crowell moring

Managing the Cyber Threat Crisis: An Interactive Workshop on Cyber Threats and Cyber Security

April 4, 2013

crowell moring

Managing the Cyber Threat Crisis

Cyber Threats & Enforcement Risks for Corporate Boards & Officers

David Z. Bodenheimer

crowell moring

Signs of the Cyber Apocalypse

Is the Cyber Threat Real?

(or Just Phony Politics?)

"pork-hungry politicians"

"no substantive basis" for cyber threats

"ulterior motives and conflicts of interest"


TIMOTHY P. CARNEY

Cybersecurity pork

Companies get rich as lobbyists peddle fear of a vague threat. P. 17

POLITICS

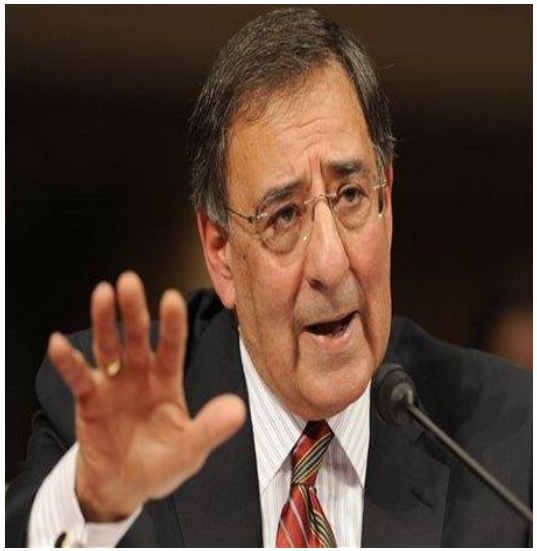
The rise of the cybersecurity-industrial complex

"The $100 billion Washington will spend on cybersecurity in the next decade may be less about guarding America from a real threat, and more about enriching revolving-door lobbyists and satisfying **pork-hungry politicians**."

"'The notion that our power grid, air traffic control system, and financial networks are rigged to blow at the press of a button would be terrifying if it were true,' Brito and Watkins write. "But fear should not be a basis for public policymaking.' The public has been given **no substantive basis** for such fears." [Carney, *The Washington Examiner (*Apr. 28, 2011)]

Digital Pearl Harbor

DoD Secretary Panetta



"cyber Pearl Harbor" (2012)

DHS Secretary Napolitano

"cyberattack" data like 9/11 (2012)

FBI Director Mueller

"greatest threat to our country" (2012)

Cyber $$ Meltdown

EU Cyber Warning

"According to the World Economic Forum, there is an **estimated 10% likelihood** of a major critical information infrastructure breakdown in the coming decade, which could cause **damages of $250 billion.**"

EUROPEAN COMMISSION

European Union
EXTERNAL ACTION

PRESS RELEASE

Brussels, 7 February 2013

Cyber 9/11 on Banks

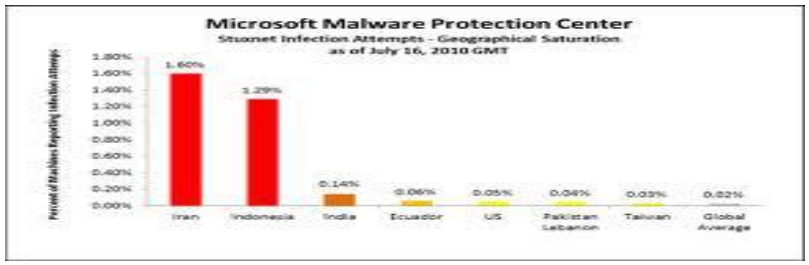
(8) According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a United States bank, the economic consequences would have been "an order of magnitude greater" than those cased by the physical attack on the World Trade Center. Mike McConnell has subsequently referred to cybersecurity as the "soft underbelly of this country".

Real-World Cyber Attacks

Stuxnet Attack

Nuclear Facility Attack. Penetrated & sabotaged control systems at Iranian **Bushehr nuclear power facility**
[Senate Stuxnet Hearings (Nov. 17, 2010)]

- Military-grade "cyber missile"
- Exploited **4 "zero-day"** vulnerabilities
- Employed stolen digital certificates
- Took months & **millions $$** to build



Pipeline Explosion

Pipeline Attack. "A previous historic example includes a reported case of stolen code that impacted a pipeline. In this case, code was secretly 'Trojanized' to function properly and only some time after installation it instructed the host system to increase the pipeline's pressure beyond its capacity. This resulted in a **three kiloton explosion, about one-fifth the size of the Hiroshima bomb**."

[*Securing Critical Infrastructure in the Age of Stuxnet: Hearings before Sen. Comm. on Homeland Security* (Nov. 17, 2010)]

crowell moring

Cyber Theft & Espionage: Why Corporate Boards & Officers Need to Worry

Secrets Gone?

Cyber Theft & Espionage

Intelligence Warnings

The loss of intellectual property due to cyber attacks amounts to the "**greatest transfer of wealth in human history.**"

(Gen. Keith Alexander, U.S. Cyber Command Chief & NSA Director, July 2012)

More Warnings

- Counterintelligence Executive Report (Oct. 2011)
- GAO Report & Testimony (June 2012)
- Defense Security Service Trend Analysis (2012)
- National Intelligence Estimate (2013)
- Mandiant Investigative Report (2013)

Foreign Cyber Threats

Foreign Cyber Threats

- **40,000 Hackers:** "There are forty thousand Chinese hackers who are collecting intelligence off U.S. information systems and those of our partners." (Adm. McConnell, Jan. 2008)
- **Daily Attacks.** "A defence force source said yesterday that attacks initiated from China occurred almost on a daily basis." (Australian Defense Force, Apr. 2009)
- **Classified Data Compromised.** "A China-based cyber espionage network had accessed 1200 computers in 103 countries containing classified documents." (Munk Centre for Int'l Studies, Apr. 2009)

China's Cyber Spy House

FIGURE 7: Unit 61398 Center Building 208 Datong (rear view, possible generator exhausts visible) Image Copyright 2013 city8.com

Data Losses & Cyber Breach

2x Library of Congress

➔ 38 terabytes of lost data

"As an example of the threat, one American company had **38 terabytes** of sensitive data and intellectual property exfiltrated from its computers – equivalent to nearly double the amount of text contained in the Library of Congress."
[Sen. Whitehouse, May 10, 2010]

2 x

It's Personal

"As an example, in 2008, [China's] APT1 compromised the network of a company involved in a wholesale industry. . . . Over the following 2.5 years, APT1 stole an unknown number of files from the victim and repeatedly **accessed the email accounts** of several executives, including the **CEO and General Counsel**."

[Mandiant Report (Feb. 2013)]

IP Cyber Losses

One Company's IP Loss

"For example, a 2011 FBI report noted, "company was the victim of an intrusion and **lost 10 years' worth of research and development data –valued at $1 billion** – virtually overnight."

CRS Report, *2013 Cybersecurity Executive Order* (Mar. 2013)

$1 Trillion IP Losses

"Last year alone, cyber criminals stole intellectual property from businesses worldwide worth up to **$1 trillion**." (President Obama, 2009)

Stock Price Losses

Investors Really Care

- **70%** of investors – interested in reviewing corporate cyber practices
- **80%** of investors – likely would not invest if history of cyber attacks

Zogby Analytics Survey (Mar. 2013)

Stock Prices Hammered

- **9% Stock Loss** – after Global Payments breach (before trading halted)
- **84% Stock Loss** – after Chinese firm took AMSC's source code

Cybered M&A Deals

Infiltrated M&A Deals

- **$2.4 Billion Huiyuan Deal.** Coca Cola's deal collapsed after hackers took key files
- **$40 Billion BHP Deal.** BHP Billiton Ltd's bid to acquire Potash Corp. collapsed after cyber theft

"Coke Gets Hacked and Doesn't Tell Anyone," *Bloomberg.com* (Nov. 2012)

Nat. Counter Intel Report

"Information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm . . . . [T]his may have helped the Chinese firm attain a better negotiating and pricing position." [National Counter-intelligence Executive, Oct. 2011]

Cybered Negotiations

$1.3 Billion Left on Table

"In one case, officials estimated the **cost of lost data** from a British company . . . . Jonathan Evans, head of Britain's MI5 domestic security service, said . . digital intruders targeting a 'major London listed company' had caused a **loss of 800 million pounds ($1.3 billion)**, in part because of the resulting disadvantage in 'contractual negotiations.'"

"China-Based Hacking of 760 Companies Shows Cyber Cold War," *Bloomberg.com* (Dec. 2011)

Double-Digit Losses

After China's APT1 compromised the network of a company in the wholesale industry, "major news organizations reported that China had successfully negotiated a **double-digit decrease in price per unit** with the victim organization for one of its major commodities."

Mandiant Report (Feb. 2013)

Cybered Operations

30,000 Dead Computers

"In August 2012, a series of cyber attacks were directed against Saudi Aramco, the world's largest oil and gas producer and most valuable company. The attacks **compromised 30,000 of the company's computers** and the code was apparently designed to disrupt or halt the production of oil."

[CRS, *2013 Cybersecurity Executive Order,* Mar. 2013]

Iranian Cyber Attacks

Bank of America & J.P. Morgan Chase Cyber Attacks. "'I don't believe these were just hackers,'" [Sen.]Lieberman said . . . . "'I believe this was **done by Iran** and the Qods force, which has its own developing cyber attack capacity.'"

"In a 'highly classified' report last week the Joint Chiefs of Staff's Intelligence Directorate, or J-2, confirmed continuing **Iranian cyber attacks against U.S. financial institutions**, NBC said."

[Matt Egan, *FoxBusiness,* Sept. 24, 2012]

crowell moring

How Do You Know When Your Company is a Cyber Target?

Who's a Cyber Target?

- **McAfee Survey**

  60% reported "chronic and recurring loss" of sensitive information

- **CSIS Report**

  85% energy/power sector experienced "network intrusions"

- **Mandiant Report**

  141 companies in 20 major industries compromised by cyber intrusions (as confirmed by Mandiant investigations)

2 Types of Companies

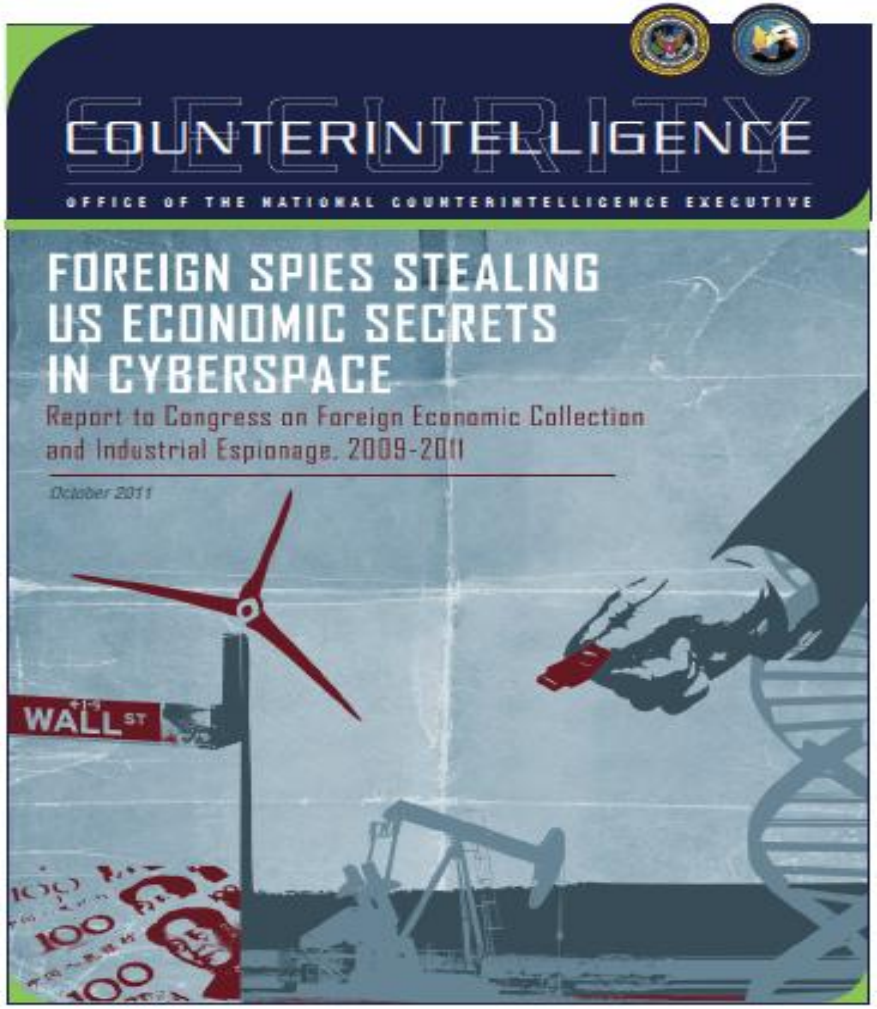
"There are only two types of companies: Those that have been hacked, and those that will be. Even that is merging into one category: Those that have been hacked and will be again."

FBI Director Robert Mueller (Mar. 2012)

Who's a Cyber Target?

Top Cyber Targets

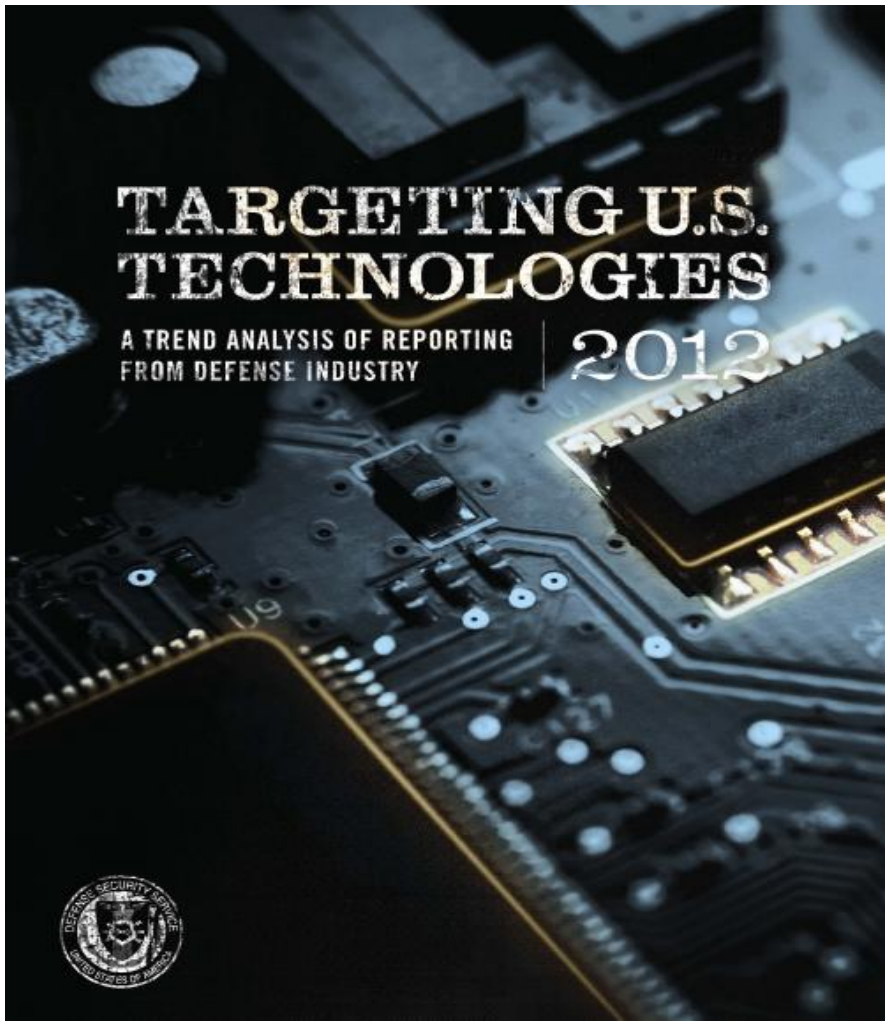
- Information Technology
- Communications
- Military Technology
- Aerospace
- Dual Use Technology
- Healthcare & Pharma
- Agricultural Technology



Who's a Cyber Target?

TOP TARGETED TECHNOLOGIES*

- INFORMATION SYSTEMS
- LASERS, OPTICS, AND SENSORS
- AERONAUTICS SYSTEMS
- ELECTRONICS
- ARMAMENTS AND ENERGETIC MATERIALS
- SPACE SYSTEMS
- MARINE SYSTEMS
- POSITIONING, NAVIGATION, AND TIME
- MATERIALS AND PROCESSES
- GROUND SYSTEMS
- INFORMATION SECURITY
- PROCESSING AND MANUFACTURING



Who's Attacking Who?

Who are the Hackers?

- Foreign Nations
- Organized Crime
- Terrorists
- Hactivists
- Hackers for Hire

What are the Targets?

- Cyber Espionage (IP)
- ID Theft (personal data)
- Critical Infrastructure
- Political Disruption
- All of the Above

crowell moring

Who Are the Enforcers Coming After You – After a Security Breach?

Secrets Gone?

Cyber Risks – SEC Scrutiny

SEC Scrutiny

- Disclose material risks?

Impact

➔ SEC scrutiny or actions

"Cyber risk management is a critical corporate responsibility. Federal securities law requires publicly traded companies to disclose 'material' risks and events, including cyber risks and network breaches. A review of past disclosures suggests that a significant number of companies are failing to meet these requirements." [Senate Commerce News Release, May 12, 2011]

U.S. Senate Committee on Commerce, Science, and Transportation

SEC Disclosure Duty

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 Duties

- **Risk of Cyber Incidents**
- **Prior Security Breaches**
- **Adequacy of Preventative Measures**

Cyber Risks – Shareholders

Disclose Risks – Or Not?

➔Rock & a Hard Place?

$20 Million Suit. Countrywide's lax "internal procedures" & security breach [Courthouse News, Apr. 5, 2010]

$7.2 Million/Incident. "average cost of a data breach hit $7.2 million last year" [*NYT*, Dec. 2011]

Shareholder Actions

- Delaware case law (corporate director's good faith duties re information & reporting systems, plus potential liability for damages)
- National Counterintelligence Executive Report (Oct. 2011)

Cyber Risks – Congress

Congressional Inquiry

- **Sen. Rockefeller's Letter**
- **300 CEOs Responded**

Did Your CEO Respond?

- **What did your CEO say?**
- **Is your company doing it?**
- **Will a plaintiff get hold of it?**

United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEB SITE: http://commerce.senate.gov

September 19, 2012

Fortune 500 CEO USA

I was profoundly disappointed that the United States Senate's effort to pass comprehensive cybersecurity legislation was blocked by a partisan filibuster last month. The cyber threats we face are real and immediate, and Congress's failure to pass legislation this year leaves the country increasingly vulnerable to a catastrophic cyber attack. Because of the urgency of the need to address this threat, in August following the Senate's failure to act, I urged President Obama to use his authority to implement cybersecurity protections for our country through an Executive Order.

To help me understand your company's views on cybersecurity, I ask that you provide responses to the following questions by Friday, October 19, 2012.

1. Has your company adopted a set of best practices to address its own cybersecurity needs?
2. If so, how were these cybersecurity practices developed?
3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.

Cyber Risks – Executive Order

Information Sharing

➔ **Should you be sharing?**

Yes?

- Critical for identifying threats
- Essential tool for cybersecurity

No? -- Safe Harbors?

- Investigation due to reporting?
- Lawsuit triggered by sharing?
- Antitrust issue for B-2-B sharing?

Executive Order

The White House

Office of the Press Secretary

For Immediate Release February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

Cyber Risks – Info Sharing

Sharing Data with Feds

What do you say when the Feds come knocking?

- **Authority to share data?**
- **Potential 3rd party liability?**
- **Privacy issues?**

Potential Exposure

- **Attorney-client privilege?**
- **FOIA protection?**
- **Use for other investigations?**

$50 Billion Lawsuit

"One lawsuit alone, filed May 12 by a purported national class of Verizon customers, seeks $50 billion in damages."

["Court Will Decide State Secrets Issues First in NSA Phone Surveillance Class Action Suit," *Privacy Law Watch,* June 9, 2006]

Cyber Risks – FCA Actions

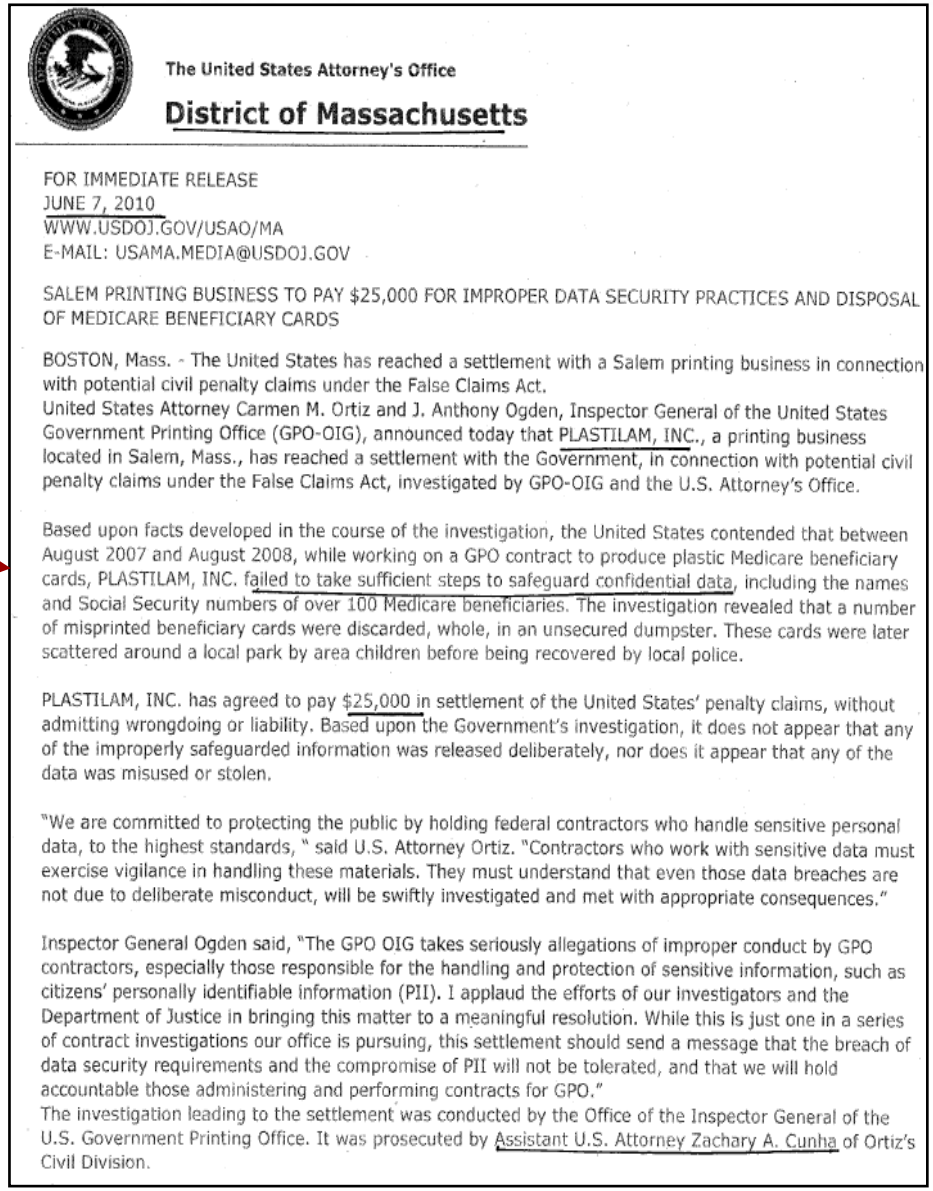
Cyber Fraud Risks

- What did you tell the Federal agency?

Failed Cybersecurity

➔ False Claims Act suit

"PLASTILAM, INC. failed to take sufficient steps to safeguard confidential data, including the names and Social Security numbers of over 100 Medicare beneficiaries. The investigation revealed that a number of misprinted beneficiary cards were discarded, whole, in an unsecured dumpster."



The United States Attorney's Office

District of Massachusetts

FOR IMMEDIATE RELEASE
JUNE 7, 2010
WWW.USDOJ.GOV/USAO/MA
E-MAIL: USAMA.MEDIA@USDOJ.GOV

SALEM PRINTING BUSINESS TO PAY $25,000 FOR IMPROPER DATA SECURITY PRACTICES AND DISPOSAL OF MEDICARE BENEFICIARY CARDS

BOSTON, Mass. - The United States has reached a settlement with a Salem printing business in connection with potential civil penalty claims under the False Claims Act.
United States Attorney Carmen M. Ortiz and J. Anthony Ogden, Inspector General of the United States Government Printing Office (GPO-OIG), announced today that PLASTILAM, INC., a printing business located in Salem, Mass., has reached a settlement with the Government, in connection with potential civil penalty claims under the False Claims Act, investigated by GPO-OIG and the U.S. Attorney's Office.

Based upon facts developed in the course of the investigation, the United States contended that between August 2007 and August 2008, while working on a GPO contract to produce plastic Medicare beneficiary cards, PLASTILAM, INC. failed to take sufficient steps to safeguard confidential data, including the names and Social Security numbers of over 100 Medicare beneficiaries. The investigation revealed that a number of misprinted beneficiary cards were discarded, whole, in an unsecured dumpster. These cards were later scattered around a local park by area children before being recovered by local police.

PLASTILAM, INC. has agreed to pay $25,000 in settlement of the United States' penalty claims, without admitting wrongdoing or liability. Based upon the Government's investigation, it does not appear that any of the improperly safeguarded information was released deliberately, nor does it appear that any of the data was misused or stolen.

"We are committed to protecting the public by holding federal contractors who handle sensitive personal data, to the highest standards, " said U.S. Attorney Ortiz. "Contractors who work with sensitive data must exercise vigilance in handling these materials. They must understand that even those data breaches are not due to deliberate misconduct, will be swiftly investigated and met with appropriate consequences."

Inspector General Ogden said, "The GPO OIG takes seriously allegations of improper conduct by GPO contractors, especially those responsible for the handling and protection of sensitive information, such as citizens' personally identifiable information (PII). I applaud the efforts of our investigators and the Department of Justice in bringing this matter to a meaningful resolution. While this is just one in a series of contract investigations our office is pursuing, this settlement should send a message that the breach of data security requirements and the compromise of PII will not be tolerated, and that we will hold accountable those administering and performing contracts for GPO."
The investigation leading to the settlement was conducted by the Office of the Inspector General of the U.S. Government Printing Office. It was prosecuted by Assistant U.S. Attorney Zachary A. Cunha of Ortiz's Civil Division.

Questions?

David Z. Bodenheimer

Crowell & Moring LLP

dbodenheimer@crowell.com

202.624.2713

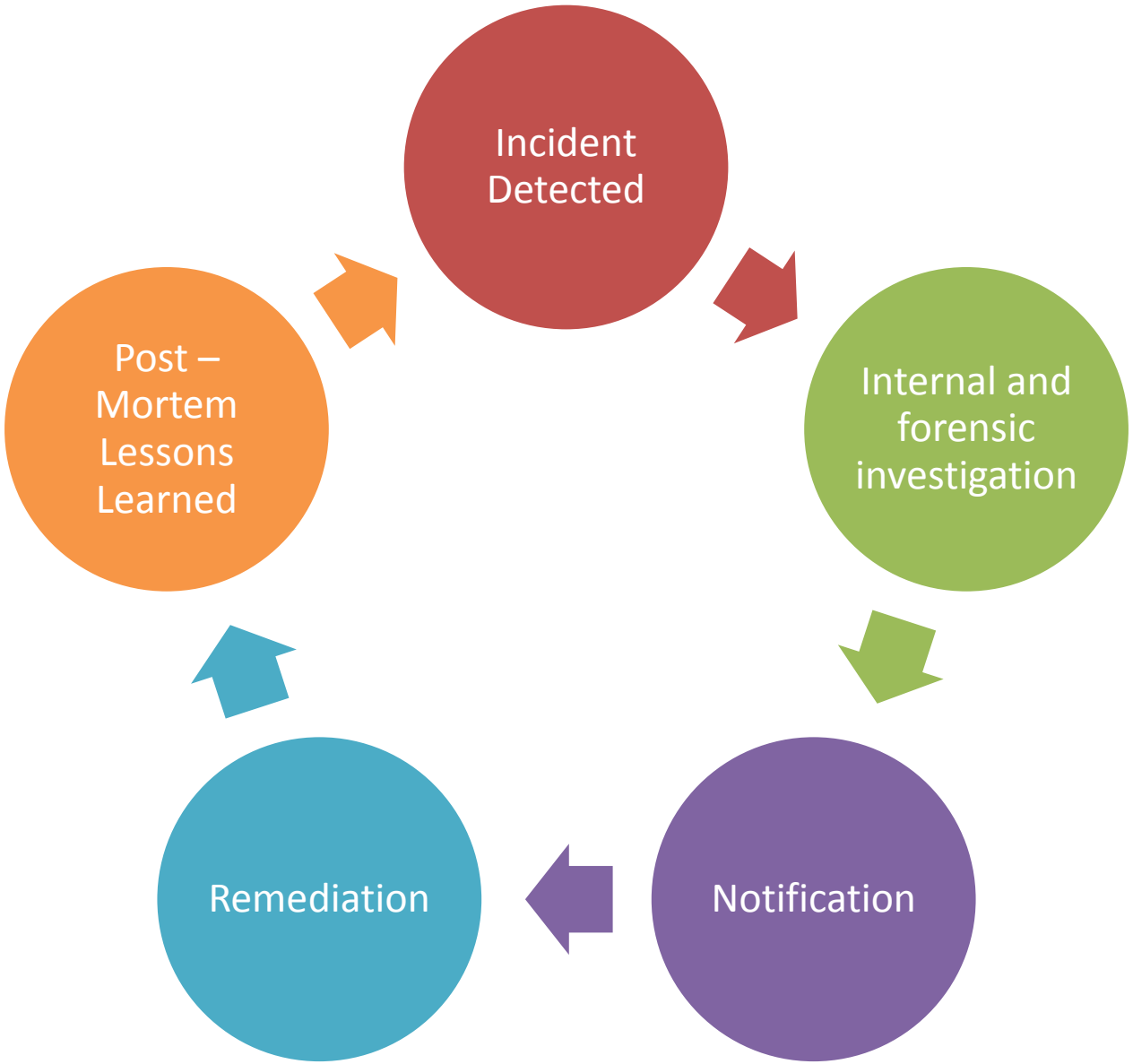
crowell moring

Security Breaches & Crisis Management

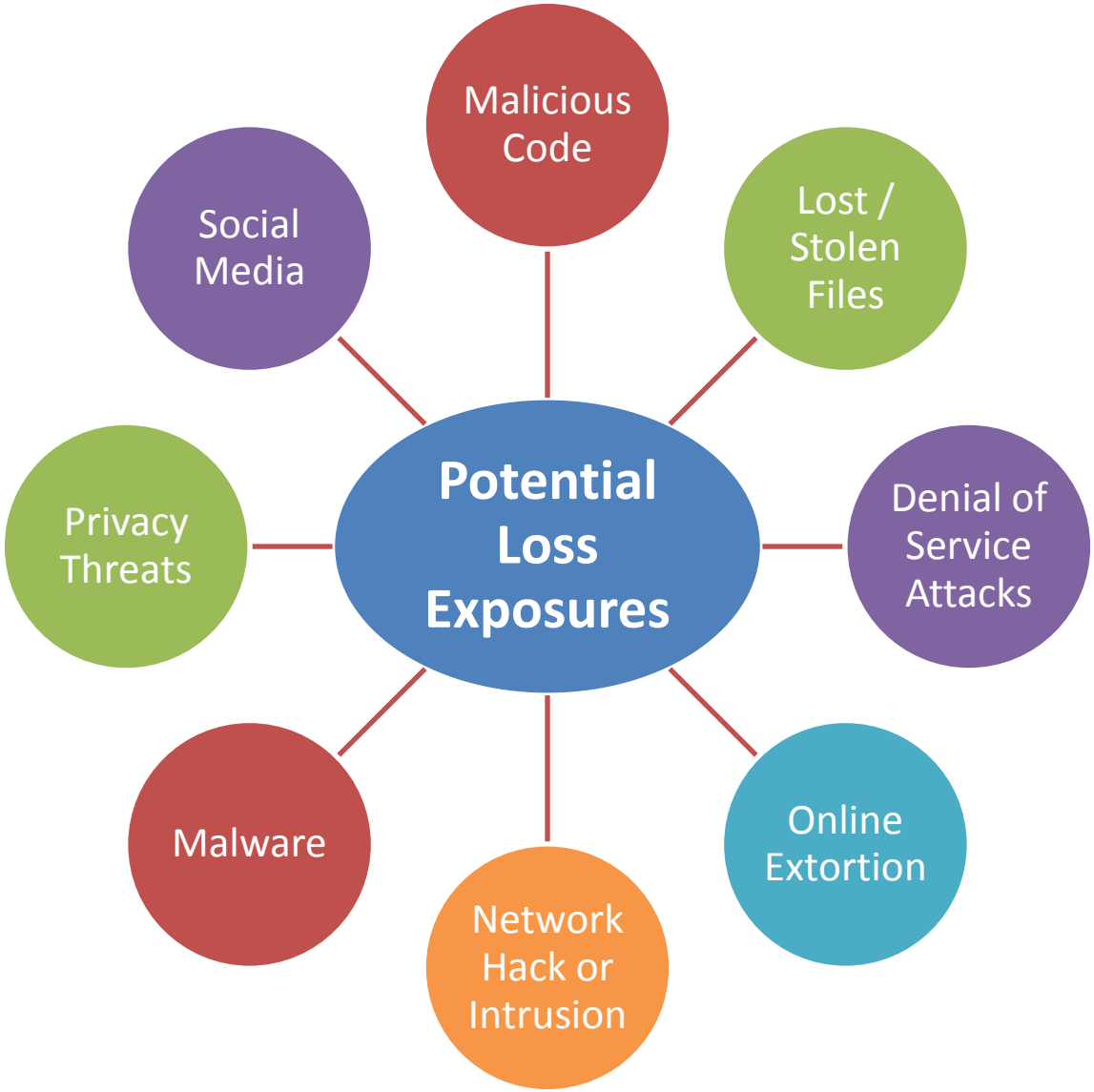
Catherine A. Mulligan
Zurich

Cheryl A. Falvey
Scott L. Winkelman
Crowell & Moring

Your Security Breach Event: The Crisis Response Cycle



Security & Privacy Exposures: Risk Types



Security & Privacy Exposures: Cost Categories

Crisis Management Costs
- legal, public relations, other service fees
- advertising, related communications

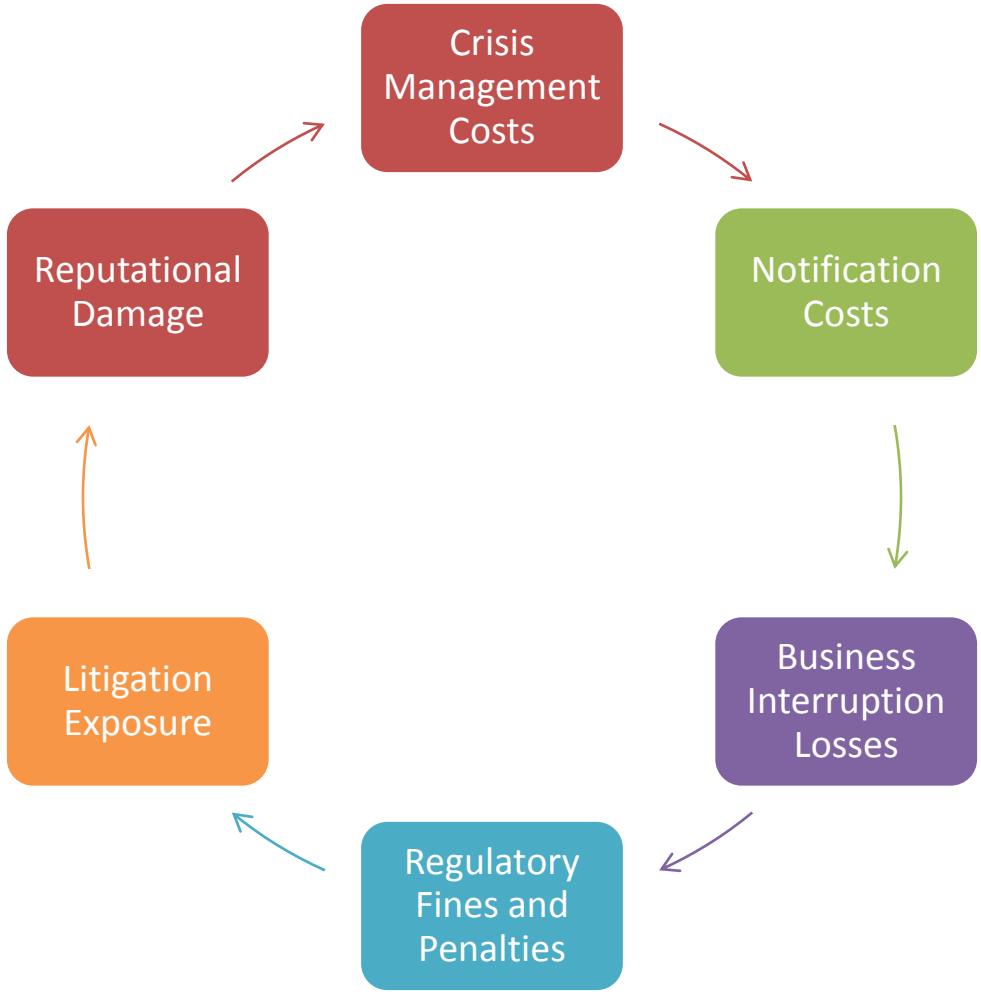
Costs of Notification
- forensic investigation
- credit monitoring services

Business Interruption Losses
- loss of Income
- costs to Recreate Lost or Stolen Data

Regulatory Fines and Penalties

Litigation Exposure
- class/mass litigation
- suits by customers, vendors

Reputational /Broader Business Damage

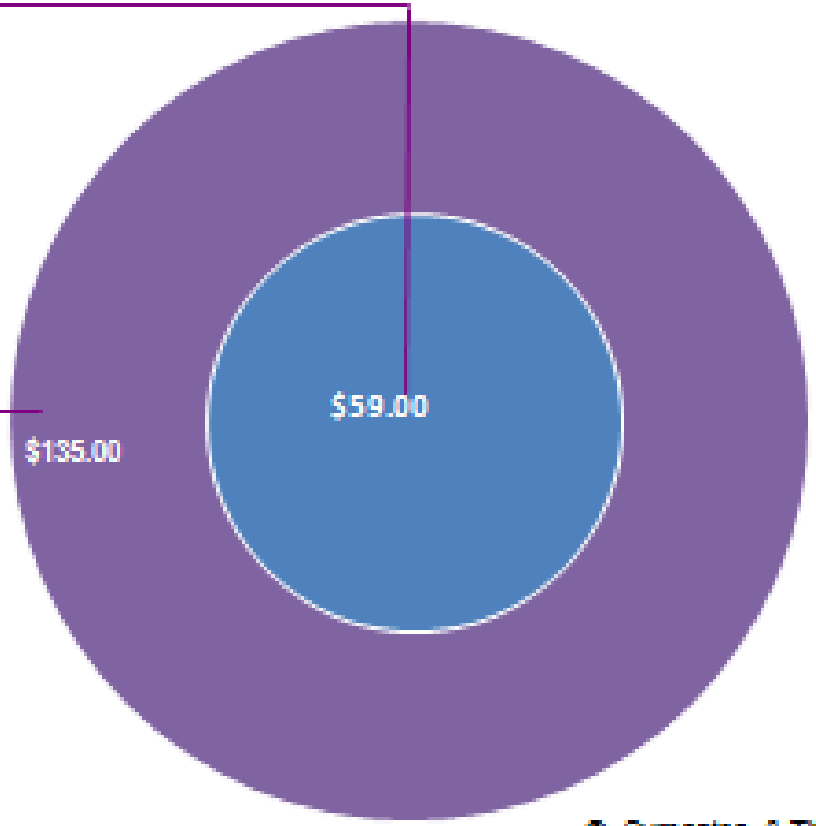


Security & Privacy Exposures: Cost of Breach

Cost per record:
$194 (2011) (down $20 from 2010)

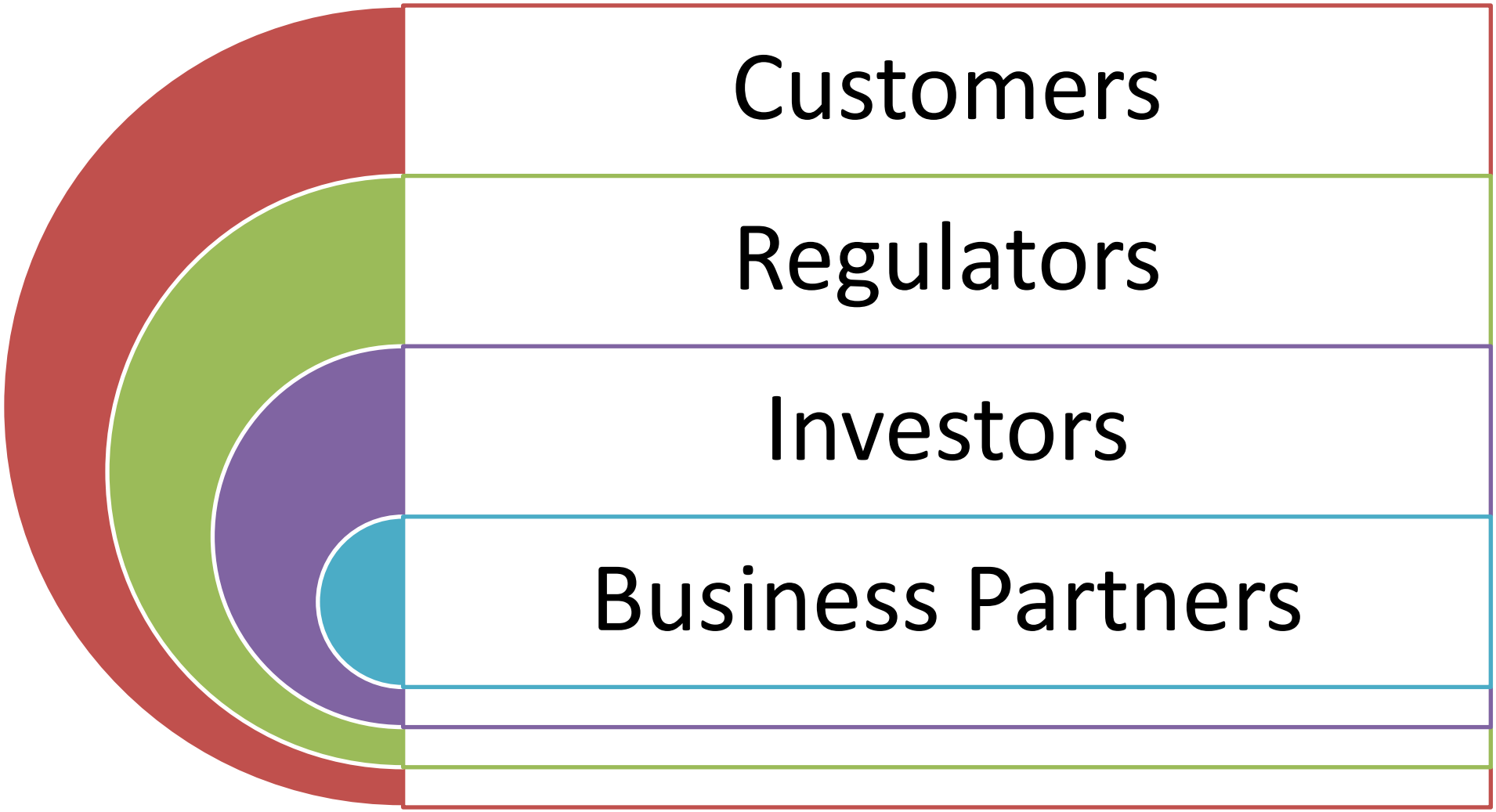
DIRECT COSTS
- Notification
- Call Center
- Identity Monitoring (credit/non-credit)
- Identity Restoration
- Discovery / Data Forensics
- Loss of Employee Productivity

INDIRECT COSTS
- Restitution
- Additional Security and Audit Requirements
- Lawsuits
- Regulatory Fines
- Loss of Consumer Confidence
- Loss of Funding



© Symantec & The Ponemon Institute
2012 US Cost of a Data Breach

Regulatory and Litigation Risks



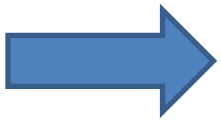
Mitigating Legal Risks

"old school" v. "new school" risks

conventional tort/contract principles apply

- no per se liability for security devices
- key Q: is security breach reasonably foreseeable?
- "standard of care" evolves as technology evolves

industry standards anchor court analysis



ignorance is *not* bliss

prompt responsive action is your best "defense"

Security & Privacy Exposures: Gaps in Traditional Coverage

traditional Property and Casualty policies are seeing more exclusions pointed at Cyber Liability, which widens the potential exposure

CGL	Property	K&R	D&O

data is considered "intangible property" – many traditional property forms only cover tangible property

no express coverage for Privacy Breach Costs which are the loss leader associated with the coverage

Zurich Security & Privacy Protection Policy: Review of Available Coverages

six (6) available coverages

1. Security & Privacy Liability*
2. Privacy Breach Costs Coverage*
3. Business Income and Dependent Business Income Loss Coverage
4. Digital Asset Replacement Expense Coverage
5. Cyber Extortion Threat and Reward Payments Coverage
6. Internet Media Liability

* = *required coverage*

Zurich Security & Privacy Protection Policy: Privacy Breach Cost Coverage

WHAT'S INCLUDED

- Computer Forensic Analysis;
- Determination of Indemnification Obligations under Written Contract with a Service Provider;
- Determination and Notification of Affected Individuals or Regulatory Agencies;
- Compliance with Privacy Regulations;
- Planning, Implementation and Execution of a Public Relations Campaign;
- Credit Monitoring

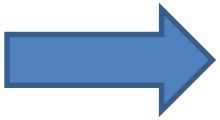
WHAT'S NOT INCLUDED

- Regular or Overtime Wages, Salaries or Fees
- Cost to Comply with Injunctive or Non-Monetary Relief;
- Taxes, Fines or Penalties

What To Do?

"planning without action is futile; action without planning is fatal"

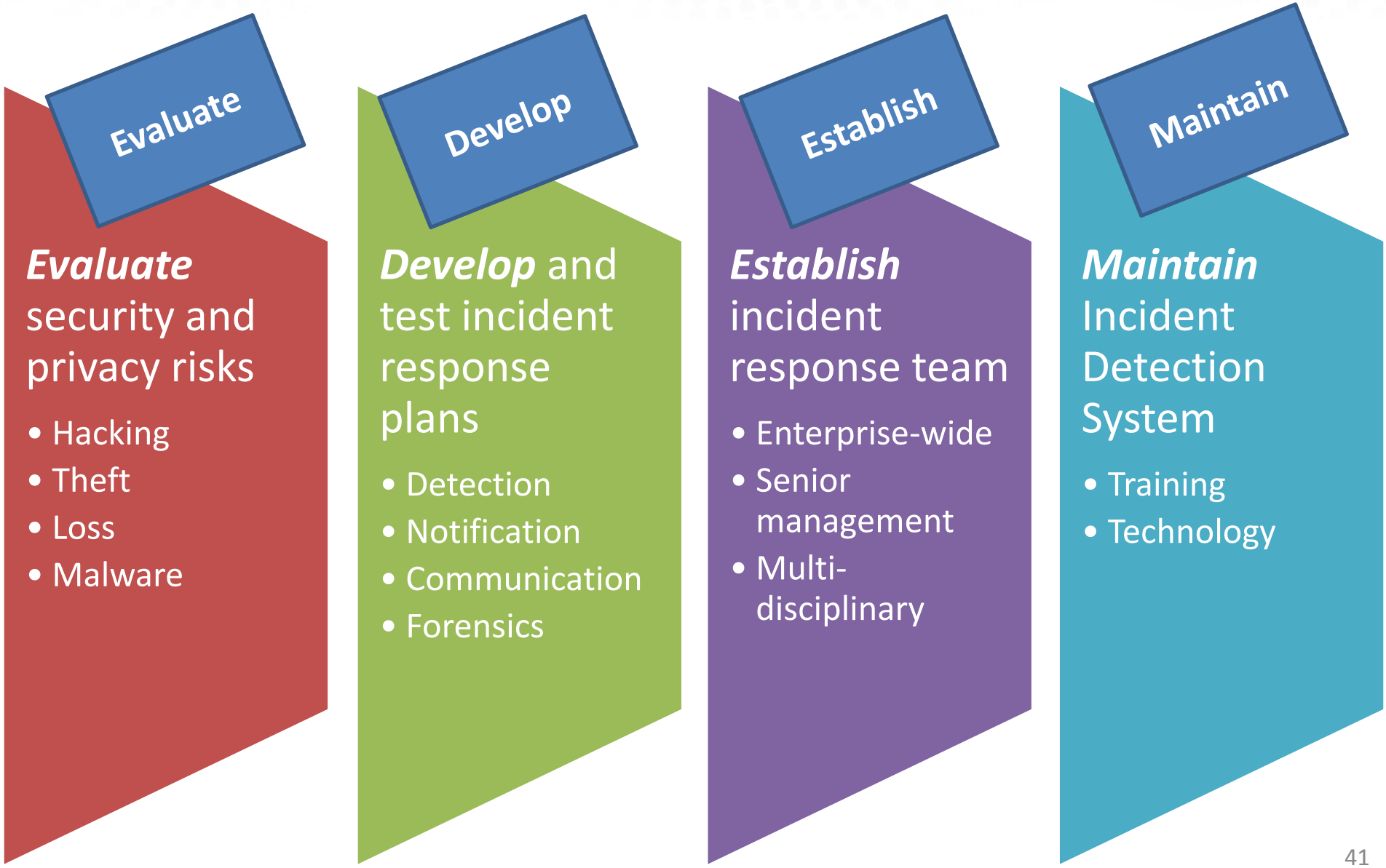
-- *Japanese proverb*



plan, plan, plan

(readiness)

Crisis Readiness Plan



crowell moring

The Cyber Threat Crisis

Richard Clarke

crowell moring

Assistance from the Government: DOJ Involvement and the Obama Administration's Efforts to Mitigate Cyber Threats

Mike Songer
Steve Byers
Jeff Snyder

Substantive Offenses

- Economic Espionage Act
  - 18 U.S.C. §§ 1832 & 1831
  - No private right of action
- Computer Fraud and Abuse Act
  - 18 U.S.C. § 1030
  - Private right of action
- Other offenses
  - Export control, mail/wire fraud, ITSP

Points of Contact

- FBI
  - Field offices, Cyber Division, National Security Division
- DOJ
  - Computer Crime and Intellectual Property Section, U.S. Attorneys Offices
- Other agencies
  - Dept. of Commerce BIS

DOJ Involvement: Pros

- Deterrence
- Additional remedies
  - forfeiture, restitution
- Additional tools
  - search warrants, MLATs, extradition
- Benefits in civil litigation
  - Fifth Amendment invocations, individual pleas/immunity, pressure/leverage, global resolution

DOJ Involvement: Cons

- Publicity
- Lack of control
- Crying “wolf”
- Risk of exposure of confidential information
- Drawbacks in civil litigation (stays, valuing “loss”)

Managing the Investigation

- Pro-active engagement
- Striking the right tone; ethics considerations
- Credibility
- Protecting confidential information
- Shaping remedies (restitution, forfeiture, injunctive relief, fines)

Exfiltration and Export Controls

- Exfiltration
  - Unauthorized release/escape
- Is it an “export”?
  - International Traffic in Arms Regulations (ITAR)
    - § 120.17 - “Sending or taking a defense article out of the United States in any manner”
  - Export Administration Regulations (EAR)
    - § 734.2 - “an actual shipment or transmission of items subject to the EAR out of the United States”
- Who is the exporter?

Exfiltration and Export Controls

- Duty to disclose or report?
  - Example: ITAR § 126.1
    - (a) Prohibited exports, imports, and sales to or from certain countries. It is the policy of the United States to deny licenses and other approvals for exports and imports of defense articles and defense services destined for or originating in certain countries. This policy applies to Belarus, Cuba, Eritrea, Iran, North Korea, Syria, and Venezuela. This policy also applies to countries with respect to which the United States maintains an arms embargo (e.g., Burma, **China**, and the Republic of the Sudan) or whenever an export would not otherwise be in furtherance of world peace and the security and foreign policy of the United States.
    - (e)(1) Duty to notify: Any person who knows or has reason to know of such a final or actual sale, **export**, **transfer**, reexport, or retransfer of such articles, services, or data must immediately inform the Directorate of Defense Trade Controls.

Exfiltration and Export Controls

- Agency Views
  - Reporting is becoming more common
  - Victims, not Violators
  - Cooperation

- Ongoing Export Control Compliance
  - Theft is not new, method is
  - Addressing ‘vulnerabilities’
    - Always make new mistakes

An Hour in the Life of the Internet .....

crowell moring

crowell moring

Breach Response and Litigation Involving Personally Identifiable Information

Jeffrey L. Poston
Robin Campbell

CONSEQUENCES OF A BREACH OF PII

- LEGAL LIABILITY
  - Government Enforcement Action
  - Class Actions
  - Individual Actions
- REPUTATIONAL EXPOSURE
- BUSINESS CONSEQUENCES
- SEC/SHAREHOLDER ISSUES
- EMPLOYEE/CUSTOMER ISSUES
- TYPICAL BREACH COSTS $MILLIONS
  - Forensics
  - Outside Counsel
  - Credit Monitoring
  - Security & Technology upgrades
  - Defense costs
  - Fines
  - Settlements

TYPES OF INCIDENTS

- Cyber-Hacking
- Employee/Vendor Negligence
  - Lost laptop
  - Inadvertent transmission
- Employee/Vendor Theft

EVERY INDUSTRY AFFECTED

- Healthcare
- Financial Services
  - Banks
  - Credit Card Companies
  - Insurance Companies
  - Mortgage Companies
- Technology
- Education
- Retail
- Government

Can involve Employee or Consumer Data

MULTIPLE FEDERAL LAWS IMPLICATED, E.G.

- HIPAA
- GRAMM LEACH BLILEY
- FTCA
- FERPA
- FCRA/FACTA

STATE BREACH NOTIFICATION LAWS

- If PII is potentially comprised, must comply with State Breach Notification laws
  - States plus D.C., Puerto Rico and Virgin Islands
  - 46 Different standards some involving “risk of harm”
  - AGs Have Enforcement Authority
  - Timing: “in the most expedient time possible,” “without unreasonable delay”

DEFINITION OF PERSONAL INFORMATION

- Generally defined as combination of first and last name PLUS any one of the following:
  - SSN
  - Drivers License No.
  - Account No.
  - Credit Card No.
  - Medical Information

- Personal Information
  - Consumer data
  - Employee data
  - Member data

ENFORCEMENT ACTIONS

- FTC:
  - Major Internet Company for $22 million
  - Sues major hotel chain for $10 million
  - $10 million fine against Data Aggregator
  - 20 years of security audits for Blood Bank
- HHS:
  - National Health Insurer fined $4.3 million
  - State Health Agency fined $1.7 million

<u>STATES</u>

- Penalties available under state breach laws ($10k to $500k but can go higher), also separate penalties under state insurance and DTPA laws
- CA & MD have established special privacy enforcement units

CASE STUDIES
INSURANCE COMPANY VENDOR

- Could Not Account for 6 Disk Drives
  - Data of 2 million members
    - PHI
    - SSNs
    - Credit Card Numbers
    - Not Encrypted
  - 11 Class Actions
  - Multiple State and Federal Investigations

DEFENSE CONTRACTOR HACKING

- Defense Contractor cyber-hacked from Asia
  - Target was Military Plans
  - Hackers access server with data involving 20,000 employees (SSNs, Names, DOBs)
    - Data Not Encrypted
    - Notified Affected Employees
    - State AG investigation

DATA MANAGEMENT COMPANY

- Inadvertently sent Data from 48 Universities to wrong University
  - Not encrypted
  - Data regarding millions of students
  - No SSNs
  - No Notification
  - No Enforcement Action
  - No Class Actions

HOW TO MANAGE CRISIS WHEN PII COMPROMISED

1. DO NOT SWEEP UNDER THE RUG
2. BE PREPARED
   - Breach Response Plan
     - GC's Office
     - Privacy Office
     - IT
     - Media Relations
   - Anticipate Litigation/Investigations
3. INVESTIGATE
   - Physical
   - Forensics
   - What Data?
   - Whose Data?

HOW TO MANAGE CRISIS WHEN PII COMPROMISED (cont'd)

4. MITIGATE/REMEDIATE

5. FIRST 24-48 HOURS CRITICAL
   - Can you recover data?
   - Can you forensically prove data not accessed?

6. INVOLVE IN-HOUSE/OUTSIDE COUNSEL IMMEDIATELY
   - If beyond de minimis expect further scrutiny
   - Can assert privilege to maximum extent possible
   - Assert privilege over outside consultants
   - Use counsel to conduct employee interviews
   - Maintain chain of custody over documents to prevent spoliation

HOW TO MANAGE CRISIS WHEN PII COMPROMISED (cont'd)

7. IF DATA IS MISSING/POSSIBLY ACCESSED
   - Be Proactive with Regulators
   - Establish Relationship/Bring them in the loop

8. INVOLVE CORPORATE COMMUNICATIONS
   - States Require Certain Content in Notification Letters
   - Speak with one consistent voice

9. CONSIDER POTENTIAL LITIGATION WHEN REMEDIATING BREACH
   - Take steps to preserve indemnification rights
   - Present a united front with vendors
   - Early offering of services may prevent litigation
   - BUT may reduce options at later settlement

Emerging Litigation Issues

- Typical Claims
  - Negligence
  - Breach of Contract
  - Unfair Trade Practices
  - Breach of Privacy
  - State Statutes
- Threshold issues
  - Standing to sue (Federal Court)
  - Actual injury or harm (common law claims)

Emerging Litigation Issues (cont'd)

- Class Certification Issues
  - Rare (Dismissal or Settlement)
  - Claims often turn on individualized issues or causation and damages
  - Thus common questions of law & facts do not predominate over questions affecting individual members.
- Damages
  - Aggregate exposure to nominal damages
  - Due process violation?

TYPICAL SETTLEMENTS

- Non-monetary relief (e.g., credit monitoring)
- Monetary payments to privacy non profits (e.g. Privacy Rights Clearinghouse)
- Consent Decree requiring security improvements
- Attorneys fees to Plaintiffs' counsel
- Capped individual payments to Plaintiffs who can prove causation

SUMMARY

- Security incidents are inevitable/litigation is not

When a breach hits:

- Do the right thing
  - Protect your company
  - Protect your customers/employees/members
  - Protect your data
  - Not mutually exclusive
- Respond quickly and aggressively to:
  - Mitigate Damage
  - Lessen likelihood of litigation/investigation
  - Protect yourself if they do arise

crowell moring

Cyber Threats, Corporate Risks and Regulatory Disclosures: Minimizing Financial and Legal Exposure

Bryan Brewer
Morris DeFeo
Jake Olcott

crowell moring

Concluding Thoughts

David Bodenheimer