Ehuan has received industry credentials including: EnCase® Certified Examiner (EnCE®), Certified Information Systems Security Professional (CISSP) He also maintains the Information Assessment Methodology (IAM) credentials with the National Security Agency (NSA).
- Mr. Ehuan was previously an Adjunct Professor/Lecturer at George Washington University, Georgetown University and Duke University where he taught courses on cyber crime, incident response, digital investigations and computer forensics. He is a contributing author of Techno-Security's Guide to E-Discovery and Digital Forensics from Elsevier Publishing.

Scott Harrison

Managing Director

Washington DC

Phone: 703-967-0339
E-mail Address:
srharrison@alvarezandmarsal.com

- Scott Harrison is a Managing Director with Alvarez & Marsal Insurance and Risk Advisory Services. He serves as a trusted advisor to insurance companies and their strategic partners seeking regulatory, compliance and corporate governance solutions.
- For nearly 25 years, Scott has helped companies improve operations, manage their businesses and mitigate risk in a rapidly changing regulatory environment. He provides counsel on business and public affairs strategies, issue advocacy, corporate governance, the development of regulatory and legislative policy and market regulation/compliance. National insurance companies, banks and trade associations are among Scott's key clients.
- Scott serves as Executive Director for the Affordable Life Insurance Alliance (ALIA), an independent insurance trade association with the mission to fundamentally reform state laws and regulations governing life insurance reserves.
- He has also represented a group of life insurance companies on complex reserve valuation issues before states and the National Association of Insurance Commissioners. This initiative resulted in the ongoing effort to replace the current valuation system with a principles-based approach.
- Scott has worked as Deputy Superintendent of the New York State Insurance Department and as Deputy Commissioner of the Delaware Insurance Department.
- Additionally, Scott served as interim Chief Compliance Officer for a Fortune 500 life and health insurance company and as partner at KPMG LLP where he managed the firm's national insurance regulatory practice. He was on the Board of Directors of a New York life insurance company as a member of its Audit and Investment committees.
- Scott holds a J.D. from Suffolk University Law School and a B.A. in Political Science from Gordon College. He is admitted before the Supreme Court of the United States and is licensed to practice law in the District of Columbia and in the state and federal courts of Delaware, Massachusetts and Pennsylvania.
- Scott is a frequent speaker before insurance groups and associations on compliance, privacy and the emerging issues concerning the financial services industry.

Morgan Lewis

MARK L. KROTOSKI
PARTNER

mkrotoski@morganlewis.com

Silicon Valley Phone **+1.650.843.7212** Fax **+1.650.843.4001**

2 Palo Alto Square \\ 3000 El Camino Real, Ste. 700 \\ Palo Alto, CA 94306-2121 \\ United States

Washington, DC Phone **+1.202.739.5024** Fax **+1.202.739.3001**

1111 Pennsylvania Ave. NW \\ Washington, DC 20004-2541 \\ United States

Mark L. Krotoski represents and advises clients on antitrust cartel investigations; cybersecurity and privacy matters; trade secret, economic espionage, fraud, and foreign corrupt practices cases; and government investigations. With nearly 20 years of experience as a federal prosecutor and a leader in the US Department of Justice (DOJ), Mark provides clients with a unique blend of litigation and investigative experience. He has tried 20 cases to verdict and successfully argued appeals before the US Court of Appeals for the Ninth and Sixth Circuits.

During nearly 20 years as a federal prosecutor, Mark handled a variety of complex and novel investigations and high-profile cases. As the assistant chief of the National Criminal Enforcement Section in the DOJ's Antitrust Division, he oversaw international criminal antitrust cartel investigations and successfully led trial teams in prosecuting antitrust and obstruction of justice cases involving corporations and executives. He also provided guidance on electronic evidence and forensic issues.

Mark served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, which involved approximately 250 federal prosecutors specially trained to prosecute cybercrime and intellectual property enforcement cases. He successfully prosecuted and investigated virtually every type of computer intrusion, cybercrime, and criminal intellectual property violation.

As chief and deputy chief of the Criminal Division in the US Attorney's Office for the Northern District of California, he supervised cases involving white collar crime, securities fraud, computer intrusion, intellectual property, organized crime, and antiterrorism. While serving as a Special Assistant Attorney General in California, Mark was counsel of record on 10 amicus briefs filed in the US Supreme Court on criminal justice matters.

He is a former law clerk to Judge Procter R. Hug Jr. of the US Court of Appeals for the Ninth Circuit and Chief Judge William A. Ingram of the US District Court for the Northern District of California.

Mark frequently speaks at national and international conferences on topics involving criminal antitrust enforcement, cybersecurity, cybercrime, and trade secret issues, as well as the use of electronic evidence in investigations and at trial.

SELECTED REPRESENTATIONS

Note: This list includes engagements completed prior to joining Morgan Lewis.

Criminal Antitrust Cases

- Lead counsel on the conviction of an executive for agreeing on bids and prices for automotive instrument panel clusters sold to an automobile manufacturer
- Led a team on the conviction of a former executive and company director for obstructing an automotive parts investigation
- Lead counsel for the retrial of a former airline executive concerning the price fixing of fuel surcharge rates on air cargo shipments from Miami to South America; five days before trial, a guilty plea was entered
- Lead counsel concerning other investigations involving price fixing, bid rigging, and market allocation among international corporations in the automotive parts and air cargo industries

Economic Espionage and Trade Secret Misappropriation

- Obtained the first conviction in the United States involving source code under the Arms Export Control Act and International Trafficking in Arms Regulation and the first sentencing under the Economic Espionage Act of 1996 for foreign economic espionage involving the misappropriation of a trade secret with intent to benefit a foreign government (under 18 U.S.C. § 1831)
- Co-counsel in a case that resulted in a foreign economic espionage conviction involving the misappropriation of trade secrets with the intent to benefit foreign instrumentalities (under 18 U.S.C. § 1831)
- Following an international investigation, filed charges against a foreign national for computer intrusions involving NASA and a leading provider of computer network equipment and theft of trade secrets involving source code
- Lead counsel in the investigation and conviction of a company vice president for the theft of trade secrets from his former employer, a Fortune 15 company
- Led other criminal convictions and investigations involving the misappropriation of trade secrets from international, medium, and small companies

Cyber and Data Security, Unauthorized Access, Computer Intrusions, Cybercrime

- Co-counsel in a jury trial that led to a conviction concerning the intrusion into the Yahoo! account of Alaska Governor Sarah Palin and obstruction of justice; argued the appeal before the U.S. Court of Appeals for the Sixth Circuit, which affirmed the convictions (*United States v. Kernell*, 667 F.3d 746 (6th Cir. 2012))
- Obtained a jury trial conviction concerning a computer intrusion "time bomb" that corrupted more than 50,000 company records (*United States v. Shea*, 493 F.3d 1110 (9th Cir. 2007))
- Obtained a computer intrusion conviction involving high-technology companies *(United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007))
- Led numerous other prosecutions and investigations of computer intrusions, computer fraud, cybercrime, and the obstruction of justice

Other Intellectual Property Enforcement Cases

- Lead counsel on an undercover investigation, which culminated in the largest CD and DVD manufacturing piracy scheme prosecuted in the United States at the time and convictions of three key manufacturers for copyright, trademark, counterfeit labels, and FBI seal violations
- Following an undercover investigation concerning an Internet "warez" conspiracy involving pirated movies, games, and software, coordinated approximately 40 searches simultaneously executed across the United

States with other searches outside the country and developed case strategies resulting in 30 convictions in one year, with 40 total convictions for various criminal copyright violations
- Obtained the first convictions under a new federal "camming" statute (unauthorized recording of motion pictures in a motion picture exhibition facility) and a new statute for uploading prereleases on the Internet (criminal copyright infringement by distributing a copyrighted work on a computer network)
- Obtained the first conviction in California and the second in the United States under the Digital Millennium Copyright Act (DMCA)
- Obtained convictions for the unauthorized manufacture and distribution of satellite television access devices and DMCA violations as part of a satellite piracy scheme, including manufacturing and distributing software and devices that were used to steal satellite programming
- Multiple other DMCA convictions and investigations

AWARDS AND AFFILIATIONS

Award of Distinction, Assistant Attorney General, Antitrust Division

Distinguished Service Award, Assistant Attorney General, Criminal Division

Executive Office of the United States Attorneys Director's Award for Superior Performance as an Assistant U.S. Attorney

Recipient, William J. Schafer Award of Excellence from the Association of Government Attorneys in Capital Litigation (for U.S. Supreme Court amicus briefs)

Member, American Bar Association, Antitrust Law Section

Member, American Society for Industrial Security (ASIS)

Member, Sedona Working Group

Computer Hacking and Intellectual Property (CHIP) Prosecutors Working Group (2007–2011)

Bencher, William A. Ingram Inn, American Inn of Court (2006–2007)

Member, Criminal Rules and Practice Committee, U.S. District Court for the Northern District of California (2006–2007)

ADMISSIONS

- California
- District of Columbia
- U.S. Supreme Court
- U.S. Court of Appeals for the Ninth Circuit
- U.S. District Courts for the Northern, Eastern, Central, and Southern Districts of California

CLERKSHIPS

- Clerkship to Chief Judge William A. Ingram of the U.S. District Court for the Northern District of California
- Clerkship to Judge Procter R. Hug, Jr. of the U.S. Court of Appeals for the Ninth Circuit

EDUCATION

- Georgetown University Law Center, 1986, J.D.
- University of California, Los Angeles, 1980, B.A., Magna Cum Laude

SERVICES

- Antitrust & Competition
- Privacy & Cybersecurity

REGIONS

- North America

- Trade Secrets, Proprietary Information & Noncompetition/ Nondisclosure Agreements
- Brand & Product Innovation
- Trademark, Copyright, Advertising & Unfair Competition
- White Collar Litigation & Government Investigations
- Intellectual Property

Morgan Lewis

DANIEL S. SAVRIN
PARTNER

daniel.savrin@morganlewis.com

Boston Phone **+1.617.951.8674** Fax **+1.617.428.6310**

One Federal St. \\ Boston, MA 02110-1726 \\ United States

Daniel S. Savrin is a skilled trial lawyer who has represented clients in civil and criminal litigation in federal and state courts in 35 states, the District of Columbia and Puerto Rico, in internal and government investigations, in numerous arbitrations and before foreign authorities. His broad litigation and counseling practice focuses on antitrust, white collar defense and government enforcement matters, and complex commercial disputes.

Daniel has been recognized as a leading litigator and counselor both for his extensive experience in handling and trying civil and criminal matters and his practical and effective approaches to litigating and resolving disputes with government agencies and among private parties. He represents major national and international corporations, professionals, and other high-profile clients in litigating and resolving their difficult legal problems.

- Daniel's antitrust and consumer protection practice includes the representation of individuals and corporations in criminal antitrust matters; civil enforcement matters; individual and class action civil litigation; merger-related proceedings and litigation; and counseling on general and industry specific consumer protection and and antitrust matters.
- Daniel's white collar defense and government enforcement practice includes the representation of both individuals and corporate entities in federal and state criminal and civil enforcement proceedings, the defense of enforcement actions brought by state attorneys general, the defense of health care fraud and abuse and other qui tam matters, the conduct of internal investigations, and the implementation of regulatory compliance programs.
- Daniel's complex commercial litigation practice involves a wide range of civil and class action matters in a variety of areas, including, among others, consumer protection, finance, insurance, and health care matters.
- Before joining Morgan Lewis, Daniel was a partner in the antitrust and trade regulation practice at another international law firm.

SELECTED REPRESENTATIONS

Note: This list includes engagements completed prior to joining Morgan Lewis.

Antitrust Matters

-

Cumberland Truck Equipment Co. v. Detroit Diesel Corporation — Represented Detroit Diesel in two class actions alleging that Detroit Diesel conspired with its distributors in violation of Section 1 of the Sherman Act. The case was settled.

- *In re New Motor Vehicles Canadian Export Litigation* — Represented BMW of North America, LLC and BMW Canada, Inc. in MDL and related state litigation concerning an alleged conspiracy and group boycott designed to restrain the export of new motor vehicles from Canada to the United States. After a series of dismissals on the merits in a number of state court proceedings and dismissals of BMW Canada on personal jurisdiction grounds, voluntary dismissals were secured of all remaining federal and state claims.
- *In re New Motor Vehicles Canadian Export Antitrust Litigation* — Defended Nissan North America, Inc., Nissan Canada, Inc. and Nissan Motor Co., Ltd. in the series of related federal and state antitrust cases concerning Canadian new motor vehicles exports. Secured judgments in three state proceedings after which the claims in the remaining states were voluntarily dismissed.
- *State of Connecticut v. Marsh and McLennan Companies, Inc., et al* — Defended reinsurance broker against a lawsuit by the Connecticut attorney general alleging that the reinsurance broker engaged in decades-long antitrust conspiracy involving the sale of reinsurance through reinsurance facilities and other reinsurance marketing practices. The case was settled.
- Representation of executives and corporations in various grand jury antitrust investigations of international cartel activities and parallel or related class action litigation
- Representation of clients being investigated by the Department of Justice, the Federal Trade Commission and state antitrust enforcement agencies
- Representation of parties in merger and acquisitions, joint ventures, joint bidding arrangements and other transactions

White Collar Defense and Government Enforcement Matters

- Defended corporation in grand jury investigation of false claims act violations related to "Big Dig" construction project. The investigation terminated with no charges being filed.
- Defense of numerous healthcare providers and individuals with respect to Medicare and Medicaid false claims action violations. Resolved matters civilly or secured closure of investigations with no civil or criminal liability
- Defense of numerous corporations with respect to state attorneys general investigations involving consumer protection, deceptive advertising, Internet advertising practices, pricing and antitrust matters
- Represented corporate executive in investigation of environmental crimes at unpermitted demolition site. The investigation terminated with no charges being brought against the executive.
- Represented healthcare providers in drug diversion investigations and litigation
- Conducted internal investigations related to business practices and financial reporting
- Representation of clients in audits of Bank Secrecy Act and anti-money laundering compliance audit and investigation
- Counseling and representation of parties with respect to alcoholic beverage sale and distribution strategy and compliance matters

Commercial Litigation Matters

- *The Great Atlantic and Pacific Tea Company v. The Stop & Shop Supermarket Company, LLC, et al* — Representation of major supermarket in Lanham Act litigation in challenge to its comparative advertising campaign highlighting clients' lower pricing. Injunction denied.
- Representation of retailers in class action litigation challenging promotions and advertising practices
- Representation of major insurance broker in investigations and individual litigation matters
- Defense of financial and securities firms in arbitration matters relating to financial products and marketing practices
- *National Ass'n of Chain Drug Stores, et al, v. New Eng. Carpenters Health Benefits Fund*, 582 F.3d 30 (1st Cir. 2009) — Representation of leading healthcare trade associations in District Court and appellate challenges

to efforts, through a class action settlement, to alter the reported pharmaceutical average wholesale price (AWP)

AWARDS AND AFFILIATIONS

- Editorial Board, Consumer Protection Law Developments 2011 Update (ABA Section of Antitrust Law)
- Co-chair, New England/Boston Region of the ABA White Collar Crime Committee
- American Bar Association
- Boston Bar Association
- Massachusetts Bar Association
- *Best Lawyers*, leading lawyer in Antitrust (2006–2014)
- *Chambers USA*, leading lawyer in Antitrust (Massachusetts) (2008–2014)
- *Super Lawyers*, Massachusetts (2005–2009); Antitrust Litigation (2010–2011)

ADMISSIONS

- Massachusetts
- New York
- Massachusetts Supreme Judicial Court
- US Court of Appeals for the First Circuit
- US District Court for the District of Massachusetts

EDUCATION

- Union College, 1984, Bachelor of Arts
- University of Virginia School of Law, 1989, Juris Doctor

SECTORS

- Retail
- Life Sciences

SERVICES

- Commercial Litigation
- Antitrust & Competition
- Litigation, Regulation & Investigations
- Class Actions
- Healthcare Regulatory & Litigation
- Privacy & Cybersecurity
- White Collar Litigation & Government Investigations
- Trademark, Copyright, Advertising & Unfair Competition