Morgan Lewis

Looking Ahead: Cybersecurity in 2015

Morgan Lewis Seminar

March 12, 2015

Reece Hirsch and Mark Krotoski

Overview: A Look Ahead

- Board of director oversight issues
- SEC disclosure issues
- Security breach response planning
- Cyber Threats
- Enforcement issues
- Cyber attacks and cyber espionage
- Key Cybersecurity issues in Congress

Board of Director Oversight Issues

Cybersecurity As A Critical Risk Area

- Each year it becomes more and more clear that data security is a critical legal compliance issue
- A recent survey report from Experian Data Breach Resolution and the Ponemon Institute lists data breach “among the top three occurrences that affect a company’s reputation”
- However, in a recent FTI Consulting survey, 27% of directors said their company did not have a written security breach response plan; 31% weren’t sure
- Cybersecurity and breach response planning are areas where many companies have not yet appropriately addressed their risk

A Question of Trust

- Failure to appropriately address privacy and cybersecurity compliance is a bottom-line issue for companies because
  - Privacy is personal
  - Privacy goes right to the heart of a consumer's relationship with a company
  - No company can have perfect security and breaches are inevitable
  - Privacy and security regulatory enforcement and litigation are on the rise

The Worst Case Scenario

- Most security breaches are garden-variety incidents that do not pose significant risks if properly handled
- A major security breach that results in actual damages can lead to:
  - Class action lawsuits
  - Drop in stock price for public companies
  - Regulatory action by state Attorneys General or other regulators
  - DAMAGE TO BRAND AND CUSTOMER RELATIONSHIPS

Cybersecurity As A Board-Level Concern

- Corporate boards have a duty to protect corporate assets and, increasingly, those assets take the form of information
- Even companies outside the tech sector are reliant upon computers and software for mission-critical functions
- Most companies maintains sensitive electronic data, from trade secrets to employees' personal information

Boards Held Accountable for Cybersecurity

- Several recent security breaches have been followed by shareholder derivative lawsuits against directors and officers
  - Alleging failure of oversight and inadequate cybersecurity systems led to breaches
- Proxy advisory services have also questioned board conduct following certain security breaches
- Although most derivative lawsuits have either settled or not progressed beyond pleadings, boards should not wait for case law to define their scope of responsibility

SEC Focus on Board Responsibility for Cybersecurity

- In a June 2014 speech at the New York Stock Exchange on "Cyber Risks and the Boardroom," SEC Commissioner Aguilar stated
  - "Given the significant cyberattacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyberattacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk-oversight responsibilities."

Addressing Cybersecurity

- How can directors address the emerging risk area of cybersecurity?

- First, remove the intimidation factor
  - Cybersecurity can involve technical jargon
  - Directors, particularly in mature companies, tend to be older and less comfortable with technology
  - Information technology is constantly evolving and it's difficult for non-IT professionals to keep up

Removing the Intimidation Factor

- Remember that directors are not required to become cybersecurity experts
  - They're entitled to rely on management and outside experts for advice
- Given the significance of the risks, directors should develop a high-level understanding of those risks through briefings from management and others
- Boards should have adequate access to expertise
- Discussions about cyber risk management should be given regular, adequate time on the board agenda

External Evaluation of Security Risk Management

- Outside consultants are available to audit a company's cybersecurity practices and should be considered
- Even if an outside consultant is not hired, boards should be careful not to rely too heavily for education and assessment on the company's IT and security employees
  - It's their work that is being evaluated
- Sometimes overreliance on internal personnel can even lead to overspending on security
  - In-house security team may interpret legal standards to support securing funding for their "wish list"

Structure Board and Committees To Address Cybersecurity

- The board's risk oversight function often either lies with the full board or is delegated to the audit committee
  - Unfortunately, both may lack the technical expertise or resources to adequately manage cybersecurity risk
- Address any deficiencies by conducting cybersecurity education for the board or by recruiting board members specifically based upon their knowledge of cybersecurity

Enterprise Risk Committee

- Another approach cited by Commissioner Aguilar is creation of a separate enterprise risk committee on the board
  - Would develop a “big picture” approach to cybersecurity and other companywide risks
- A Deloitte study indicates that 48% of corporations have board-level risk committees responsible for privacy and security risks
  - Up from only 8% that reported having such a committee in 2008

Board Risk Oversight Functions

- In 2009, SEC amended its rules to require public companies to disclose information about the board's role in risk oversight
  - Including a description of whether and how the board administers its oversight function (*i.e.*, through the whole board, a separate risk committee or the audit committee)
- Although it can be highly technical, cybersecurity is in the end just another risk that boards must manage
  - If they manage the risk with due diligence and care, they should enjoy the protections of the business judgment rule

Don’t Ignore Cybersecurity

- Commissioner Aguilar says:
  - “Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril.”

SEC Disclosure Issues

SEC Guidance

- In the current environment, there is an increasing likelihood that a public company will experience a data breach that will have a material adverse effect on the company's business
- In October 2011, the SEC issued guidance on public company disclosure of data security breaches
- Does not create a new legal obligation to disclose breach, but does place cybersecurity within the context of existing public company reporting obligations

The Materiality Standard

- Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision OR

- If the information would significantly alter the total mix of information available
  - *Basic Inc. v. Levinson*, 485 U.S. 224 (1988)

Risk Factors

- Public companies should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky
- In determining whether risk factor disclosure is required, public companies must take into account all available relevant information
  - Including prior cyber incidents
  - Severity and frequency of those incidents

Is Disclosure Necessary?

- Public companies should consider:
  - The probability of cyber incidents occurring
  - The quantitative and qualitative magnitude of those risks
  - Potential costs and other consequences resulting from
    - *Misappropriation of assets or sensitive information*
    - *Corruption of data*
    - *Operational disruption*

Is Disclosure Necessary? (cont.)

- Public companies should also consider the adequacy of preventative actions taken to reduce cyberliability risks in the context of
  - The industry in which the company operates
  - Risk to that security, including threatened attacks that the company is aware of
- In accordance with Reg S-K Item 503(c) requirements for risk factor disclosures, cybersecurity risk disclosure must specify how the risk affects the company
- Generic cybersecurity risk factor disclosures are not acceptable

Examples of Appropriate Disclosures

- Discussion of aspects of company's business or operations that give rise to material cybersecurity risks
- If the company outsources functions that have material cybersecurity risks, describe those functions and how the risk is addressed
- Description of cyber incidents that the company has experienced, including costs and consequences
- In a June 2014 speech, SEC Commissioner Luis Aguilar said companies "should go beyond the impact on the company" and weigh the effect on others, including customers

Examples of Appropriate Disclosures (cont.)

- Risks related to cyber incidents that may remain undetected for an extended period
- Description of relevant insurance coverage
- SEC notes that where a company has experienced a material cyber attack, it is not sufficient to merely disclose the general risk
  - Broader discussion of the cyber risk should mention to specific attack to put the risk in context

Too Much Information?

- SEC Guidance emphasizes that companies need not disclose details of security that might actually compromise security
  - Disclosures should just provide sufficient disclosure to allow investors to appreciate the nature of the risk facing the company

- Need to strike a balance between an inappropriate "boilerplate" disclosure and one that is overly detailed

MD&A Disclosures

- In addition to the Risk Factors section, cybersecurity risk should be addressed in the Management's Discussion and Analysis of Financial Condition and Results of Operations IF
  - The costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the company's

MD&A Disclosures (cont.)

  - Results of operations
  - Liquidity
  - Financial condition
  - Or would cause the reported financial information not to be necessarily indicative of future operating results or financial condition
- SEC gives example of material intellectual property that is stolen in a cyber attack
  - Company should describe the property stolen and the potential effect of the attack

SEC Comments on Cyber Risk Disclosures

- Companies that fail to include adequate disclosures about data security risks have begun receiving SEC comments for 10-Ks
  - Example: In SEC's comment letter on Freeport-McMoRan Copper & Gold Inc.'s 10-K for 2011, lack of a cyber risk disclosure was noted
  - SEC stated that Freeport's next 10-Q should provide "risk factor disclosure describing the cybersecurity risks that you face or tell us why you believe such disclosure is unnecessary"
  - Freeport addressed cyber risk in a subsequent 10-Q

Economic Espionage

- It has been widely reported that hackers, often based in China or Russia, have been systematically targeting the intellectual property of major U.S. corporations
  - In May 2014, DOJ indicted five officers in China's People's Liberation Army for hacking Alcoa, U.S. Steel, Westinghouse Electric Co. and others to steal trade secrets
- Companies will need to evaluate whether these increasingly common thefts of IP rise to the level of a reportable event

Security Breach Response Planning

Security Breach Incident Response Plan

- A key component of a security compliance program is a security breach response plan
- Often developed as a stand-alone module distinct from security policies and procedures
  - More than just a technical, systems document, requires input from legal, compliance and others
  - Includes employee-facing components
- Commissioner Aguilar says the primary difference between a cyberattack and other crises faced by a company is the speed with which the company must respond

Incident Response Plans

- An effective incident response plan should:
  - Establish an incident response team with representatives from key areas of the organization
  - Identify necessary external resources in advance (forensic IT consultant, mailing vendor, call center operator, credit monitoring service)
  - Provide for training of rank-and-file personnel to recognize and report security breaches
  - Outline media relations strategy and point person

The Incident Response Team Leader

- There should be an incident team leader
  - Often an attorney or Chief Privacy Officer
  - Manages overall response
  - Acts as liaison between management and incident response team members
  - Coordinates responsibilities of team members
  - Develops project budgets
  - Ensures that systemic issues brought to light by a breach are addressed going forward

The Incident Response Team

- Because of the far-reaching impact of a significant breach, the Incident Response Team should include representatives from
  - Management
  - IT & Security
  - Legal
  - Compliance/Privacy
  - Public relations

The Incident Response Team (cont.)

- Customer care
- Investor relations
- Human resources
- External legal counsel (as appropriate)
- Data breach resolution provider (as appropriate)

Meet In Peacetime

- No incident response team should be forced to learn their roles on the fly during a breach
  - Meet in peacetime
  - Understand the steps outlined in the breach response plan and each team member's role and responsibility
  - Run scenarios in advance
    - *What does your company's worst-case scenario look like?*
    - *Is your company protected from potential breach liabilities through indemnification? Cyberinsurance?*
    - *How likely is it that breach damages might exceed contractual limitations of liability? Insurance liability limits?*

Line Up External Resources

- Prior to a breach, the Incident Response Team should vet and engage appropriate external resources, to be employed as needed, including:
  - Computer forensics firm
  - Data breach resolution vendor (which may include call center, notification mailing services and credit monitoring services)
- Offering credit monitoring services is increasingly becoming a best practice
  - Previously reserved for incidents involving actual fraud or identity theft

Training

- Incident response plan should include a module that is shorter and directed to employees
  - Can form the basis for regular training (once a year is advisable)
  - Employees should be able to identify the significance of a breach when it occurs and report it promptly to supervisors
- Discovery of a breach by an employee may be imputed to the organization
  - Clock begins ticking for notification of affected individuals
  - HIPAA recognizes this type of constructive knowledge

Cyber Threats

Cyber Threats

- International hacking groups
- Cyber-espionage
- State-sponsored intrusions
- Cyber fraud
- Hacktivists

- Greater sophistication
- Malware

Cyber Threats

- "We face **sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists**. They seek our **state secrets, our trade secrets, our technology, and our ideas** – things of incredible value to all of us. They may seek to strike our critical infrastructure and our economy. The threat is so dire that cyber security has topped the Director of National Intelligence list of global threats for the second consecutive year."

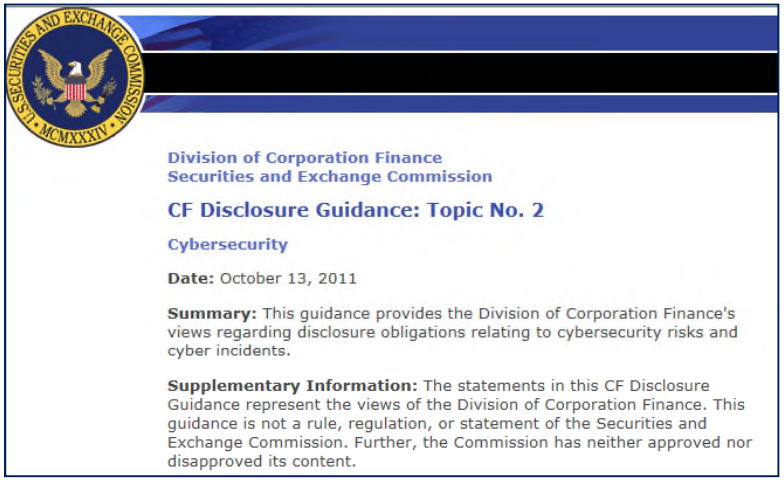
Statement of James B. Comey, Jr., FBI Director, Senate Judiciary Committee, Oversight Of The Federal Bureau Of Investigation (May 21, 2014)

http://www.judiciary.senate.gov/imo/media/doc/05-21-14ComeyTestimony.pdf

Motives

- Cybercrime
  - Steal and use information for financial benefit
  - Steal and use credit card information
  - Steal money, assets, or intellectual property
  - Ransom efforts
- Cyber Espionage
- Disrupt operations, cause damage
- Expose vulnerabilities
- Cyber-vandalism, trespassing

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.

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

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

Many Costs and Consequences

- Reputational harm
  - Media coverage
- Loss of business or customers
- Investor questions
- Enforcement actions?
- Working with law enforcement
  - Crime victim publicity?
  - Multiple agencies
- Redirected company efforts responding to breach
- Costs to respond to breach
  - Notification
  - Call centers
  - Forensics
  - Investigation
- Litigation defense costs

Enforcement Issues

DOJ

- National CHIP Network
  - Computer Hacking and Intellectual Property (CHIP) Prosecutors
  - Computer Crime and Intellectual Property Section
  - Investigative agencies
    - *FBI*
    - *Secret Service*
    - *Homeland Security*



- Prosecutions
  - Computer intrusions
  - Computer crime and fraud
  - Identify Theft
  - Intellectual Property
    - *Trade secrets*
    - *Economic espionage*
    - *Trademark*
    - *Copyright*

New DOJ Cybersecurity Unit

- Announcement by Criminal Division Assistant Attorney General Leslie Caldwell (Dec. 4, 2014)

- New DOJ Cybersecurity Unit
  - New unit "will provide a **central hub for expert advice and legal guidance** regarding the criminal electronic surveillance statutes for both US and international law enforcement conducting complex cyber investigations to ensure that the powerful law enforcement tools are effectively used to bring the perpetrators to justice while also protecting the privacy of everyday Americans."

http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-cybercrime-2020-symposium

New DOJ Cybersecurity Unit

- Computer Crime and Intellectual Property Section, Criminal Division, USDOJ

- New Cybersecurity Unit
  - Public outreach
  - Enforcement guidance
  - Legislative issues

Cyber Reward Program

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Tuesday, February 24, 2015

Reward Announced for Cyber Fugitive

The Justice Department, in partnership with the U.S. Department of State's Transnational Organized Crime (TOC) Rewards Program, announced today a reward of up to $3 million for information leading to the arrest and/or conviction of a prolific cyber criminal. Evgeniy Mikhailovich Bogachev was charged with numerous violations for his role as an administrator of the GameOver Zeus botnet.

The software was used to capture bank account numbers, passwords, personal identification numbers and other information necessary to log into online banking accounts. It is believed GameOver Zeus is responsible for more than 1 million computer infections, resulting in financial losses of more than $100 million.

Bogachev is on the FBI's Cyber's Most Wanted and is believed to be at large in Russia.

The TOC reward offer reaffirms the commitment of the U.S. government to bring those who participate in organized crime to justice, whether they hide online or overseas.

Bogachev was charged in 2014 in Pittsburgh, Pennsylvania, with conspiracy, computer hacking, wire fraud, bank fraud, and money laundering in connection with his alleged role as an administrator of the GameOver Zeus botnet. Bogachev was also indicted by criminal complaint in Omaha, Nebraska, in 2012 and charged with conspiracy to commit bank fraud related to his alleged involvement in the operation of a prior variant of Zeus malware known as Jabber Zeus.

Anyone with information on Bogachev should contact the FBI via the Major Case Contact Center, 1-800-CALL-FBI (225-5324), or the nearest U.S. Embassy or Consulate. You may also submit a tip online via tips.fbi.gov. All information will be kept strictly confidential.

http://www.justice.gov/opa/pr/reward-announced-cyber-fugitive

New Cyber Threat Intelligence Integration Center

- Lisa O. Monaco
  - Assistant to the President for Homeland Security and Counterterrorism (Feb. 10, 2015)

- "Currently, **no single government entity** is responsible for producing coordinated cyber threat assessments, ensuring that information is shared rapidly among existing Cyber Centers and other elements within the government, and supporting the work of operators and policy makers with timely intelligence about the latest cyber threats and threat actors. The CTIIC is intended to **fill these gaps**. "

http://www.whitehouse.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun

New Cyber Threat Intelligence Integration Center

1) “improve our defenses — employing better basic preventative cybersecurity”
2) “improve our ability to disrupt, respond to, and recover from cyber threats”
3) “enhance international cooperation, including between our law enforcement agencies, so that when criminals anywhere in the world target innocent users online, we can hold them accountable”
4) “make cyberspace intrinsically more secure”

Cyber Attacks
and
Cyber Espionage

Theft of Trade Secrets

- "Our **foreign adversaries and competitors are determined to acquire, steal, or transfer a broad range of trade secrets** in which the United States maintains a definitive innovation advantage. This technological lead gives our nation a competitive advantage in today's globalized, knowledge-based economy. Protecting this competitive advantage is vital to our economic security and our national security."

Statement of Randall Coleman, FBI Assistant Director, Counterintelligence Division, Senate Judiciary Subcommittee On Crime And Terrorism, Economic Espionage And Trade Secret Theft: Are Our Laws Adequate For Today's Threats? (May 13, 2014)

Criminal Prosecution Factors

- Scope of the criminal activity, including evidence of involvement by a foreign government, agent, or instrumentality;
- Degree of economic injury to the trade secret owner;
- Type of trade secret misappropriated;
- Effectiveness of available civil remedies; and
- Potential deterrent value of the prosecution [USAM § 9-59.100]

Other Questions:

- What was the manner of the misappropriation (circumstances of theft, substantial planning and preparation; leaving jurisdiction / country)?
- Was the misappropriated trade secret used (specific plans made to use it)?
- What steps were taken to disclose the trade secret to a foreign government or competitor?

Economic Espionage Act of 1996

- Theft of trade secret
  - Intent to injure trade secret owner
  - Intent to convert the trade secret "to the economic benefit of anyone other than the owner"
  - About 25 cases last year
- Foreign economic espionage
  - Intent to benefit
    - *Foreign government*
    - *Foreign instrumentality*
    - *Foreign agent*
  - Ten cases since 1996
  - Special DOJ approval process

Prior Authorized EEA Case

- *US v. Takashi Okamoto*
  (NDOH 2001) (Japan)
- *US v. Fei Ye and Ming Zhong*
  (NDCA 2002) (PRC)
- *US v. Xiaodong Sheldon Meng*
  (NDCA 2006) (PRC)
- *US v. Lan Lee and Yuefei Ge*
  (NDCA 2007) (PRC)
- *US v. Dongfan Chung*
  (CDCA 2008) (PRC)
- *US. V. Hanjuan Jin*
  (NDIL 2008) (PRC)
- *US v. Kexue Huang*
  (SDIN 2010) (PRC)
- *US v. Elliott W. Doxer*
  (D. Mass 2010) (Israel)
- *US v. Walter Liew*
  (NDCA 2012) (PRC)
- *US v. Wang Dong et al*
  (WDPA 2014) (PRC)

FBI Statement

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS

National Press Releases

Home • News • Press Room • Press Releases • Update on Sony Investigation

Twitter (3,816) Facebook (3,008) Share

Update on Sony Investigation

Washington, D.C.
December 19, 2014

FBI National Press Office
(202) 324-3691

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the "Guardians of Peace" claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE's network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations.

http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

FBI Statement

As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following:

- Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.
- The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.
- Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.

We are deeply concerned about the destructive nature of this attack on a private sector entity and the ordinary citizens who worked there. Further, North Korea's attack on SPE reaffirms that cyber threats pose one of the gravest national security dangers to the United States. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior. The FBI takes seriously any attempt—whether through cyber-enabled means, threats of violence, or otherwise—to undermine the economic and social prosperity of our citizens.

Economic Espionage

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Monday, May 19, 2014

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

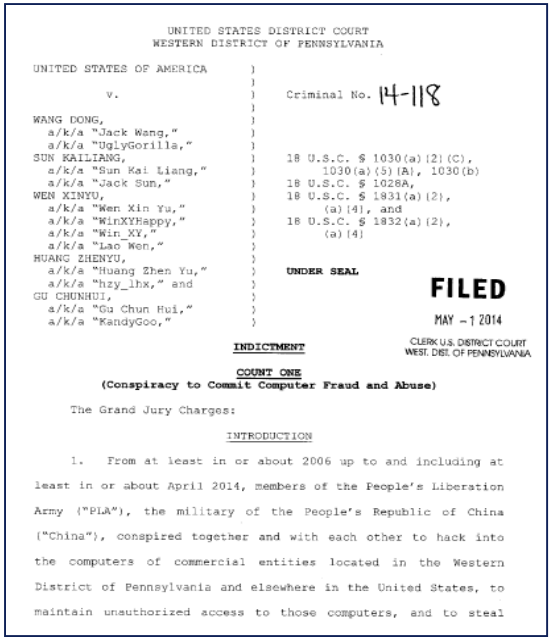
A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Economic Espionage

- Attorney General Eric Holder
  - "This is a case alleging economic espionage by members of the Chinese military and represents the **first ever charges against a state actor for this type of hacking**."
  - "The range of trade secrets and other sensitive business information stolen in this case is significant and **demands an aggressive response**."



UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA
v.
WANG DONG, a/k/a "Jack Wang," a/k/a "UglyGorilla,"
SUN KAILIANG, a/k/a "Sun Kai Liang," a/k/a "Jack Sun,"
WEN XINYU, a/k/a "Wen Xin Yu," a/k/a "WinXYHappy," a/k/a "Win_XY," a/k/a "Lao Wen,"
HUANG ZHENYU, a/k/a "Huang Zhen Yu," a/k/a "hzy_lhx," and
GU CHUNHUI, a/k/a "Gu Chun Hui," a/k/a "KandyGoo,"

Criminal No. 14-118

18 U.S.C. § 1030(a)(2)(C), 1030(a)(5)(A), 1030(b)
18 U.S.C. § 1028A,
18 U.S.C. § 1831(a)(2), (a)(4), and
18 U.S.C. § 1832(a)(2), (a)(4)

UNDER SEAL

FILED
MAY – 1 2014
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

COUNT ONE
(Conspiracy to Commit Computer Fraud and Abuse)

The Grand Jury Charges:

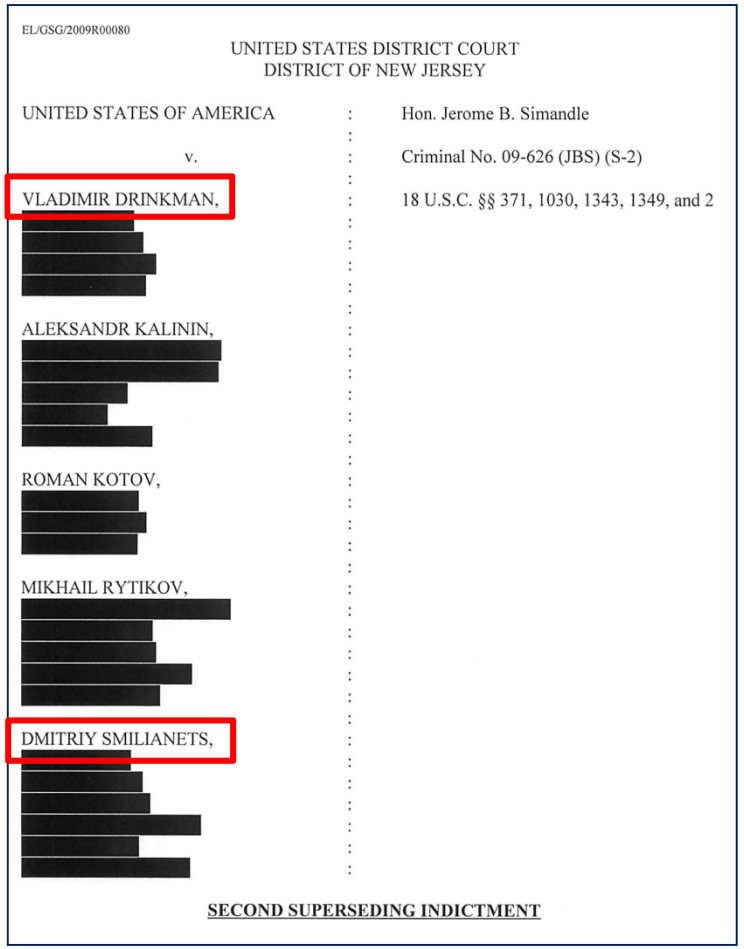
INTRODUCTION

1. From at least in or about 2006 up to and including at least in or about April 2014, members of the People's Liberation Army ("PLA"), the military of the People's Republic of China ("China"), conspired together and with each other to hack into the computers of commercial entities located in the Western District of Pennsylvania and elsewhere in the United States, to maintain unauthorized access to those computers, and to steal

http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Recent Extradition

- Charged with hacking “the computer networks of several of the largest payment processing companies, retailers and financial institutions in the world, stealing the personal identifying information of individuals”
- “[A]t least 160 million card numbers” and more than $300 million reported losses
- Drinkman & Smilianets arrested during travel in Netherlands (June 2012)



EL/GSG/2009R00080

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Jerome B. Simandle
v.	:	Criminal No. 09-626 (JBS) (S-2)
VLADIMIR DRINKMAN, [redacted]	:	18 U.S.C. §§ 371, 1030, 1343, 1349, and 2
ALEKSANDR KALININ, [redacted]	:	
ROMAN KOTOV, [redacted]	:	
MIKHAIL RYTIKOV, [redacted]	:	
DMITRIY SMILIANETS, [redacted]	:	

SECOND SUPERSEDING INDICTMENT

Morgan Lewis

Recent Extradition

Court rules accused Russian credit card 'megahacker' can be extradited to the US

Dutch court approves extradition of Russian man for his alleged involvement in one of the largest US corporate hacks of more than 160m credit card details

Russian defendant Vladimir Drinkman, left, is escorted by police officers at the courthouse in The Hague. Drinkman is accused of helping to lead a prolific computer hacking ring. Photograph: Jerry Lampen/AFP/Getty Images

Agence France-Presse in The Hague, Netherlands

Tuesday 27 January 2015 11.40 EST

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Tuesday, February 17, 2015

Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States

Defendant Brought From Netherlands

After Fighting Extradition for Over Two Years

A Russian national appeared in federal court in Newark today after being extradited from the Netherlands to face charges that he conspired in the largest international hacking and data breach scheme ever prosecuted in the United States, announced Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, Secretary Jeh Johnson of the Department of Homeland Security, U.S. Attorney Paul J. Fishman of the District of New Jersey and Acting Director Joseph P. Clancy of the U.S. Secret Service.

Vladimir Drinkman, 34, of Syktyykar and Moscow, Russia, was charged for his alleged role in a data theft conspiracy that targeted major corporate networks, stole more than 160 million credit card numbers, and caused hundreds of millions of dollars in losses. Prior to his extradition, he had been detained by the Dutch authorities since his arrest in the Netherlands on June 28, 2012.

Drinkman appeared today before U.S. Magistrate Judge James B. Clark and entered a plea of not guilty to all 11 counts charged in the indictment and was ordered detained without bail. Trial before U.S. District Judge Jerome B. Simandle was scheduled for April 27, 2015.

http://www.theguardian.com/world/2015/jan/27/russian-megahacker-vladimir-drinkman-credit-cards-extradition

Company Issues

- Whether, when to notify law enforcement?
  - Crime victim rights
  - Avoid naming company
- Ability to obtain evidence
  - Preserve evidence, pursue investigation
  - Coordinated raids
- Consider parallel civil remedies?
- Protecting trade secrets at trial
  - Discovery, Trial

Cooperating with the Government

- 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

Key Cybersecurity Issues in Congress

Key Cybersecurity Issues in Congress

- State of the Union
- White House Summit on Cybersecurity and Consumer Protection, Stanford University

- New federal civil remedy for trade secret misappropriation
- National data breach standard
- Cybersecurity Information Sharing Act
- Computer Fraud and Abuse Act

State of the Union

- "**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.…**

- "I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber-attacks, 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."

Cybersecurity Summit

- On February 13, 2015

- Focus on how to improve the security of cyberspace
  - Public and private commitments
  - Information sharing
  - Secure payment technology
  - Calls for legislative action
  - New Executive Order

Key Cybersecurity Issues in Congress

- State of the Union
- White House Summit on Cybersecurity and Consumer Protection, Stanford University

- **New federal civil remedy for trade secret misappropriation**
- National data breach standard
- Cybersecurity Information Sharing Act
- Computer Fraud and Abuse Act

Trade Secret Legislation
113th Congress (2014)

Federal civil private right of action

- ✓ New federal remedy
- ✓ Amends Economic Espionage Act
- ✓ New civil seizure order
- ✓ Five-year statute of limitations
- ✓ Bipartisan support

- Trade Secrets Protection Act of 2014 (H.R. 5233)
  - Passed House Judiciary Committee (Sept. 2014)
- Defend Trade Secrets Act of 2014 (S. 2267)
  - Introduced (April 29, 2014)

Federal Private Right of Action for Trade Secrets

- Promote and protect national economic innovation and the development of trade secrets
- Filling a gap in federal intellectual property law
- New civil seizure order to preserve evidence or the trade secret
- Stronger protection of trade secrets during litigation
- Longer statute of limitations
- Specific extraterritorial provision
- More specific definition of trade secrets
- Non-preemption of state remedies

Key Cybersecurity Issues in Congress

- State of the Union
- White House Summit on Cybersecurity and Consumer Protection, Stanford University

- New federal civil remedy for trade secret misappropriation
- **National data breach standard**
- Cybersecurity Information Sharing Act
- Computer Fraud and Abuse Act

CA Data Breach Notification

- First data breach notification law
  - Cal. Civ. Code § 1798.80 et seq. (businesses)
  - Cal. Civ. Code § 1798.29 (state government agencies)
  - Effective July 1, 2003

- Since 2012, duty to report any breach involving more than 500 Californians to the California Attorney General

CA Data Breach Notification

State *of* California Department *of* Justice
Office *of the* Attorney General

Translate Website | Traducir Sitio Web
Search

Kamala D. Harris ~ Attorney General

Home | About the AG | In the News | Careers | Services & Information | Programs A-Z | Contact Us

Cybersafety › eCrime › Data Security Breach Reporting

DATA SECURITY BREACH REPORTING

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a) and California Civ. Code s. 1798.82(a))

Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (California Civil Code s. 1798.29 (e) and California Civ. Code s. 1798.82(f))

If you are a Business or State Agency

Please use our on-line form to Submit Data Security Breach notification samples.

If you are a Resident

You may Search Data Security Breaches that have been submitted to and published by our office; or you may contact us using our online complaint form.

Data Security Breach (SB24)

Data Security Breach Reporting
Submit Data Security Breach
Search Data Security Breaches

Related Information

2014 Data Breach Report, pdf
2012 Data Breach Report, pdf
Breach Help: Tips For Consumers
Cybersafety
eCrime
Identity Theft
Privacy

http://oag.ca.gov/ecrime/databreach/reporting

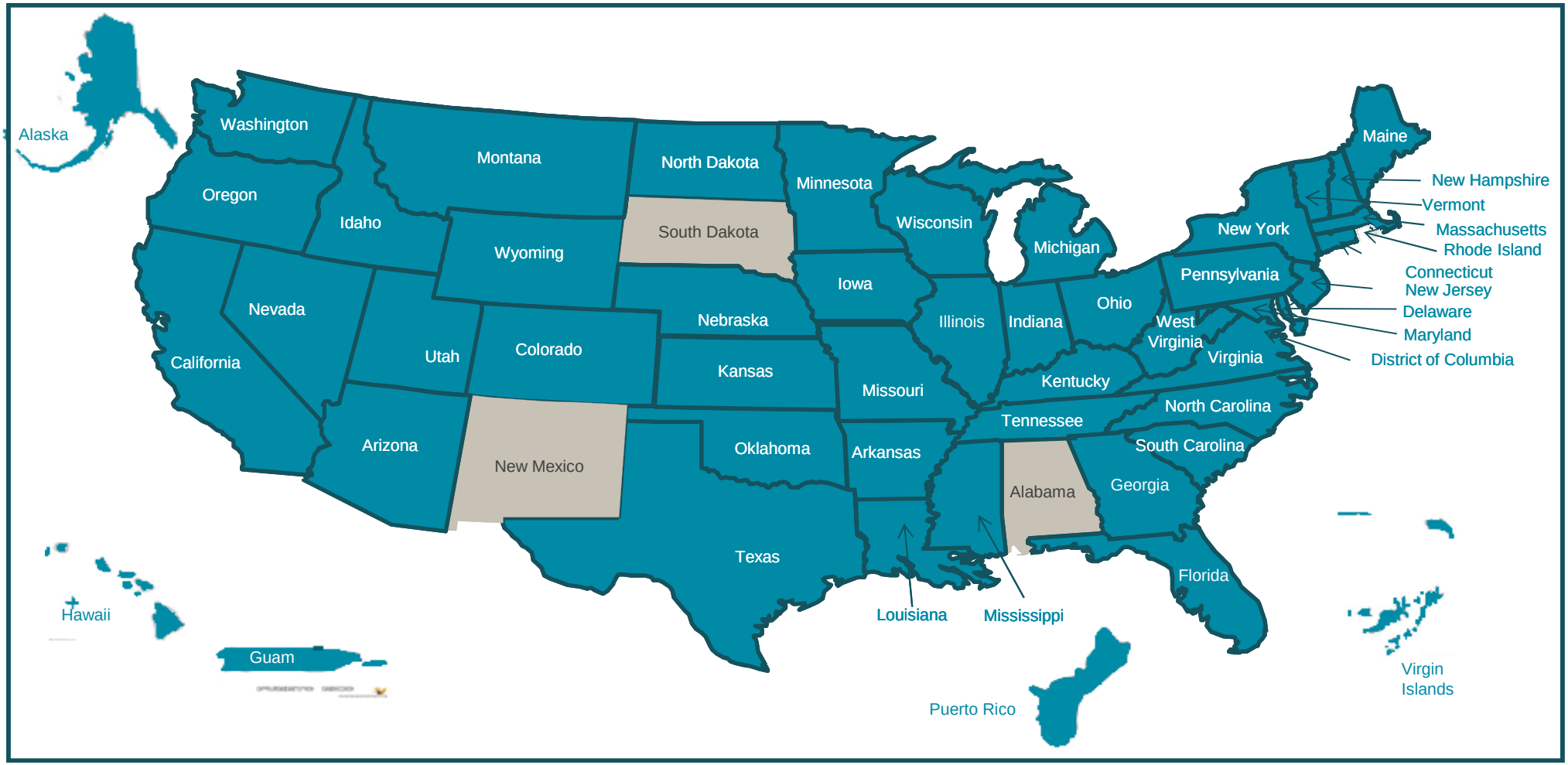
Security Breach Notification Laws

State	Citation
Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code §§ 1798.29, 1798.80 et seq.
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i) (2014 S.B. 1524, S.B. 1526)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 et seq.
Idaho	Idaho Stat. §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934 (2014 H.B. 5, H.B. 232)
Louisiana	La. Rev. Stat. § 51:3071 et seq., 40:1300.111 to .116 (2014 H.B. 350)
Maine	Me. Rev. Stat. tit. 10 § 1347 et seq.
Maryland	Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code § 2-6-504, 30-14-1701 et seq.

Security Breach Notification Laws

State	Citation
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
New Jersey	N.J. Stat. § 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65
North Dakota	N.D. Cent. Code § 51-30-01 *et seq*.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Oregon Rev. Stat. § 646A.600 *et seq*.
Pennsylvania	73 Pa. Stat. § 2301 *et seq.*
Rhode Island	R.I. Gen. Laws § 11-49.2-1 *et seq*.
South Carolina	S.C. Code § 39-1-90, 2013 H.B. 3248
Tennessee	Tenn. Code § 47-18-2107
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053, Tex. Ed. Code § 37.007(b)(5)
Utah	Utah Code §§ 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9 § 2430, 2435
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05
Washington	Wash. Rev. Code § 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. § 40-12-501 *et seq.*
District of Columbia	D.C. Code § 28- 3851 *et seq.*
Guam	9 GCA § 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico § 4051 *et seq.*
Virgin Islands	V.I. Code tit. 14, § 2208

47 Breach Notification States



Morgan Lewis

State Data Breach Laws

- Common Provisions
  - Who is covered?
    - *State resident consumer*
  - What information (PII) is covered?
    - *Name combined with SSN account, drivers license*
  - What triggering or breaching event?
    - *Unauthorized acquisition of data*
  - What notice requirements?
    - *Timing or method of notice*
    - *Who must be notified*
    - *Exemptions (e.g., for encrypted information)*

Differing 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

New Federal Legislation?

- On Jan. 12, President Obama called for the passage of the Personal Data Notification & Protection Act
  - Would create a single national standard for security breach notification
  - Would preempt patchwork of 47 state security breach notification laws
  - Encourage cyber threat information sharing within the private sector and between private sector and federal government
  - Enhance law enforcement's ability to investigate and prosecute cyber crimes

Key Cybersecurity Issues in Congress

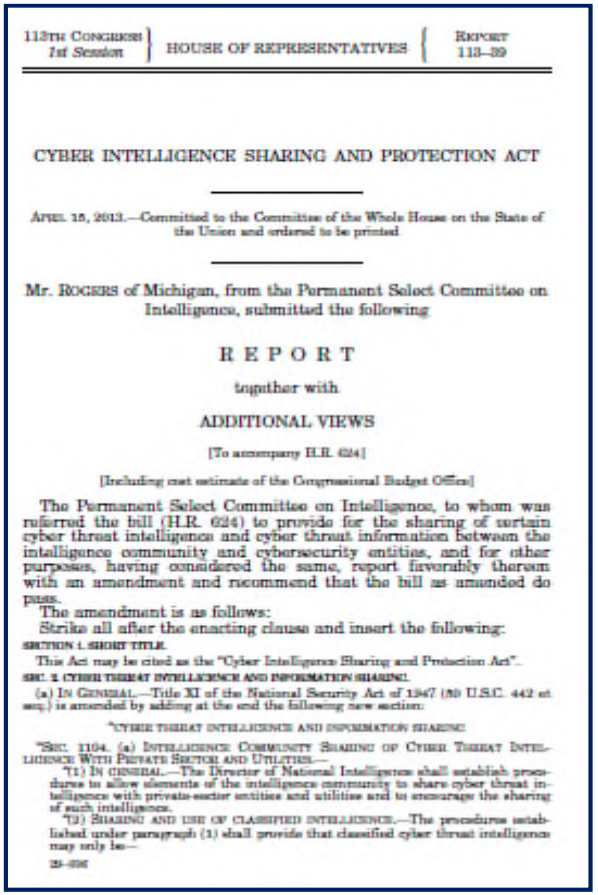
- State of the Union
- White House Summit on Cybersecurity and Consumer Protection, Stanford University

- New federal civil remedy for trade secret misappropriation
- National data breach standard
- **Cybersecurity Information Sharing Act**
- Computer Fraud and Abuse Act

Cyber Intelligence Sharing and Protection Act

- "There can be no question that in today's modern world, economic security is national security and the **government must help the private sector to protect itself**."

- "**[V]oluntary, private sector defense of private sector systems and networks informed by government intelligence information** — best protects individual privacy and takes advantage of the natural incentives built into our economic system, including harnessing private sector drive and innovation."



113TH CONGRESS, 1st Session | HOUSE OF REPRESENTATIVES | REPORT 113–39

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

APRIL 15, 2013.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. ROGERS of Michigan, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany H.R. 624]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cyber Intelligence Sharing and Protection Act".

SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—Title XI of the National Security Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding at the end the following new section:

"CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

"SEC. 1104. (a) INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR AND UTILITIES.—

"(1) IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities and to encourage the sharing of such intelligence.

"(2) SHARING AND USE OF CLASSIFIED INTELLIGENCE.—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—

29-006

Morgan Lewis

Cybersecurity Legislation
113th Congress (2013-2014)

- Key Issues:
  - Authorizes the Director of National Intelligence to increase the sharing of classified and unclassified cyber threat information
  - Authorizes companies and individuals to voluntarily share cyber threat information for cybersecurity purposes
  - Liability protections for companies and individuals that appropriately monitor their networks or share cyber information
  - Government procedures for the receipt, sharing and use of cyber information
  - Limit government's ability to use shared cyber threat information for cyber-related purposes and not for inappropriate investigations or regulation

Cybersecurity Legislation
112th Congress (2011-2012)

- House of Representatives
  - Cyber Intelligence Sharing and Protection Act (CISPA)
    - *H.R. 3523: Passed 248 to 168 (Apr. 26, 2012)*

- Senate
  - No action

Cybersecurity Legislation
113th Congress (2013-2014)

- House of Representatives
  - Cyber Intelligence Sharing and Protection Act of 2013 (CISPA) (H.R. 624)
    - *Passed House: 288 to 127 (April 18, 2013)*
    - *Identical to CISPA 2012 [H.R. 3523 (112th Cong.)]*
- Senate
  - Cybersecurity Information Sharing Act of 2014 (CISA) (S.2588)
    - *Reported out of Select Committee on Intelligence (July 10, 2014)*
    - *Further Senate action unlikely this year*

Key Cybersecurity Issues in Congress

- State of the Union
- White House Summit on Cybersecurity and Consumer Protection, Stanford University

- New federal civil remedy for trade secret misappropriation
- National data breach standard
- Cybersecurity Information Sharing Act
- **Computer Fraud and Abuse Act**

Computer Fraud and Abuse Act

- Section 1030(a)(2)
- "Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
  - (A) information contained in a financial record of a financial institution, …;
  - (B) information from any department or agency of the United States; or
  - (C) information from any protected computer;"

Computer Fraud and Abuse Act

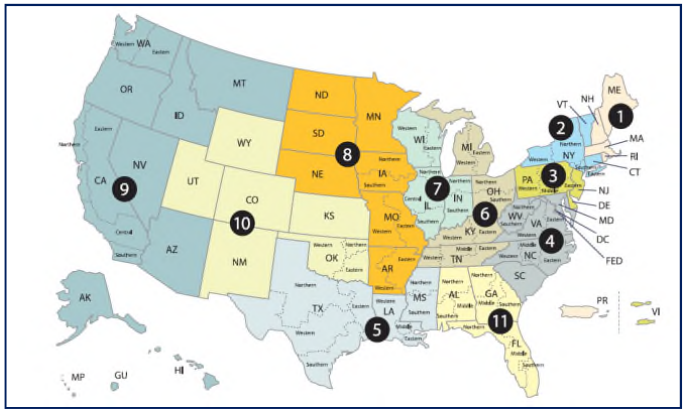
- Section 1030(a)(2)
- "Whoever intentionally accesses a computer ***without authorization*** or ***exceeds authorized access***, and thereby obtains—
  - (A) information contained in a financial record of a financial institution, …;
  - (B) information from any department or agency of the United States; or
  - (C) information from any protected computer;"

Computer Fraud and Abuse Act

- Circuit Split
  - Whether an insider or employee acting with the intent to steal the company's trade secrets and confidential business information with the company's computer violates the CFAA
- "Without authorization"
  - Undefined
- "Exceed[ing] authorized access"
  - "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."

Computer Fraud and Abuse Act

- Narrow
  - *United States v. Nosal*, 676 F.3d. 854, 863 (9th Cir. 2012) (en banc) (narrow construction under CFAA)
  - *WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (adopting ‘‘a narrow reading’’ under the CFAA)



- Broad
  - *Int’l Airport Centers v. Citrin*, 440 F.3d. 418, 420-21 (7th Cir. 2006) (‘breach of “duty of loyalty’’ terminates ‘‘authority to access” under the CFAA)
  - *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (CFAA covers access of personal records for nonbusiness reasons)
  - *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010) (‘‘authorized access’’ can encompass use limits, ‘‘at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.’’)
  - *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st 2001) (contrary to non-disclosure and use terms)

Computer Fraud and Abuse Act

Possible Options:

- Supreme Court resolution?
- Congressional amendment?
  - Redefine the Definition of “Exceeds Authorized Access”
  - Remove the "Exceeds Authorized Access" Standard and Substitute New Language
  - Distinguish “Access” from “Use” or “Purpose”
  - Misappropriation of Information Option

Questions

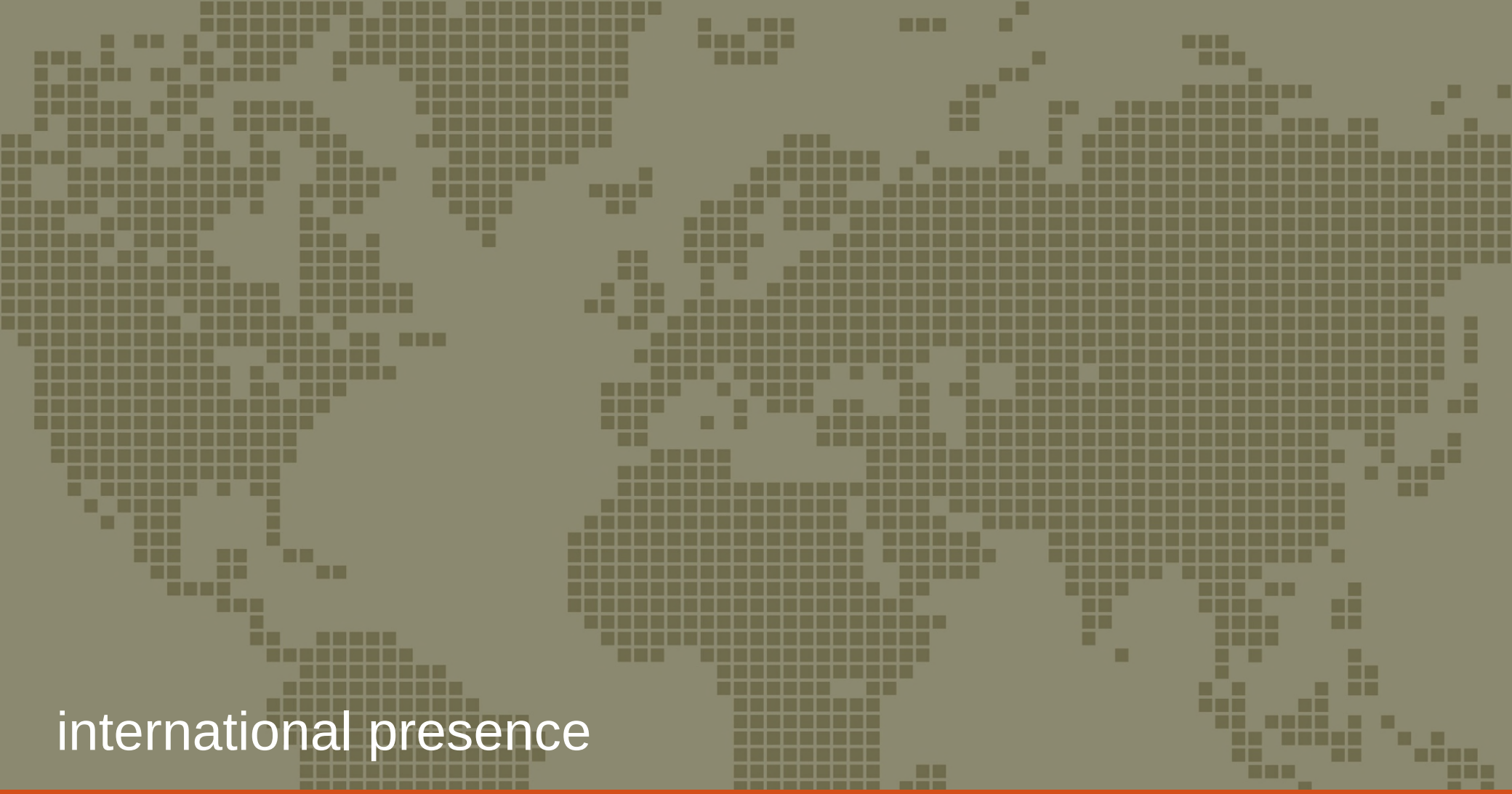
Reece Hirsch

San Francisco, California
tel. +1.415.442.1422
fax. +1.415.442.1001
rhirsch@morganlewis.com

Mark L. Krotoski

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

Morgan Lewis



international presence

Almaty Astana Beijing Boston Brussels Chicago Dallas Dubai Frankfurt Harrisburg
Hartford Houston London Los Angeles Miami Moscow New York Orange County
Paris Philadelphia Pittsburgh Princeton San Francisco Santa Monica Silicon Valley
Tokyo Washington Wilmington