Top 5 Ways to Keep the Boardroom out of the Headlines and the Courtroom

Jessica Perry

ORRICK

Top 5 Tips

1. Arbitration Agreements
2. Transparent Promotion/Review Processes
3. Process to Questions Decisions
4. Privileged Audits
5. Exits Really Matter

Arbitration Agreements

Key Provisions:

- Class action waiver
- FAA governs
- Mutuality
- Clear English
- Link to governing rules
- Opt out provision?

Transparent Promotion/Review Processes

Black box systems = distrust

Ambiguity breeds anxiety

Combat with:

- Clear and transparent criteria
- Well documented feedback

Process to Question Decisions

- Wide variety of options
- Depends on organization and culture

Conduct Privileged Audits

Key Concepts:

- Management buy-in
- Design to fit organizational needs
- Attorney-Client/Work Product protections
- Collect and analyze all relevant information
- Fix the problems

Exits Really Matter

- Don’t be afraid to cut the cord
- Consider severance agreements as a tool
- Don’t underestimate the value of a smooth transition and the goodwill
- Releases


ORRICK

ORRICK

OCTOBER 27, 2015

Six Things to Consider in Conducting an Employment Audit

Jessica Perry
Partner, Employment Law

Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
650.614.7350
jperry@orrick.com

www.orrick.com

ORRICK

Over the past few years, employers around the country have faced increasing regulation and private litigation over myriad of employment issues. The US Department of Labor has widely publicized its enforcement push with President Obama committing millions in federal funds to combat misclassification claims, and the Department of Labor adding 250 wage and hour investigators to its arsenal and updating regulations and interpretations of employment protections. Legislatures around the nation have enacted new bills aimed at ensuring equal pay. Courts, particularly in populous states such as California, New York, and Florida continue to be plagued with class actions. There is no better time for employers to consider conducting employment audits. An effective employment audit serves multiple purposes – it can identify problems, encourage corrective action, and keep an employer abreast of new developments in a field of constantly changing laws.

The depth and complexity of any audit will necessarily vary. All worthwhile audits, however, require management's commitment of resources and organizational support; a clear organizational process; mastery of basic legal principles; and consideration of privilege protections. Set forth below are tips for conducting an effective audit.

1. **Obtain Top Management Buy-In**

It is likely a tremendous waste for an employer to vest in an employment audit without securing in advance management buy-in for both the audit process and the correction of any problems it might reveal. The process requires time – to strategize, organize, conduct and respond to the audit – and that investment is pointless if the auditor does not receive full cooperation during the investigation or problems do not receive the attention needed to correct them. Moreover, if privilege problems occur, as discussed below, the audit results ultimately may support claims that the employer is liable for punitive damages, extra years of liability under the Fair Labor Standards Act or willfulness penalties under California Labor Code section 203 because it failed to correct violations. Accordingly, get a commitment up front from top management for time, money and the correction of possible violations.

2. **There is No Single Right Way to Conduct an Employment Audit**

Employment audits do not come in a "one size fits all" model. All audits should be tailored to meet the employer's needs and resources. Audits can explore a variety of employment practices – hiring, compensation, promotion, wage and hour practices including exemptions, recordkeeping and other compliance with Equal Employment Opportunity statutes, including the Family and Medical Leave Act and the Americans with Disabilities Act. An audit also can target certain departments, facilities or groups, or focus upon specific positions (for example, whether men and women earn equal pay for the same or similar role or exemptions from overtime pay apply).

The decision regarding audit scope should be depend on assessment of risks, priorities, and available resources. Certainly, if the company has knowledge of practices which are in the employment litigation hotbed, it may make sense to start with those practices. Audits can be performed in phases, with specific timelines set for those phases (for example, phase one might target the exemption status of employees in a particular department; phase two might target recordkeeping and timecard compliance; phase three may move to exemption classifications in other groups; phase four might concern meal breaks for non-exempt employees).

At the start of the process, there should be careful planning regarding the scope of the audit and the commitment of resources necessary to accomplish any phases. When resources are limited, it may be wise to choose in-depth analysis of a particular high risk practice over breadth. A superficial review due to inadequate resources typically causes rather than cures problems.

3. Maintain the Attorney-Client Privilege

An audit can be a double-edged sword. While an effective audit may reduce future litigation by identifying and resolving compliance problems, careless distribution of sensitive audit information can substantially increase the company's exposure for those problems. It is therefore important that all phases of an audit be properly protected by the attorney-client privilege and work product doctrine (if applicable). The employer should clarify from the outset that its goal in conducting the audit is to ensure compliance with relevant employment laws. The initial audit authorization should typically issue from top management or in-house counsel. Outside counsel should open a separate billing matter for the audit, and the employer should receive an engagement letter that authorizes the audit and makes clear that its purpose is to obtain legal advice concerning the company's compliance with relevant employment laws. That letter should also authorize counsel to obtain the assistance of all necessary company personnel to obtain information and should stress the confidential nature of the inquiry. This added authorization and direction will help clarify that lower-level personnel are viewed as "the client" for purposes of the privilege.

The company should take all reasonable steps to ensure that the results of the audit are kept private and the privilege is protected. Once the audit begins, all communications concerning the audit should be disclosed only to those with a need to know and should stress the need for confidentiality. All documents created during the audit should be clearly marked as "privileged and confidential," and should be treated with the same confidentiality as other sensitive legal documents. No disclosure of audit results should be made beyond those with a need to know.

4. Collect All Relevant Information

As the audit begins, the audit team should compile all pertinent documents. The documents at issue will, of course, vary depending on the scope of the audit. In a wage and hour exemption audit for example, relevant information may include written policies and procedures, job descriptions, and performance evaluation forms. In a compensation audit, relevant information may consist of historical pay data back to the date of hire, as well as salary bands, performance rankings, job codes and descriptions, and other information about the role actually performed.

In addition to reviewing written materials, the audit team will need to assess how to conduct an independent investigation of actual practices. This information can be acquired through questionnaires, on-site inspections, and/or interviews. The employer will need to determine who should provide the necessary information – are Human Resources employees equipped to understand and convey the employee's actual job duties, would managers be more appropriate, or does the audit team need to speak with the employees actually performing the jobs at issue? Also important is determining who will collect the information. In some cases, it may be appropriate for HR to elicit and compile the audit information; while in other circumstances, it may be more desirable for outside counsel to take the laboring oar directly.

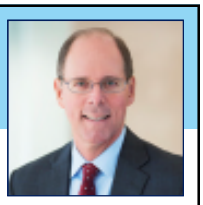
Morgan Lewis

Avoiding Recurring Weak Links To Enhance Cybersecurity©

Mark L. Krotoski

October 27, 2015

Presenter: Mark Krotoski



- Litigation partner in Morgan Lewis's Privacy and Cybersecurity and Antitrust practices.
- Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the Department of Justice (DOJ) in Washington, D.C., and as a CHIP prosecutor in Silicon Valley, among other DOJ leadership positions.
- Successfully led prosecutions and investigations of nearly every type of international and domestic computer intrusion, cybercrime, and criminal intellectual property cases.
- Served as a DOJ leader on foreign economic espionage cases involving the theft of trade secrets with the intent to benefit a foreign government. He and his team successfully prosecuted two foreign economic espionage cases out of eleven that have been authorized by DOJ since 1996.
- Advises clients on developing effective Cybersecurity and Trade Secret Protection Plans and assists them in responding to a data breach incident or misappropriation of trade secrets. He has written extensively on these issues.

Overview

- Cyber Threat Environment
  - Cyber Attack Motives Vary
  - Increasing Enforcement and Regulatory Scrutiny
- Eight Key Weak Links in Cybersecurity Protection

INCREASING CYBER THREATS

Cyber Threat Environment

- Organized, international hacking groups
- State-sponsored actors
- Hackers for hire
- Cyber terrorists
- Hacktivists

- Insider threat
  - Inadvertence
  - Misconduct

- Greater sophistication
- Malware
- Ransomware

- Targeting
  - Specific Customer Data
  - Valuable Corporate Information

Morgan Lewis

5

Cyber Attack Motives Vary

- 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

Morgan Lewis

6

Financial Gain

- "The value to a criminal of a stolen Social Security number is greater than the value of payment card data."
- "The mean fraud amount for stolen **Social Security numbers is $2,330**, compared to $2,026 for a debit card and $1,251 for a credit card."

Morgan Lewis https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf? 7

Cost of Data Breach Continues to Increase

- The average cost for each lost or stolen record containing sensitive and confidential information increased from $201 to **$217**
  - $143 pertains to indirect costs (abnormal turnover or churn of customers)
  - $74 represents the direct costs incurred to resolve the data breach (investments in technologies or legal fees)
- The total average cost paid by organizations increased from $5.9 million to **$6.5 million**.

Morgan Lewis http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF 8

Criminal Cyber Attacks Trend

Ponemon INSTITUTE

MEASURING TRUST IN PRIVACY AND SECURITY

About Us | Strategic Consulting | Ponemon Fellows | Research | Blog | Contact | Responsible Information Management

Receive important updates and special reports

Subscribe to the Ponemon News Feed

News & Updates

FOR IMMEDIATE RELEASE
Ponemon Institute Releases 11th Annual Most Trusted Companies for Retail Banking Study U.S. Bank earns top honors; Ally Bank is second most trusted

...more

Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study

Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study

Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study

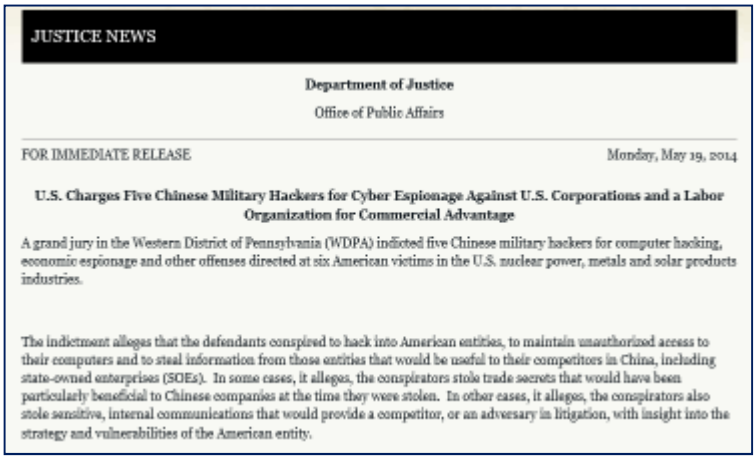
Study Reveals Five-Year Data Breach and Security Trends of Growing $6 Billion Epidemic That Puts Millions of Patients and Their Information at Risk

Study Reveals Five-Year Data Breach and Security Trends of Growing $6 Billion Epidemic That Puts Millions of Patients and Their Information at Risk

TRAVERSE CITY, Mich. and PORTLAND, Ore. — May 7, 2015 — The healthcare industry is experiencing a surge in data breaches, security incidents, and criminal attacks—exposing millions of patients and their medical records—according to the latest Ponemon Institute study, sponsored by ID Experts®, the Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data. The study reveals that criminal attacks in healthcare are up 125 percent since 2010 and are now the leading cause of data breach. The findings also show that most healthcare organizations are still unprepared to address this rapidly changing cyber threat environment and lack the resources and processes to protect patient data. According to the FBI, criminals are targeting the information-rich healthcare sector because individuals' personal information, credit information, and protected health information (PHI) are accessible in one place, which translates into a high return when monetized and sold. To learn more about the Fifth Annual Study on Privacy & Security of Healthcare Data, visit www2.idexpertscorp.com/ponemon for a free copy.

http://www.ponemon.org/news-2/66

Chinese Military Hackers



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

Chinese Military Hackers

- Then-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**."


FILED

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

North Korean Government


FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US ABOUT US MOST WANTED NEWS STATS

National Press Releases

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 attack 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

State Sponsored Hacking Efforts

https://www.opm.gov/cybersecurity/

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

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)

http://www.judiciary.senate.gov/imo/media/doc/05-13-14ColemanTestimony.pdf

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)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA
v.
VLADIMIR DRINKMAN,
[redacted]
ALEKSANDR KALININ,
[redacted]
ROMAN KOTOV,
[redacted]
MIKHAIL RYTIKOV,
[redacted]
DMITRIY SMILIANETS,
[redacted]

Hon. Jerome B. Simandle
Criminal No. 09-626 (JBS) (S-2)
18 U.S.C. §§ 371, 1030, 1343, 1349, and 2

SECOND SUPERSEDING INDICTMENT

82144925

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

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 Syktyvkar 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.

Agence France-Presse in The Hague, Netherlands

Tuesday 27 January 2015 11.40 EST

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

Recent Conviction

Department of Justice

U.S. Attorney's Office

District of New Jersey

FOR IMMEDIATE RELEASE

Tuesday, September 15, 2015

Russian National Admits Role In Largest Known Data Breach Conspiracy Ever Charged

Hackers Targeted Major Payment Processors, Retailers and Financial Institutions Around the World

CAMDEN, N.J. – A Russian national today admitted his role in a worldwide hacking and data breach scheme that targeted major corporate networks, compromised more than 160 million credit card numbers and resulted in hundreds of millions of dollars in losses – the largest such scheme ever prosecuted in the United States.

The guilty plea was announced by New Jersey U.S. Attorney Paul J. Fishman, U.S. Secret Service Director Joseph P. Clancy and Assistant Attorney General Leslie Caldwell.

Vladimir Drinkman, 34, of Syktyvkar, Russia, and Moscow, pleaded guilty before Chief U.S. District Judge Jerome B. Simandle of the District of New Jersey to one count of conspiracy to commit unauthorized access of protected computers and one count of conspiracy to commit wire fraud. Drinkman was arrested in the Netherlands on June 28, 2012, and was extradited to the District of New Jersey on Feb. 17, 2015.

"Defendants like Vladimir Drinkman, who have the skills to break into our computer networks and the inclination to do so, pose a cutting edge threat to our economic well-being, our privacy and our national security," U.S. Attorney Fishman said. "The crimes to which he admitted his guilt have a real, practical cost to our privacy and our pocketbooks. Today's guilty plea is a tribute to the skill and perseverance of the agents and prosecutors who brought him to justice."

http://www.justice.gov/usao-nj/pr/russian-national-admits-role-largest-known-data-breach-conspiracy-ever-charged

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**."

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

https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

Increasing Enforcement and Regulatory Scrutiny

- Increasing focus of many regulators
  - FTC
  - SEC
  - State Attorneys General
  - DOJ
  - FBI, USSS, DHS

Increasing Enforcement and Regulatory Scrutiny

- What constitutes reasonable cybersecurity?
  - What constitutes "unfair cybersecurity practices"?
  - Agency inquiry shifting to: Whether the company could have taken steps to prevent the cybercrime?

- Data breach disclosure obligations
  - Breaches affecting more than 500 Californians are required to be reported to the Attorney General, Under Civil Code §§ 1798.29(e) and 1798.82(f)

Morgan Lewis

21

FTC

- "**Data security is one of our top consumer protection priorities**. In our enforcement actions and policy initiatives, we focus on the harms that consumers may suffer when companies fail to keep information secure. Unauthorized access to data puts consumers at risk of fraud, identity theft, and even physical harm. Data can reveal information about our health conditions, financial status, or other sensitive traits. **Security is also an essential part of maintaining consumers' privacy**, which is another **top consumer protection priority** at the FTC."

FTC Commissioner Julie Brill (Sept. 17, 2014)

Morgan Lewis

22

FTC

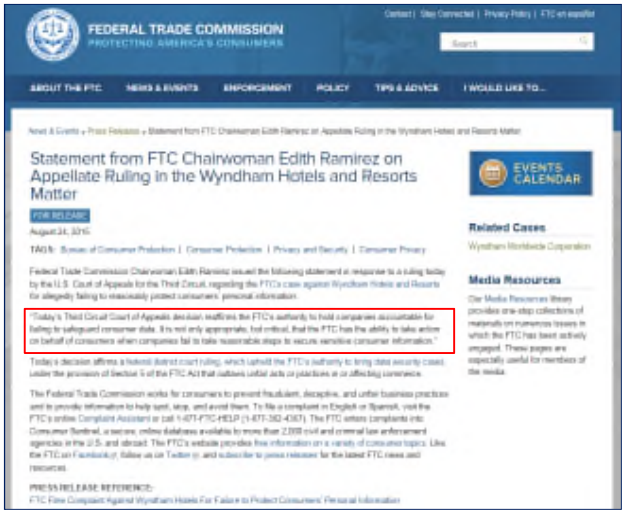
- Request for More Authority
  - "The FTC supports federal legislation that would

(1) **strengthen its existing authority** governing data security standards on companies and

(2) require companies, in appropriate circumstances, to **provide notification** to consumers **when there is a security breach**."

FTC Chairwoman Edith Ramirez, Statement on Protecting Personal Data from Cyber Attacks and Data Breaches Before the Senate Committee on Commerce, Science, and Transportation (Mar. 26, 2014)

FTC v. Wyndham Worldwide Corp. (3d Cir.)



https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect

SEC

- "The SEC's formal jurisdiction over cybersecurity is directly focused on the
  - [1] integrity of our market systems,
  - [2] customer data protection, and
  - [3] disclosure of material information."

SEC Chair Mary Jo White, SEC Cybersecurity Roundtable (March 26, 2014)

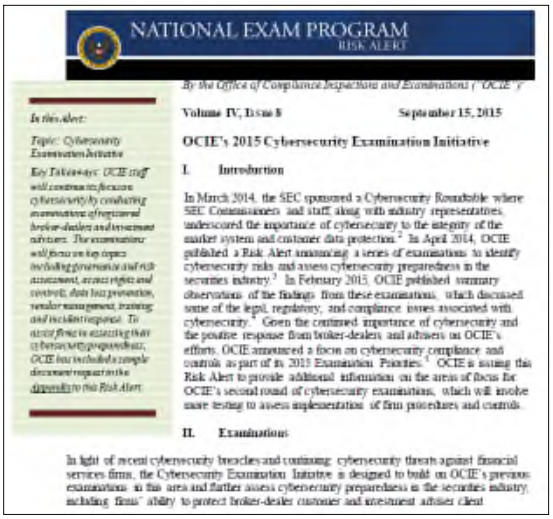
SEC

- "**[B]oard oversight of cyber-risk management** is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks.
- There is **no substitution** for proper preparation, deliberation, and engagement on cybersecurity issues.

  - Given the heightened awareness of these rapidly evolving risks, directors should take seriously their **obligation to make sure that companies are appropriately addressing those risks**."

SEC Commissioner Luis A. Aguilar (June 10, 2014)

SEC



NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")

In this Alert:

Topic: Cybersecurity Examination Initiative

Key Takeaways: OCIE staff will continue its focus on cybersecurity by conducting examinations of registered broker-dealers and investment advisers. The examinations will focus on key topics including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response. To assist firms in assessing their cybersecurity preparedness, OCIE has included a sample document request in the Appendix to this Risk Alert.

Volume IV, Issue 8 September 15, 2015

OCIE's 2015 Cybersecurity Examination Initiative

I. Introduction

In March 2014, the SEC sponsored a Cybersecurity Roundtable where SEC Commissioners and staff, along with industry representatives, underscored the importance of cybersecurity to the integrity of the market system and customer data protection.[2] In April 2014, OCIE published a Risk Alert announcing a series of examinations to identify cybersecurity risks and assess cybersecurity preparedness in the securities industry.[3] In February 2015, OCIE published summary observations of the findings from these examinations, which discussed some of the legal, regulatory, and compliance issues associated with cybersecurity.[4] Given the continued importance of cybersecurity and the positive response from broker-dealers and advisers on OCIE's efforts, OCIE announced a focus on cybersecurity compliance and controls as part of its 2015 Examination Priorities.[5] OCIE is issuing this Risk Alert to provide additional information on the areas of focus for OCIE's second round of cybersecurity examinations, which will involve more testing to assess implementation of firm procedures and controls.

II. Examination

In light of recent cybersecurity breaches and continuing cybersecurity threats against financial services firms, the Cybersecurity Examination Initiative is designed to build on OCIE's previous examinations in this area and further assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client

https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

EIGHT KEY CYBERSECURITY WEAK LINKS

When?

- No longer a question of "if" but "when"
- Vulnerability and significant exposure and costs can come from any one weak link in the cybersecurity program

A Few Key Weak Links in Cybersecurity Protection

(1) Need For A Holistic, Tailored, Integrated Cybersecurity Program
(2) Deter Spear Phishing Attacks
(3) Protect Third Party Data Transfers
(4) Prevent Exposure To Unencrypted Data
(5) Attorney-Client Privilege Protected Investigation
(6) What Does Your Cyber-Insurance Cover?
(7) Tested Incident Response Plan
(8) Mitigating Harm Following A Breach

(1) Need For A Holistic, Tailored, Integrated Cybersecurity Program

Consequences from any weak link:

- Reputational harm
  - Media coverage
- Loss of business or customers
- Investor questions
- Enforcement actions?
  - Fines
  - Adverse publicity
- 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

(1) Need For A Holistic, Tailored, Integrated Cybersecurity Program

- Tailored approach
  - Designed around information, needs and risks
- Do you have a cybersecurity culture in your organization?
  - Any areas to improve?
- Prepare for diverse cyber threats

- **Integrated Approach**
  - Technical Security
    - IT Network
    - Cyber Threat Updates
  - Physical Security
  - Administrative Security
    - Policies
    - Training
  - Incident Response Plan

(2) Deter Spear Phishing Attacks

- Target particular users to entice them into opening an attachment or clicking on a link which launches malware on the system
- Nearly "80% of all espionage-motivated attacks used either a link or attachment in a phishing email to gain access to their victim's environment"

Morgan Lewis

http://www.verizonenterprise.com/DBIR/2014/
http://www.mcafee.com/us/resources/reports/rp-phishing-quiz-assessment.pdf?snspd-0115

33

Daily Email

- 116+ Billion business emails sent/received each day

Daily Email Traffic	2013	2014	2015	2016	2017
Total Worldwide Emails Sent/Received Per Day	**182.9**	**191.4**	**196.4**	**201.4**	**206.6**
% Growth		*5%*	*3%*	*3%*	*3%*
Business Emails Sent/Received Per Day	**100.5**	**108.8**	**116.2**	**123.9**	**132.1**
% Growth		*8%*	*7%*	*7%*	*7%*
Consumer Emails Sent/Receive Per Day	**82.4**	**82.6**	**80.2**	**77.5**	**74.5**
% Growth		*0%*	*-3%*	*-3%*	*-4%*

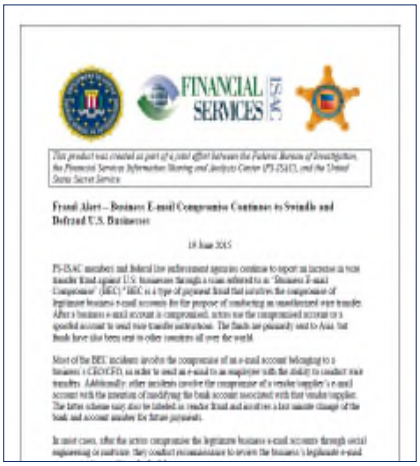
Morgan Lewis

http://www.radicati.com/wp/wp-content/uploads/2014/04/Email-Statistics-Report-2014-2018-Brochure.pdf
http://sourcedigit.com/4233-much-email-use-daily-182-9-billion-emails-sentreceived-per-day-worldwide/

34

Fraud Alert: Business E-mail Compromise

- "Most of the BEC incidents involve the compromise of an **e-mail account** belonging to a business's **CEO/CFO**, in order to send an e-mail to an employee with the ability to **conduct wire transfers**."
- "[O]ther incidents involve the compromise of a **vendor/supplier's e-mail account** with the intention of modifying the **bank account** associated with that vendor/supplier."



https://www.fsisac.com/sites/default/files/news/BEC_Joint_Product_Final.pdf?utm_source=hs_email&utm_medium=email&utm_content=19064920&_hsenc=p2ANqtz-9wi5WFkCmzCmWDI-Z3g2N6n8MrzmLqqXoyXMAwblLJ0wYOm8WbKXL4gh-jzpsXpt2QuKWeF4uqxOhWEChCi3HlS3RVfg8&_hsmi=19064920

Business E-mail Compromise Increasing Impact

Internet Crime Complaint Center Reports	Oct. 2013 to Aug. 2015
Total U.S. Victims	**7,066**
Total U.S. exposed dollar loss	**$747,659,840.63**

Internet Crime Complaint Center Reports	Oct. 2013 to Dec. 2014
Total U.S. Victims	**1,198**
Total U.S. exposed dollar loss	**$179,755,367.08**

http://www.ic3.gov/media/2015/150827-1.aspx
http://www.ic3.gov/media/2015/150122.aspx

(3) Protect Third Party Data Transfers

- Data is often shared with third parties
- Is the data sufficiently protected?

Insider Trading Case


U.S. Securities and Exchange Commission

ABOUT DIVISIONS ENFORCEMENT REGULATION EDUCATION FILINGS NEWS

PRESS RELEASE

SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases

Hackers, Traders Allegedly Reaped More Than $100 Million of Illegal Profits

FOR IMMEDIATE RELEASE
2015-163

Washington D.C., Aug. 11, 2015 – The Securities and Exchange Commission today announced fraud charges against 32 defendants for taking part in a scheme to profit from stolen nonpublic information about corporate earnings announcements. Those charged include two Ukrainian men who allegedly hacked into newswire services to obtain the information and 30 other defendants in and outside the U.S. who allegedly traded on it, generating more than $100 million in illegal profits.

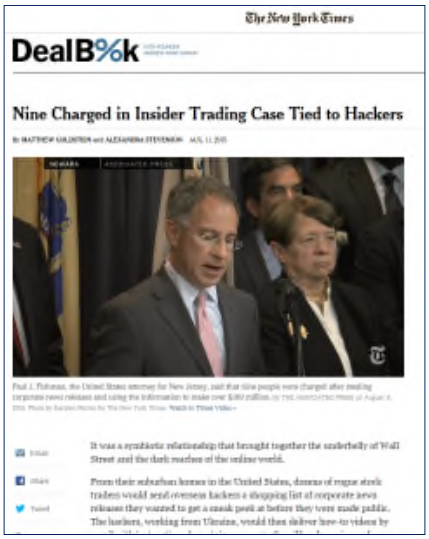
The SEC's complaint unsealed today was filed under seal on August 10 in U.S. District Court in Newark, N.J., and the court entered an asset freeze and other preliminary relief that day.

"This international scheme is unprecedented in terms of the scope of the hacking, the number of traders, the number of securities traded and profits generated," said Securities and Exchange Commission Chair Mary Jo White. "These hackers and traders are charged with reaping more than $100 million in illicit profits by stealing nonpublic information and trading based on that information. That deception ends today as we have exposed their fraudulent scheme and frozen their assets."

Related Materials

- SEC complaint

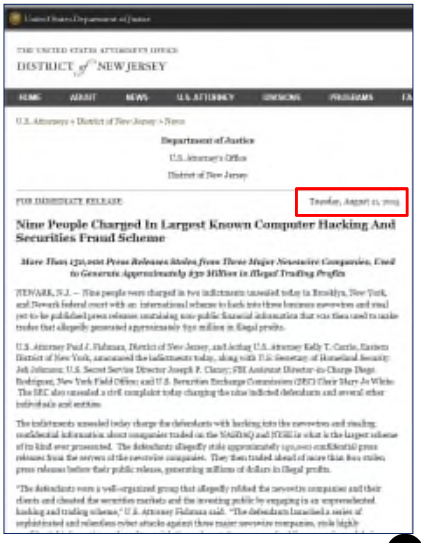
Insider Trading Case



The New York Times

DealB%k

Nine Charged in Insider Trading Case Tied to Hackers



DISTRICT of NEW JERSEY

Department of Justice

U.S. Attorney's Office

District of New Jersey

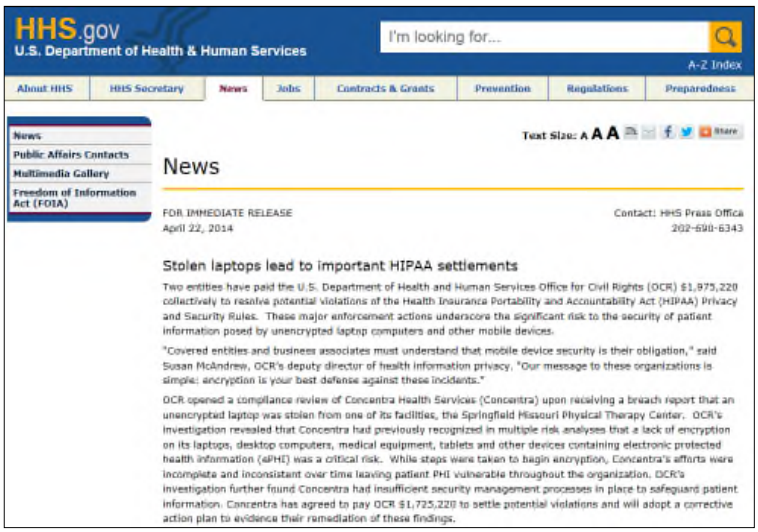
FOR IMMEDIATE RELEASE

Nine People Charged In Largest Known Computer Hacking And Securities Fraud Scheme

More Than 150,000 Press Releases Stolen from Three Major Newswire Companies, Used to Generate Approximately $30 Million in Illegal Trading Profits

http://www.justice.gov/usao-nj/pr/nine-people-charged-largest-known-computer-hacking-and-securities-fraud-scheme

(4) Prevent Exposure To Unencrypted Data



HHS.gov

U.S. Department of Health & Human Services

I'm looking for...

A-Z Index

About HHS | HHS Secretary | News | Jobs | Contracts & Grants | Prevention | Regulations | Preparedness

News

Public Affairs Contacts

Multimedia Gallery

Freedom of Information Act (FOIA)

Text Size: A A A

News

FOR IMMEDIATE RELEASE
April 22, 2014

Contact: HHS Press Office
202-690-6343

Stolen laptops lead to important HIPAA settlements

Two entities have paid the U.S. Department of Health and Human Services Office for Civil Rights (OCR) $1,975,220 collectively to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

"Covered entities and business associates must understand that mobile device security is their obligation," said Susan McAndrew, OCR's deputy director of health information privacy. "Our message to these organizations is simple: encryption is your best defense against these incidents."

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

http://www.hhs.gov/news/press/2014pres/04/20140422b.html

(4) Prevent Exposure To Unencrypted Data

- "Many of the health care breaches reported to us are of a type that could be prevented by the strategic use of encryption. Unlike other industry sectors, where computer intrusions caused the majority of breaches, in **health care 70 percent of breaches** reported in the past two years were the result of stolen or lost hardware or digital media containing **unencrypted personal information**."

Recommendations for the Health Care Sector

Recommendation 7: The health care sector should consistently use strong encryption to protect medical information on laptops and on other portable devices, and should consider it for desktop computers.

https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf

(5) Attorney-Client Privilege Protected Investigation

- The attorney-client privilege is intended to "encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."

Upjohn Co. v. United States, 449 U.S. 383, 389 (1981)

(5) Attorney-Client Privilege Protected Investigation

- Privilege aids careful evaluation of threats/intrusions and responsive action in investigative, notice, and litigation contexts
  - Importance of privilege early in the process
- Privilege covers counsel communications with third parties assisting in the investigation
- Company steps necessary to protect the privilege
  - Risks if the privilege is not properly used

(6) Testing Your Incident Response Plan

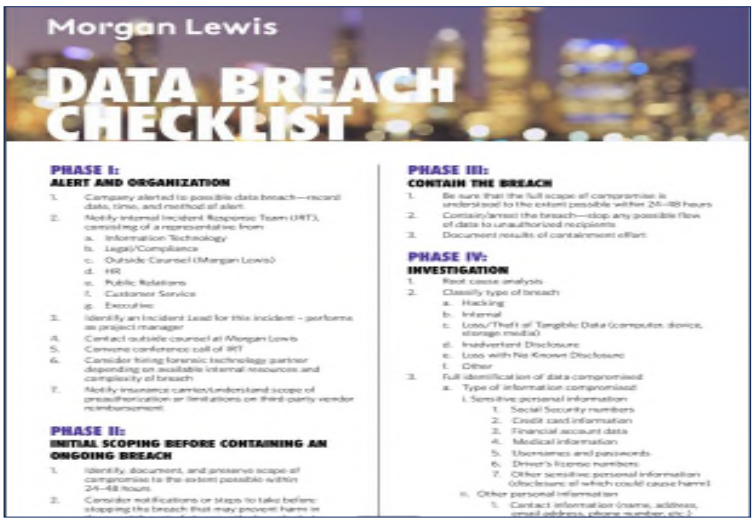
- Practical focus
- Team response

- 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

(6) Testing Your Incident Response Plan

- When was the last time your incident response plan was tested?
  - What lessons were learned?
  - What remediation efforts?
- Tested Incident Response Plan
  - Simulate "real life" circumstances
  - Consider "worst case" scenarios
  - Consider coverage/insurance liability limits
  - Identify areas to enhance and address

(6) Testing Your Incident Response Plan



(7) What Does Your Cyber-Insurance Cover?

- Protection
  - Data breaches
  - Business interruption
  - Network damage
  - Related incidents
- What is covered?

(7) What Does Your Cyber-Insurance Cover?

- First-party losses
  - Direct expenses in breach response
  - Forensics, notification costs, credit monitoring services, legal services, data restoration and remediation costs
- Third-party losses
  - Coverage varies
  - Defense costs, data loss, fines and penalties
- Network interruption
  - Loss of business income causing actual disruption or impairment of business operations

(8) Mitigating Harm Following A Breach

- Don't fumble in implementing your incident response plan
  - Significant reputational risks and costs at stake
- Identify Key steps to mitigate harm
  - Contain damage
  - Determine any use of data
  - Customer relations
  - Is credit monitoring report sufficient?

Are You Prepared?

- Do you have:
  - A holistic and integrated cybersecurity program?
  - A tailored program designed to fit information, needs and risks?
  - A culture of cybersecurity?
  - Support from highest levels of the company?
  - Mechanisms to identify and report any weak links and to prevent and detect incidents and respond appropriately?
- There is no better time than **now** to prepare and adopt an effective, tailored Cybersecurity Program

Questions

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

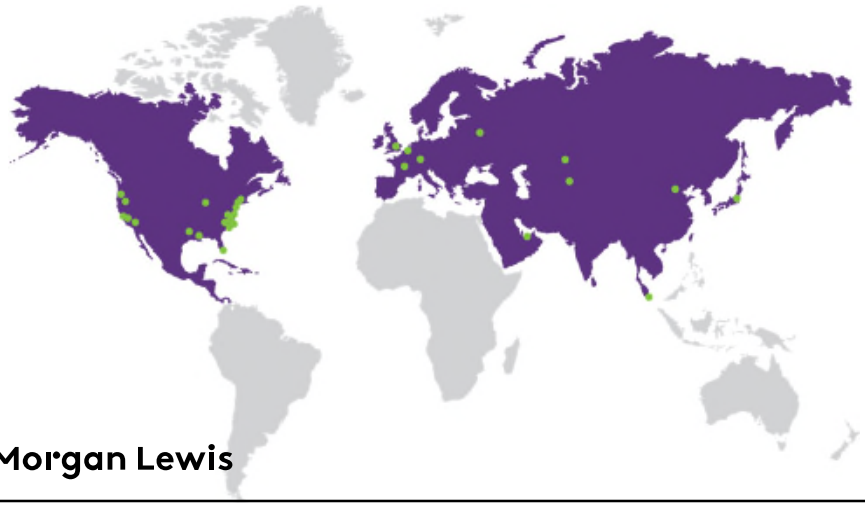
THANK YOU

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

Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Employment law tips for businesses in California

October 2015

Personnel administration is one of the most highly-regulated day-to-day functions of any business. California employment laws are complex and often vary significantly from federal law or address issues not addressed by federal statutes. While employers that manage to be in full compliance often rank high in best places to work, compliance is complex, requires devout attention to detail and even the most minor violation can lead to expensive litigation. The list below provides important examples of California employment laws that draw the attention of potential plaintiffs and the attorneys who would represent them.

Hiring new employees

When hiring an employee, California law requires an employer to provide written notice of, among other information, the rate and basis of pay, the regular payday, the location and telephone number of the employer's office, the name of its workers' compensation carrier and its paid sick leave policy, and subsequent notice of any change to this information unless the change can be found in the pay statement.

In conducting a credit check, an employer may not obtain consumer credit reports on applicants or employees in most non-managerial positions, except for those with access to confidential information or who have signatory authority on bank accounts.

Many companies explore various websites, such as LinkedIn and Facebook, in the process of reviewing candidates for most jobs. This may be standard practice elsewhere, but California law prohibits employers from asking applicants or employees to disclose a user name or password for the purpose of accessing personal social media or disciplining, discharging or retaliating against an applicant or employee who refuses to comply with a request for such disclosure.

Pay practices

California, among a few other states, requires employers to pay non-exempt employees overtime for work in excess of 8 hours per day and double pay for working more than 12 hours a day as well as over 40 hours per week. Hours worked over 8 in a day must be paid, but are not counted again when total hours worked the same workweek exceed 40.

Many employers pay non-exempt employees a salary, but that method of payment does not render such employees exempt. California requires employers who pay a "fixed salary" to non-exempt employees to pay overtime for work in excess of the daily and weekly limits.

Although the federal Fair Labor Standards Act permits some forms of pay averaging, California employment law prohibits it even when pay in a payroll period exceeds minimum wage, but does not include compensation for all hours worked.

While piece rate pay under federal law covers all hours of work when minimum wage and overtime standards are met, California law prohibits pay averaging and requires paid meal and rest periods for piece rate employees and may require that commissioned employees be paid for all hours worked "under the employer's control" when they are not engaged in commissionable activities.

California law requires employers to pay a minimum hourly wage ($9.00 per hour effective July 1, 2014 and $10 per hour on January 1, 2016) that is higher than current federal minimum wage and some municipalities require even higher minimum compensation (San Francisco minimum wage is $12.25 and San Jose minimum wage is $10.30 per hour).

California law also:

- Requires employers to comply with the Fair Pay Act effective January 1, 2016 ensuring that women performing the same or similar duties as male employees are paid at the same rate unless the employer can affirmatively show that differences are based on a bona fide factor other than sex
- Requires California employers to pay out-of-state employees who come into the state to work at California daily, weekly and double overtime wage rates
- Requires employers to pay a higher minimum salary for exempt employees than the federal law minimum
- Requires that pay statements accompanying pay checks identify up to 9 separate items, and imposes substantial penalties for failing to comply
- Requires employers to have written agreements with commission-based employees effective January, 2013
- Imposes serious penalties for willfully misclassifying employees as independent contractors, including posting a notice on the website that it has committed a serious violation by engaging in such willful misclassification
- Requires payment of final wages at the time of termination in most instances, subject to a penalty of up to 30 days' pay
- Requires payment of accrued and unused vacation pay on termination, subject to a penalty of up to 30 days' pay
- Entitles employees to get copies of their payroll records within 21 days
- Entitles employees and former employees to inspect their personnel records and get copies of their personnel records within 30 days
- Requires employers to keep pay records for three years
- Prohibits employers from offsetting an employee's debt to the employer from the final paycheck
- Permits a court to bar an employer from doing any business in California without posting a bond if the employer has been convicted twice of violating California's wage laws or failed to pay a wage judgment
- Requires employers to provide 2-10 minute paid rest periods during the work day and a 30-minute unpaid meal period for every 5 hours of scheduled work
- Requires employers to provide a "cool down" period of recovery to prevent heat illness when working outdoors in warmer weather, subject to a penalty of one hour of pay for failure to comply

Leaves of absence

- Permits employees (from date of hire) to take a pregnancy disability leave of up to 4 months and employers to reasonably accommodate a leave of undetermined length if the disability continues beyond 4 months
- Requires employers of 5 or more employees to continue group health coverage for pregnancy disability for up to 4 months, regardless of the employee's eligibility for FMLA leave
- Permits employees who take a leave for pregnancy disability to take an additional 12 weeks of family leave following the birth of the child or end of the disability related to the pregnancy
- Requires employers to continue group health coverage for employees during a family and medical leave, including employees who are on such leave following a pregnancy disability leave
- Prohibits employers from discriminating against employees who take pregnancy leave, requires employers to engage in an interactive process and, when reasonable, to provide as an accommodation an augmented disability leave beyond 4 months taken for child birth
- Provides employees on family leave benefits to substitute for lost earnings while on family leave through employee payroll deductions
- Requires employers to provide all employees a minimum of three paid sick days per year and to accrue such days at the rate of one hour for every thirty hours worked beginning after 90 days of employment
- Allows employees to use one-half of accrued and unused paid sick leave to care for sick relatives
- Permits employees leave for children's school activities, for jury duty, to vote on election day, and to testify on issues of domestic violence, sexual assault, and stalking or a victim of such conduct

Non-discrimination practices

- Protects employees not otherwise protected by federal law from discrimination based on sexual orientation, marital status, gender identity, gender appearance, military status and political affiliation
- Requires that all employment-related benefits be available to same sex couples as are available to spouses of the opposite gender
- Gives registered domestic partners the full protections of law
- Guarantees women the right to wear pants at work
- Imposes individual liability on supervisors who engage in unlawful harassment
- Imposes prohibitions against harassment on all private employers, regardless of size
- Requires employers of 50 or more to train all supervisors for 2 hours every 2 years on issues of harassment, discrimination and retaliation
- Requires employers to take all reasonable steps necessary to prevent and correct harassment and discrimination
- Protects an employee claiming a physical or mental disability if the employee can show that the impairment limits (even if not "substantially") a major life activity
- Creates an independent cause of action against an employer who fails to engage in an interactive process with a disabled individual to determine whether a reasonable accommodation is available
- Requires that accommodation to religious practices includes religious dress and religious grooming practices unless the accommodation would be an undue hardship
- Requires employers to provide reasonable accommodation for lactating mothers and includes breast-feeding in the definition of "sex"

Other laws in the workplace

- Creates a constitutional right to privacy that extends to the workplace
- Prohibits retaliating against employees who engage in numerous specific categories of conduct protected in the Labor and Government codes
- Prohibits employers from restricting employees who engage in most activities when off-premises and off-duty
- Protects the right of employees to discuss workplace issues with co-workers, including how much they earn
- Requires consent of both parties before recording any confidential or telephonic communications
- Requires employers of 75 or more persons to provide a "mini-WARN" 60-day notice to employees in the event of a mass layoff or relocation
- Denies employers the right to enforce covenants not to compete
- Entitles former employees in many circumstances the right to solicit customers of their former employers

These and other statutory, regulatory and case law requirements alone or intertwined with federal laws impose significant burdens on attorneys counseling employers, in-house counsel and human resources administrators, while granting a wide range of protections to applicants and current and former employees. Doing Business in California: An Employment Law Handbook (3rd Edition, October, 2016), available from the author, follows the flow of personnel laws and best practices from the hiring process through employment, including compensation, pre-termination, and post-termination issues and record-keeping and posting requirements.

Contact

If you would like further information, please contact:

Los Angeles

Arthur Silbergeld
Partner
Tel +1 213 892 9235
arthur.silbergeld@nortonrosefulbright.com

Arthur F. Silbergeld, identified by the Los Angeles Daily Journal as one of the Top 70 Employment Lawyers in California, defends employers in federal and state individual and class litigation and bench and jury trials involving wage, meal and rest period, termination, discrimination, and harassment claims and counsels companies across the broad spectrum of employment laws. A trial attorney with the NLRB early in his career, he also represents companies in union organizing campaigns, unfair labor practice trials, collective bargaining negotiations, and arbitrations.

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

ORRICK

5. Analyze All Collected Information

Once the information obtained in the audit is gathered, it must be systematically analyzed for compliance with legal requirements and for conformity with other company objectives. Virtually every audit will benefit from the development and use of detailed audit checklists or intake questionnaires. These documents provide a step-by-step method of analysis for a discrete subject area. All such checklists or questionnaires should be prepared or carefully reviewed by legal counsel.

The audit process should culminate with the preparation of a final report for distribution to upper management, which can be written or oral. Ideally, legal counsel authors the final report or is closely involved in all stages of its preparation. The report should be thorough and include conclusions concerning the audited policies and practices, potential compliance efforts and practical problems. Inevitably, the final report will contain highly sensitive information. Therefore, all reasonable steps must be made to preserve its confidentiality.

6. Solve The Problems You Identify

Once the audit is complete, it is important to remedy promptly any problems it identified. A failure to resolve those violations can increase the company's liability for penalties, possibly punitive damages, and other claims. In addition, a failure to address identified problems will impact the morale of those employees who worked hard to ensure the audit was successful. To respond to changing legal requirements and dynamic business changes, as well as to monitor progress made on prior audit recommendations, the audit should be renewed on a regular, periodic basis.

Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Fall Back On Insurance For Data Breach Fallout

Law360, New York (September 05, 2014, 12:10 PM ET) -- Even before the highly publicized Target Corp. data breach, it appears there is an article in the press every day announcing yet another incident. The incidents are not limited to the retail industry, but affect virtually every business sector. On Aug. 6, 2014, media outlets including the New York Times reported that a Russian crime ring had amassed the largest known collection of stolen Internet data — at least 1.2 billion username and password combinations, as well as more than 500 million email addresses. Since then, a company operating more than 200 hospitals announced that hackers had stolen data on 4.5 million patients, and a major supermarket company announced a large data breach involving customer credit card data. But the Target situation remains, to date, the most thoroughly analyzed, and provides a good case study for evaluating potential claims and losses that might arise from a major breach, and whether such claims and losses would be covered by insurance.

Cristina M. Shea

The Target incident, and the many that have been reported since, should be a wake-up call for all businesses to assess their exposure, and whether or not they are adequately protected in the event a breach occurs.

According to Target, the digital intruder accessed and stole data from about 40 million credit and debit card accounts from customers who shopped at Target between Nov. 17, 2013, and Dec. 15, 2013, through malware that was installed on its point-of-sale system in its U.S. stores. The intruder also purportedly stole certain other customer information for up to 70 million people, including names, mailing addresses, phone numbers or email addresses.

On March 26, 2014, the U.S. Senate's Committee on Commerce, Science and Transportation issued a report on the Target data breach, reporting that the intruders gained access to Target's network through a heating, ventilation and air conditioning vendor's computer systems. Target had given the vendor, a small Pennsylvania company, remote access to its network for electronic billing, contract submission and project management purposes. The intruders apparently stole the vendor's credentials for accessing Target's network using emails infected with malware. The committee's report suggests that Target failed to properly isolate its most sensitive network assets. And, according to the report, Target did not respond to multiple automated warnings from its anti-intrusion software that malware was being installed, and further did not respond to warnings regarding "escape routes the attackers planned to use to exfiltrate data from Target's network."

As fallout, Target now reports that it faces more than 100 lawsuits brought by customers, payment card issuing banks, shareholder derivative lawsuits and a number of state and federal governmental investigations.

In its most recent U.S. Securities and Exchange Commission Form 10-Q filing, Target states it maintains "$100 million of network-security insurance coverage above a $10 million deductible" and that this coverage, as well as "certain other customary business-insurance coverage has reduced" its exposure. As of May 3, 2014, Target states it received an initial payment of $13 million on its insurance claim from its "primary layer of network-security insurance." In an Aug. 20, 2014, earnings release, Target announced that since the data breach, the company incurred "total net breach-related expenses of $146 million, reflecting $236 million of gross expenses, partially offset by the recognition of a $90 million insurance receivable."

Cyberliability Insurance

In the wake of so many cyber breaches, cyberliability insurance should be a critical component of every company's risk management portfolio and comprehensive breach response plan.

In recent years, more than two dozen liability insurers have introduced new or revamped cyberliability insurance forms or endorsements. Current cyberliability insurance forms generally contain insuring agreements for first-party losses and a third-party liability, although the policies may differ in scope and format from insurer to insurer and depending on the size, industry, risks and needs of a particular company. These policies may also include other related insurance coverages, such as business interruption coverage triggered by interruptions in computer networks and damage to nonphysical property or data, professional errors and omissions liability, multimedia liability or crime coverage.

Cyberliability coverage may be placed as a stand-alone policy, as part of a "module" or coverage section in a "package" policy containing other coverage, or as endorsements to more traditional policies, such as property or business interruption. Where coverage is part of package policy or endorsement, it may share its limits of liability with other insurance in that package, such as E&O and multimedia liability coverage.

The first-party insuring agreement, often referred to as "breach response" coverage, typically covers the costs and expenses incurred in responding to, investigating and remedying a breach incident, and may pay the following costs: breach notification costs, the costs of maintaining a system for potentially affected persons to communicate with the company, the fees of a "breach coach" attorney, forensic examiner costs, costs to hire communications professional for the purpose of maintaining customer goodwill or reputation, costs to replace or restore data or electronic information, cyber-extortion payments, criminal rewards and remedial expenses, such as credit file monitoring, out-of-pocket expense reimbursement (e.g., to pay the cost of reissuing checks or credit cards) or identity theft insurance remedies. Coverage for these types of losses vary between policies and insurers and may be subject to separate terms and conditions and sublimits of liability.

The third-party cyberliability insurance agreement generally covers losses arising from claims made against the company, its directors, officers and/or employees for the unintentional disclosure of private information resulting in a risk of or actual identity theft, the misappropriation of private information, the failure to protect confidential information from misappropriation or disclosure, the failure to disclose or notify victims of a breach incident, violations of laws and regulations governing data protection and privacy, including certain regulatory actions. The losses paid under third-party cyberliability insuring agreements may include damages, judgments, settlements, defense costs, claims administration costs, consumer redress fund payments in a regulatory action.

As with other insurance, cyberliability policies contain a number of exclusions from coverage. Common exclusions involve: dishonest, fraudulent or criminal acts (e.g., conduct exclusion); intellectual property violations; products liability; "anti-spam," "blast-fax" and similar laws; infrastructure failures; compromised usage of certain technology products and software; and content created by third parties. Those in the market for cyberliability insurance should tailor exclusions to be as narrow as possible. With respect to these exclusions, the application of the "conduct exclusion" should be strictly limited to dishonest, fraudulent or criminal acts committed by the company and/or its senior management. Although the majority of data and security breaches are committed by negligent acts, (e.g., the failure to properly configure software or firewalls), many breaches are caused by malicious acts, often perpetrated or assisted by insiders. Thus, it is important to carve out an exception to this the conduct exclusion for "rogue" or disgruntled employees, to guarantee coverage for malicious conduct by an insider. Also, the conduct exclusion should apply only after a final adjudication, or determination, that the excluded conduct did, in fact, occur.

Cyberliability insurance is a rapidly developing market and insurance products currently on the market vary widely in the type of coverage provided. Purchasers of this insurance should ensure that the coverage they purchase is tailored to the specific policyholder's needs. Major carriers offer policies that treat data security and privacy risks as a combined form of liability and crime coverage. Under these forms, coverage for liability for a "claim" arising from a data security or privacy event typically is claims-made and written on either a duty-to-defend or reimbursement basis. In general, to trigger potential coverage under the policy, only timely written notice or tender of claim is required. Coverage for losses that may arise "preclaim," such as breach notification, forensic investigations and crisis management expenses, are treated similar to crime or fidelity bond losses and are subject to the more involved (and potentially tricky) "discovery" notice trigger common in bonds, commercial crime and other first-party insurance policies. Discovery-triggered policies may require not only timely notice of claim but submission of a sworn proof of loss within a short time frame. This could give rise to privilege concerns because the company may not have a privileged relationship with the insurer, or its counsel, and may contain contractual limitations periods for resolving disputes.

Coverage For Cyber Events and Related Matters Under Traditional Insurance Policies

Recent breach incidents have given rise to more than just claims for data security and privacy liability, and thus may trigger other liability and first-party insurance. Following a number of disclosures concerning its data breach, Target's investors filed putative shareholder and derivative actions against the company's board of directors and senior officers, claiming misrepresentations in connection with securities disclosures and breaches of fiduciary duties relating to the company's data security risks and responses. These types of claims may be covered under directors and officers insurance policies. A company that allows its personnel to invest in company securities through a 401(k) or other benefit plan may be exposed to claims by the participants of the plan under the Employee Retirement Income Security Act for breaches of fiduciary duty by plan trustees, which may be covered under fiduciary liability insurance policies. If a company provides professional services to others for a fee or other compensation, and that company's security is compromised, it may be subjected to claims by clients or customers, which may implicate the company's E&O coverage. Fidelity or financial institution bonds and commercial crime policies may contain coverage for certain direct losses caused by cyber or computer fraud, and property policies may contain coverage for damage to certain electronic data. Finally, some privacy claims may also be covered under traditional commercial general liability policies.

Insureds should not presume the absence of coverage under their traditional policies without carefully considering the nature of the loss and the language of the policy at issue.

In the end, coverage will turn on the specific facts of the claim and the specific policy language at issue. Consideration should also be given to controlling legal standards that may have developed in the relevant jurisdictions, which can vary significantly.

In the end, a company's first-party and third-party liability insurance program is a critical part of its planning for and response to a data breach. Companies should review their full coverage portfolio for potential overlapping, or complementary, coverage for claims arising from or related to security breaches. Insureds should also seek guidance from experienced coverage counsel not only to maximize their potential for coverage for existing cyber-related liability claims under traditional lines of insurance, but also to evaluate whether they would benefit from specialized cyber coverage.

—By J. Andrew Moss, Cristina M. Shea and David E. Weiss, Reed Smith LLP

Andrew Moss is a partner in Reed Smith's Chicago office.

Cristina Shea and David Weiss are partners in Reed Smith's San Francisco office.

ReedSmith

Alert

Insurance Recovery

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Douglas E. Cameron
Partner, Pittsburgh
+1 412 288 4104
dcameron@reedsmith.com

David E. Weiss
Partner, San Francisco
+1 415 659 5966
dweiss@reedsmith.com

J. Andrew Moss
Partner, Chicago
+1 312 207 3869
amoss@reedsmith.com

Cristina M. Shea
Partner, San Francisco
+1 415 659 4736
cshea@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Cyber and Data Security and Privacy Liability: The Problem Isn't Going Away. Get Out in Front of the Problem By Insuring Your Risks.

On August 6, 2014, the *New York Times* – and other media outlets – reported that a Russian crime ring had amassed the largest known collection of stolen Internet data – a cache of at least 1.2 billion user name and password combinations, as well as more than 500 million email addresses. The sheer volume of this stolen information underscores the fact that staying ahead of hackers has become an increasingly losing battle. Despite the publicity and increasing urgency in addressing this concern, data security breaches are becoming more frequent, more severe, and more costly, and have increasingly greater consequences for the company and its management. For example, the *New York Times* report comes on the heels of Target's recent announcement that its losses related to its data breach during the 2013 holiday season were expected to top $148 million, resulting in a "hold" rating on its stock and lowering its earnings forecast.

A string of high-profile data breaches at well-recognized companies, hospitals, professional firms and restaurants make clear that no business is immune from this risk. This, along with increased regulatory scrutiny and reporting requirements and well-publicized lawsuits against company boards and management by shareholders and financial institutions, has elevated cybersecurity to the single most important issue to board members and management, according to a recent survey by EisnerAmper.

One thing is clear: companies must be proactive and get out in front of the problem by including an assessment of their coverage needs, and any existing coverage they may have, as part of a comprehensive breach protection and response strategy and security plan. Waiting until a breach occurs may be too late.

ReedSmith

The landscape for insurance covering these types of risks is evolving and changing rapidly. Historically, policyholders have looked to commercial general liability (CGL) policies for defense and indemnification of third-party claims. Alternatively, coverage for losses related to a policyholder's property may exist under a first-party property policy. Liability for these losses has also spawned shareholder lawsuits, resulting in claims for coverage under D&O policies. But the insurance industry is contesting coverage of cyber risks under these types of policies, and is making every effort to exclude coverage from most new CGL and property policy forms. At the same time, the market has seen an influx of cyber-specific policies, but coverage under these policies can vary widely from policy-to-policy and from industry-to-industry, and the forms themselves differ greatly in their terminology and structure. Moreover, because these are relatively new insurance products, it will be some time before policyholders have definitive guidance from the courts on how coverage under these new policies will be interpreted.

With coverage being increasingly limited under traditional policies, and with the breadth and uncertainty of coverage offered under cyber-specific policies, companies should seek guidance from experienced coverage counsel to maximize their potential coverage under both cyber-specific and other insurance coverage – well before they face a cyber crisis.

If you are considering this type of coverage, or are interested in determining whether this type of coverage is appropriate for your enterprise, please contact one of the authors of this Alert, or the Reed Smith attorney with whom you frequently work.

ReedSmith

The business of relationships.

Does Your Cyber Risk Policy Protect You In the Event of an Insider Attack or Data Breach?

14 October 2014

Reed Smith Client Alerts

Author(s): Brian T. Himmel, J. Andrew Moss, Robert H. Owen

News & Knowledge

Practice Areas

Insurance Recovery

Cyberliability

Offices

Chicago

Pittsburgh

Protecting a company against data breaches requires not only measures to prevent the adverse cyber event, but also adequate insurance to minimize the financial impact should such an event occur. Unlike traditional lines of insurance for which there is substantial uniformity among the coverage available in the marketplace, the evolving market for data security and privacy liability ("cyberliability") insurance coverage reveals significant differences in the scope of coverage afforded under these policies. Policy forms may vary widely depending on the particular insurer and the industry served, reflecting material differences in contract language, terminology and structure. As a result, whether coverage is available under a particular cyberliability policy requires a careful analysis of the nature of the event as measured against the terms of that policy. What once appeared to have been comprehensive coverage may be revealed to have significant gaps.

A coverage gap that may exist under some policies is for ***insider*** cyber attacks. While ***external*** attacks receive substantial news coverage and many companies have become more vigilant and better prepared to prevent an external cyber attack, a recent study published in the *Harvard Business Review* finds that businesses may be far less equipped to stave off attacks involving insiders – employees, vendors, suppliers and others who may have authorized access to critical or sensitive data. Liability insurance protection – even under specialized cyberliability policy forms – may potentially lag behind on this important issue. It is therefore critical to understand the scope of coverage provided under your company's cyberliability policy in response to insider attacks or data breaches.

In evaluating whether a particular policy adequately protects against both external and insider cyber risks, it is important to closely review the insuring agreements and any exclusions that may apply to such claims. Some forms, for example, expressly exclude coverage for dishonest or fraudulent conduct by any Insured, including claims arising out of an Insured's collusion or assistance provided to third parties. Other policy forms expressly exclude coverage for any unauthorized use or accessing of a computer, network or data storage device by an Insured. If the policy at issue defines an "Insured" to include current or former employees, insurers may assert that these exclusions are triggered in many situations for which the company thought coverage existed.

In contrast, other policy forms take a more constrained approach, excluding claims involving only a limited class of insiders. For example, conduct exclusions in some policy forms only preclude claims arising out of an act, error or omission of a director, officer, or senior manager, rather than by ***any*** current or former employee.

Thus, in evaluating policy forms when purchasing or renewing coverage, it is important to understand how differences in policy language – including policy definitions and exclusions – may have a significant impact on the scope of coverage available for a cyberliability claim, particularly for claims arising out of malicious conduct by "rogue" employees or other insiders. Companies considering cyberliability coverage or interested in determining whether certain types of claims may be included as

an insured risk under a particular policy form should therefore seek guidance from experienced coverage counsel to evaluate that coverage. Because liability insurance should be a vital part of any company's comprehensive data breach response plan, the time to identify and address potential gaps in coverage is ***before*** an adverse cyber event occurs.

Client Alert 2014-269

ReedSmith

The business of relationships.

Hackers Don't Care About the Terms of Your Insurance Policy: The Importance of Retroactive Dates and Extended Reporting Periods in Effective Cyberliability Insurance Coverage

19 November 2014

Reed Smith Client Alerts

Author(s): Brian T. Himmel, J. Andrew Moss, David E. Weiss, Cristina M. Shea

News & Knowledge

Practice Areas

Insurance Recovery

Cyberliability

Offices

Chicago

Pittsburgh

San Francisco

A recent study reports that the median amount of time between an intrusion into a company's computer network and the discovery of the incident is ***229 days***. The difficulty and length of time in detecting cyber infiltrations may be critical in the context of cyberliability insurance coverage.

A typical cyberliability insurance policy is written on a claims-made basis, providing coverage only when the discovery of loss or resulting claim occurs during the policy period. Some cyberliability policy forms may, however, require that both the breach event and the discovery of loss (or resulting claim) occur during the policy period. Unfortunately, hackers do not take the terms and conditions of a company's insurance into consideration. So what happens when a breach is discovered three months into the policy period but, unbeknownst at the time, the intrusion actually occurred six months before, or even earlier? If your company's cyberliability insurance policy excludes breach events occurring before the inception of the policy period, the company could find itself without coverage for an otherwise-covered claim or loss.

Retroactive dates and extended reporting periods provide two methods to avoid such a gap in coverage. Retroactive dates extend the policy's coverage back to a date earlier than the actual policy period, with the goal of covering events that already occurred (or are occurring), but had not been discovered at the time the policy was purchased. An extended reporting period lengthens the period of time, beyond the expiration of the policy period, during which a claim or loss can be made against the insured and reported to the insurance company, so long as the event giving rise to the claim occurred before the end of the policy period. Extended reporting periods may be utilized when changing insurance companies to ensure that the cyberliability policies provide continuous, non-interrupted coverage.

These two approaches can be seen using the following hypothetical:

- Insurance Company A issues Policy 1 with a policy period from January 1 – December 31 of Year 1;
- Insurance Company B issues Policy 2 with a policy period from January 1 – December 31 of Year 2; and
- A breach occurs during Year 1 but is not discovered until Year 2

A retroactive date in Policy 2 that extends back in time to include Year 1 will enhance coverage under Policy 2 for a claim or loss resulting from the breach. So long as the breach occurred after the retroactive date, coverage is available under Policy 2 because it is triggered by the resulting claim or discovery of loss that occurs during its policy period (i.e., during Year 2). Purchasing an extended

reporting period for Policy 1 will facilitate coverage under that policy for the claim or loss arising under the same scenario. Although the breach is not discovered until Year 2, so long as notice of the breach is provided during the extended reporting period, coverage is available under Policy 1 because the breach event took place during its policy period (i.e., during Year 1).

The willingness to include a retroactive period or offer an extended reporting period may vary among cyberliability insurance carriers. The length of the retroactive period or extended reporting period – and whether an additional premium will be required for either – will need to be negotiated on an individual policy basis. Retroactive dates and extended reporting periods can provide a critical protection under a cyberliability insurance program, given the delays that may exist between a breach and its discovery.

Liability insurance should be a vital component of any company's comprehensive data breach response plan. The time to identify and address potential gaps in coverage is before an adverse cyber event occurs. Thus, when purchasing or renewing coverage, it is important to understand how retroactive dates and extended reporting periods can impact the coverage available for a cyberliability claim. Companies considering cyberliability coverage should therefore seek guidance from experienced coverage counsel to evaluate their coverage.

Please contact the authors of this Alert; the Reed Smith Insurance Recovery Group's Global Practice Group Leader, Douglas E. Cameron; or any Reed Smith coverage attorney with whom you routinely work for assistance or with questions.

For the second year in a row, *U.S. News-Best La*wyers "Best Law Firms" named Reed Smith its "National Law Firm of the Year" in Insurance Law (2014-2015). In addition, the group is named among the best policyholder coverage practices by *Chambers USA*, *Chambers UK*, *Legal 500 US* and *Legal 500 UK*. American Lawyer Media's *Legal Intelligencer* named Reed Smith's Insurance Recovery Group one of Pennsylvania's "Litigation Departments of the Year" for 2014 - the only policyholder-focused firm recognized in the Pennsylvania-based publication - and *The National Law Journal* named the Chicago Insurance Recovery team the 2014 "Chicago Litigation Department of the Year: Insurance."

Client Alert 2014-305

ReedSmith

Client Alert

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Mark S. Melodia
Partner, New York
+1 212 205 6078
mmelodia@reedsmith.com

David E. Weiss
Partner, San Francisco
+1 415 659 5966
dweiss@reedsmith.com

Cristina M. Shea
Partner, San Francisco
+1 415 659 4736
cshea@reedsmith.com

Christine Nielsen Czuprynski
Associate, Chicago
+1 312 207 6459
cczuprynski@reedsmith.com

Matthew D. Rosso
Associate, Philadelphia
+1 215 241 1220
mrosso@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Data Breaches Are Not Academic: Colleges and Universities Should Take Appropriate Steps To Avoid or at Least Minimize Their Exposure

Data breaches at colleges and universities are on the rise. These institutions are targets because their networks have access to a large amount of private information, including educational and medical records, as well as employees' personal data. But in other instances, their systems are being attacked for malicious sport. According to the Ponemon Institute, data breaches at academic institutions cost in excess of $300 per compromised record. As illustrated by a recent incident at the University of Maryland (where approximately 300,000 students' personal information may have been compromised), the potential financial and reputational impact could be crippling.

Data breaches will happen, but academic institutions should take certain measures now to protect – or at the very least minimize – their exposure in the event of a breach.

- ***Implement privacy and security policies and procedures that are known and adhered to by the institution:*** A privacy and security policy is critical to ensure that the institution: prevents the unauthorized access to devices and systems; implements technical security controls; routinely updates its process of analyzing potential cybersecurity threats; and controls and/or limits student and/or employee access to information technologies and systems. To mitigate potential claims, steps should be taken now to ensure that training and compliance programs are in place, that such programs are regularly updated, and that employee attendance is mandated and tracked.
- ***Prepare a corrective action plan in the event of a breach.*** Institutions must have an immediate response – both internally and externally – in the

event of a data breach. The response should reach all relevant parties, disclose the breach, describe mitigation efforts, and address questions that will arise.

- ***Enhance privacy and security-related language in vendor and partner agreements.*** Liability risks for data breaches may be mitigated through the front-end assessment of contracts and business relationships. Institutions should: review vendor and partner agreements for indemnity and warranty provisions that may offer protection in the event of a data breach; review the privacy and security policies of all business partners; and analyze the gaps in indemnity protections, including whether the college or university has the right to control the defense, select counsel, and make settlement decisions.
- ***Consider cyber insurance.*** Traditional policies, such as property, errors and omissions, and comprehensive general liability, may cover certain cyber-related losses. However, these risks are now frequently excluded, and insurers resist paying claims under such policies, even without specific exclusions. Cyber-liability policies address data breach risks, and will cover specific costs that will likely not be covered under a traditional policy (e.g., forensic investigation, breach response and notification costs). Moreover, many of these policies cover the institution's first-party losses, as well as associated breach response costs, including a forensic investigation, public relations experts, and support teams for customer queries and client care. There is no recognized standard form for cyber insurance, and terms may be negotiable, so it is important to carefully review proposed policy forms to make sure they meet the needs of the institution.

Reed Smith's Information Technology, Privacy & Data Security Group comprises nearly 100 lawyers globally who help clients put in place cyber-risk-reducing legal policies, disclosures and procedures, and help train administration, faculty and students to make them effective. Our team works with boards and other key stakeholders to teach about data risks from the top. We can help review vendor and joint venture documents for data risks, and work with IT, HR, Records and others to establish strong data governance. If a data crisis still arises, the Reed Smith team has advised on approximately 500 data breaches, responded to government inquiries, and defended more than 70 data-centric class actions.

Reed Smith's Insurance Recovery Group similarly is uniquely equipped to assist clients in maximizing their insurance assets in response to a data breach. If you would like to purchase insurance to protect against the possibility of a data breach, or if you find yourself faced with a breach and need assistance with submitting a claim for insurance coverage, please contact the authors of this Alert, or any of the Reed Smith attorneys with whom you routinely work.

Practice Pointers for Deponent and Witness Preparation

By David Perrott – December 20, 2012

While we all want to make sound decisions, the amount of thoughtful attention we are willing or able to invest in that process varies according to the situation we find ourselves in and from person to person. When we lack motivation or ability, we fall back on mental shortcuts to help us make decisions. Hence, it is important to know which of such shortcuts your fact finder may use when deciding whether your witness's testimony helps or hurts your case, and to factor this into your preparation strategy and communications training.

The particular array of mental shortcuts varies by witness, subject matter, and fact finder—ranging from non-verbal behavior such as fidgeting, tone of voice, and eye contact, to judgments about the witness's appearance and competence, to preconceptions and attitudes about the underlying case and the role of the witness within the case. During a trial simulation on the East Coast in which the degree of West Coast corporate witnesses' due diligence was at issue, the New York jurors made negative snap judgments about the executives' testimony based largely on their deep tans. It was easy for jurors to concur with opposing counsel that these witnesses had dropped the ball, when they were clearly so busy "baking in the California sun." Fortunately, the trial simulation was in late November, a couple of months before trial, allowing plenty of time to fade those apparently telling tans.

It is possible to obtain very detailed feedback on witness mannerisms, demeanor, likeability, credibility, overall impact, and reactions to ostensibly favorable or unfavorable deposition testimony through evaluating excerpts of videotaped depositions or mock testimony in focus-group or online-jury research. Such research can tell you in advance of trial the various mental shortcuts that decision makers may make about your key witnesses, particular fact pattern, and venue. It can also help quantify the risks associated with certain witnesses, identifying both strengths and remedial areas to address in preparation sessions.

Prepare the Whole Person—Not Just Your Substantive Agenda

Deponent preparation is often conducted under intense time pressure. There is a tendency to adopt a detached, functional, evidence-oriented approach to preparing a person to testify, which tends to focus more on the facts of the message and less on the capabilities and idiosyncrasies of the messenger. We often assume that because someone seems forthright and likeable in conversation, or because he or she

is smart and functions at a high level in the workplace, he or she will naturally come across well at a deposition or trial. When the deponent is an important or a long-term client, there is also the risk that well-intentioned but uncharacteristic constructive feedback from you will ruffle his or her feathers. Conversely, when the deponent is someone you do not know very well, it can be awkward to play armchair therapist. At the same time, witnesses may feel social pressures not to burden or distract the trial team with their personal concerns about testifying. The net result can be that potentially serious subsurface issues go unacknowledged and unaddressed.

This happened with a CEO of a technology company defending allegations of patent infringement. The CEO was fearless, self-assured, and charming in conversation when things were going his way, as usually they are. But he was also domineering, with an instinct to seize control of the situation when threatened. He viewed the lawsuit as a distraction from the more important business of running his company, and was vexed that a competitor was trying to steal his profits. Attorneys recommended professional communications training but, after indulging some preliminary pointers from the trial team, he opted to cancel the in-depth preparation. Although the CEO fared quite well on direct examination at trial, opposing counsel was able to goad him on a sensitive issue during cross-examination. The CEO became combative and visibly frustrated when he was unable to gain control of the situation. The jury ultimately perceived him as unlikeable, condescending, and elitist, and the trial team regretted not being insistent on more comprehensive communications training.

What could the CEO's attorneys have done to prepare him better? While attorneys and deponents vary greatly in their insight and comfort level with the deeper psychological aspects of witness preparation, some initial questions to draw out underlying issues include: What questions do you have about the process of being deposed or testifying? What do you think you will do well? What kinds of things do you think you will find challenging? What would you most like to work on? If your deponent has been deposed before, use the experience as a starting point for discussion. Begin by exploring self-perceptions about his or her prior performance, and how, if at all, he or she would like to do it differently this time.

One practical technique that works for nearly every attorney and deponent is reverse role-play. You will play the role of the deponent, and the deponent will role-play opposing counsel and pose to you the questions he or she most dreads being asked. This process will be both cathartic for the deponent and revelatory for you. It allows you to discover your deponent's Achilles' heel in a generally non-threatening manner. Some of the questions will point to hot-button case issues that you were already intending to address, but others will likely surprise you and provide a window into anxieties about peripheral, irrelevant, or inadmissible issues and concerns that might otherwise have needlessly elevated fear and created internal distractions while testifying. The reverse role-play also then serves as an easy segue into exploration of potential psychological vulnerabilities in terms of how the deponent typically reacts when having to explain himself or herself under duress.

While role-play would likely have helped the CEO's attorneys discover ahead of time more of his vulnerabilities as a witness, there was also his tendency to attempt to seize control of the situation when under pressure. In the courtroom, this tendency manifested itself as interjections, interruptions, and non-responsive answers often starting with "That's irrelevant. This is what you need to understand . . ." Explain to witnesses that, perhaps unlike their business experience, testifying is not a situation in which they can succeed by trying to change the rules of the game. Brace them for the reality that being deposed or cross-examined will almost certainly be an unpleasant experience, that much of the time they will not get to explain themselves fully or as they would like, and that they will need to surrender to the process and trust that you and the judge will interject as needed to ensure that opposing counsel plays by the rules. While small doses of well-timed righteous indignation can be effective, generally advise your witness to be relentlessly polite, especially in front of a jury. Build your witness's trust in you that through direct and redirect, you will elicit his or her testimony, without the witness needing to try to control the process.

Communicate the Big Picture, Case Themes, and Home Bases

The counterpart to finding out what your witness most dreads being asked about is finding out what the witness thinks are the take-home points of the testimony. Ensure that you are both on the same page as to what that is. Synthesize your case into overarching themes that tell your case story—perhaps five or six themes for a typical business dispute—and determine how your witnesses fit together like jigsaw pieces to tell that story. Assuming no countervailing procedural concerns (e.g., about discoverability), educate your witnesses how your case fits together in terms of themes, and to which themes the witness's testimony corresponds. These themes are your witnesses' safe haven, providing a mental map that will help them orient and frame their answers on both direct- and cross-examination. It will also turn moments of weakness on cross-examination into positions of strength. A leading question from opposing counsel demanding a negative admission can sometimes be used as an opportunity to reiterate a case theme to remind the trier of fact of the fundamental strengths of your case. Specifically, a deponent or witness can respond, "Although it is true that [negative admission], the bottom line is [case theme]." For example, a defense witness in a securities-fraud case might respond, "Although it is true that we did not disclose that fact in our public filings, the bottom line is that this information was already publicly available and these were highly sophisticated investors."

Hero-or-Zero Syndrome

Deponents and witnesses may become needlessly anxious by overestimating the importance of their testimony to the case outcome. For a deeply offended small-business owner accused of wrongfully terminating a minority employee, this perception was acute and led to a disastrous deposition with a litany of angry, unresponsive answers. He was convinced that if only everyone could see things his way, the lawsuit would go away. A helpful part of his trial preparation consisted of listing the key case themes on one side of a page, the names of everyone speaking on his behalf at trial (his attorney and other witnesses) on the other, and drawing lines from each theme to the witness(es) responsible for conveying a particular theme. Once he understood that his role was as part of a team, he became more cooperative and his answers more responsive. The process of educating your witnesses about the themes in your case and their position as pieces in a thematic evidentiary puzzle can aid them both mentally and emotionally.

Practice the Process of Testifying

The mechanics of careful testimony are different from those of good conversation. Testifying requires careful listening, thinking, and responding in ways that would seem stilted and unfriendly in a normal conversation. Witnesses need to be told this; it is not obvious. Habits of normal conversational smoothing to maintain positive affect and a flow in the dialogue can lead to dangerous volunteering of information and more follow-up questions. Witnesses should be trained and empowered to avoid answering questions they do not completely understand, by asking for questions to be repeated or rephrased as needed. This preparation step is especially important for tentative, frightened, or otherwise vulnerable witnesses. Similarly, witnesses should be empowered and trained to review documents carefully before answering questions about them, and to correct mistakes in their testimony as soon as they realize them. If they understand that jurors and judges do not expect witnesses to remember everything, it will be easier to refuse opposing counsel's attempts to make them speculate or agree to an unfavorable "spin," which is consistent with the oath they've given to tell nothing but the truth.

In a videotaped deposition, deponents should generally respond directly to the camera in a friendly, educational tone, bearing in mind that the ultimate audience is a neutral jury or judge curious about what the deponent or witness has to say. At trial, it is best for them to direct their answers to the jury or judge as much as possible. This orientation can also help a deponent from being discombobulated by opposing counsel. The camera magnifies body language, especially fidgeting and head-turning to look at counsel, so this should be controlled as much as possible. Things to fidget with, such as pens and rubber bands, should be placed out of reach. If the camera can be positioned behind opposing counsel with defending counsel seated adjacent, all across the table from the deponent, this will minimize the impact of head-turning on the videotape, which jurors otherwise tend to interpret as a floundering deponent looking to counsel for help. Deponents should adopt a relaxed, open posture, leaning slightly forward, and try to avoid swiveling in moveable chairs. They should take a breath before answering each question to minimize the risk of thinking aloud and to allow time for potential objections. These techniques will give the deponent control over the pace of questioning.

It is best to refresh recollection of case facts prior to practicing testifying, rather than during. While integrating the two steps seems more efficient, it tends to overwhelm the witness mentally, undermine his or her confidence, and give you a potentially misleading read on the witness's capacity to testify effectively.

Testifying is a skill that can be learned with proper training and improved with practice. Where time permits, begin with a mock direct examination to build a witness's confidence before moving onto more stressful practice cross-examination. It is better in both scenarios to pose questions on the fly based on a detailed topic outline, rather than working from a script. Scripts can give a false sense of security to the witness, who may feel cast adrift if you divert from it at trial. Moreover, working from a script on direct

makes cross-examination more stressful, and potentially sets up an undesirable contrast in demeanor of what jurors often perceive as the “rehearsed” versus the “real” witness.

Approach hot-button case issues from different angles and use different questioning styles, sometimes posing a series of short, closed-ended questions and other times open-ended questions, working through the sequence forward, backward, and from different starting points, so that the witness becomes comfortable marshaling an answer no matter what angle the questioner pursues. Also encourage the witness to practice using case themes and inject themes via the “although it’s true” formula described above. This process requires more effort from both of you, but will prepare your witness to be more resilient during cross-examination.

What should you cover when you only have a few hours to prepare a witness? Teach the general pointers outlined above, discuss case themes and which themes the witness is responsible for conveying, spend five or ten minutes on substantive direct-examination questions to accustom the witness to your personal style, and then use the remaining time to practice cross-examination. Ideally, use a colleague unfamiliar to the witness to act as opposing counsel.

Videotaping

People vary in their level of self-awareness and openness to accepting and assimilating feedback about their behavior. Videotaping can be an effective tool when used judiciously to illustrate examples of good witness behaviors versus those that detract from effective testimony.

This process proved helpful for a claims adjuster in an insurance-coverage dispute. The claims adjuster was personable enough in everyday conversation, but stiffened his voice and body noticeably during the practice session. To illustrate his change in demeanor, the trial team videotaped him answering questions about his family’s last vacation (during which he was animated and personable), as well as answering questions about the case issues. The obvious contrast made him aware of behaviors that he was then able to address to bring out more of his personality and maintain his likeability while testifying. Videotaping has also led to eye-opening moments for a number of CEOs who were surprised to see for themselves how often they interrupted the questioner and gave non-responsive answers in an attempt to take control of the situation when feeling threatened or disempowered.

Common Problems and Potential Fixes

Too Reactive to Opposing Counsel

In one case, an expert witness in a copyright dispute had a harrowing deposition during which he felt humiliated by opposing counsel. As a result, his primary goal for trial was to turn the tables and restore his self-esteem. This egocentric goal diverts attention away from honest, clear communication to the

fact finder, be it judge or jury. Witnesses in this state of mind need to be educated that the audience for their testimony is the fact finder, and that it is difficult to educate and persuade this audience when focused on trying to outsmart opposing counsel. Rather, witnesses should conceive of opposing counsel as a source of questions that are opportunities to educate the jury or judge about something that the witness knows. It may help your witness to say silently to himself or herself after each question "thank you for asking me that," and then turn to face the jury or judge and focus on teaching them. It is a small tool that can make a big difference in the likeability and credibility of a witness.

Chatty Cathys and Nervous Nellies

You can throw a lifeline to witnesses who tend to talk too much or talk too little, by preparing them with cues as to how long an answer you anticipate. Instruct the witness to respond in just a few words when you preface your question with "Explain briefly . . ." or in two or three sentences when asked to "explain in detail." A demonstrative with bullet points, a timeline, or a flowchart can also help keep a nervous or talkative witness on track.

The undesirable practice of "thinking aloud" often underlies a tendency to talk too much while testifying. When it is difficult to determine in real time whether a witness is eventually going to agree with or deny the crux of the question, he or she is thinking aloud. Urge the witness to take a breath before answering, and not to open his or her mouth to speak until he or she knows the very last word he or she is going to say. It takes considerable practice, but with discipline and focus, better habits can be formed.

If you suspect that issue-specific anxiety is the underlying problem, the role-play technique mentioned earlier may help identify the root concern. Other times, a witness's loquaciousness may stem from a combination of articulateness and detail-orientation, where the witness is trying so hard to be precise—especially during cross-examination—that the witness instead comes across as evasive and persnickety. When lawyers say that lawyers often make the worst witnesses, this is often why. Expert witnesses sometimes suffer the same problem. A strategy to deal with this is to assure the witness that you will be taking careful notes to follow up as needed on redirect to allow more precise answers. Another method is to get the witness comfortable with answers such as "Not exactly," "That's a mischaracterization," or "That's not quite right," which shift the burden back to opposing counsel to deconstruct complex questions.

If a witness is generally terrified at the notion of testifying, a prior visit to the courtroom may help (as well as techniques such as guided imagery and systematic desensitization, which are beyond the scope of this article). While on the stand, the witness should focus on deep, calm breathing, muscle relaxation, and open posture, which will help alleviate stress.

An example involved a ground-crew staff member for an airline, testifying in an employment case. The witness was very ill at ease about testifying. In addition, he was extremely suggestible, acquiescing at all the right times on direct and at all the wrong times on cross. The most helpful elements of preparation for him were showing him pictures of “unfriendly” opposing counsel and “friendly” defense counsel so that he would know who was trying to trick him and who was not. It was also helpful to advise him on the themes of his testimony as well as three or four leading questions he should be on the lookout to deny because they were false. Also important was empowering him to ask for a question to be rephrased and simplified when needed.

Witnesses Who Lack Compassion

Many jurors construe case issues from a micro-, consumer/employee perspective. When high-level executives take a macro-perspective on company issues, or claims adjusters and senior human-resource managers use jargon and dispassionately describe claim denials, reductions in force, and terminations, they may appear callous to jurors. To position the witness to educate the jury in an empathetic manner, educate the witness about jury-pool demographics, and to focus on making eye contact with individual jurors to encourage the witness to humanize the testimony. It may also be helpful for the witness to imagine that he or she is justifying a tough decision or a negative outcome to a neighbor or a family member. During a videotaped deposition, the deponent should imagine that behind the camera is someone that he or she cares about to whom he or she is explaining his or her actions.

Witnesses Who Dress Inappropriately

Deponents and witnesses should dress in a way that strikes a balance between comfort, appropriateness, and showing respect for the court. If a witness dresses in a way that violates jurors’ expectations for a job role or is too attention-getting, jurors may quickly draw negative inferences. If a witness’s appearance is surprising, it can be a distraction, or worse, imply that the witness may be someone who is prone to act unexpectedly.

Experts Who Misunderstand the Needs of Their Audience

Experimental research suggests that jurors perceive experts with moderate confidence as more credible than experts who are highly confident and that likeability enhances credibility. Expert witnesses should think of themselves as educators, and focus on the jury like a classroom. They should treat questions received on direct and cross as opportunities to educate the jury. Often, expert witnesses become accustomed to discussing case-related topics with attorneys or colleagues, and greatly overestimate the jury pool’s understanding of the issues—sometimes believing that they need to use jargon to “sound expertly.” This is a mistake because jurors may evaluate the expert in a cursory manner by the mental shortcut of “she sounds impressive” rather than by the substantive content of the testimony. Discuss this with your expert ahead of time and ensure that the questions you pose on direct are comprehensible to the jurors so that you work as a team with your expert to educate the jury. Jury research can be highly informative for finding simple local analogies to explain difficult points. Bear in mind the helpful adage that if your jurors only need to tell the time, do not teach them how to build a watch.

Another problem that experts may encounter is that their desire to be precise leads to unnecessary hedging when describing the state of knowledge in a field, which can inadvertently diminish the expert's credibility in the eyes of the jury. Instead of over-qualifying answers by listing exceptions to general principles supporting the theory or conceding lack of certainty on cross-examination in light of them, it may be better to respond with just the general principle, couching it as "The generally accepted view in our field is . . ." or that "The weight of the evidence in our field is that . . ." Jurors will not know how to weigh the outlier findings themselves, so highlighting them out of context can be misleading.

Non-English-Speaking Witnesses

A big question with a non-English-speaking witness is whether or not to use a translator. This may put a question mark in jurors' minds over the credibility of a witness, because they cannot pass their own "smell test." It is also considerably more onerous for jurors to pay attention throughout the slow rhythm of translated testimony. But sometimes you have no choice. If you do use a translator, ensure that your witness does not respond either verbally or non-verbally before hearing the translated question, as some jurors could infer that the witness is "hiding" behind the translator, especially on more difficult questions. During voir dire, explore whether there are speakers of the non-English language in the venire, as they could dangerously second-guess the translator during deliberations. If you opt against using a translator, ensure that your witness feels comfortable asking for a question to be repeated or rephrased if the witness does not fully understand it.

Conclusion

Your preparation of witnesses will be more thorough and effective if you give careful thought to the array of mental shortcuts that fact finders may use to evaluate the testimony, as well as to the psychological vulnerabilities of your witness. The strategies and techniques described above can help minimize the factors that detract from effective delivery of your witness's testimony. Moreover, early preparation from this whole-person perspective can pay off by avoiding a stark contrast between a flustered, unprepared deponent and a confident trial witness.

Keywords: criminal litigation, expert witness, deposition, testifying

David Perrott is a senior trial consultant at DecisionQuest in New York, New York.