The Evolving Threat to Corporate Cyber & Data Security

KUTAK ROCK LLP

Presented by:

Sara English, CIPP/US

Sara.English@KutakRock.com

KutakRock.com

THE WALL STREET JOURNAL. | BUSINESS

Rebecca's Journal | Live Help

LAW BLOG

On cases, trends and personalities in business

SUPREME COURT: Death of a Justice: A Roundup of Scalia Coverage

CRIMINAL JUSTICE: Centuries-Old Law at the Center of Apple Phone Encryption Battle

LAW SCHOOL | CONSTITUTIONAL LAW | SUPREME COURT | LAWYERS & LAW FIRMS | STATE LEGISLATION | INTELLECTUAL

10:00 am ET
Dec 9, 2015 TECH

Employee Error Leading Cause of Data Breaches, New Survey Says

ARTICLE | COMMENTS

CYBERCRIME HACKING

Email Print

By NICOLE HONG

A company's cybersecurity is only as strong as its weakest link.

"Employee error" turns out to be the most common reason for a data breach at companies, according to a new cybersecurity report released Wednesday by the Association of Corporate Counsel. This means the breach occurred as the result of a mistake the employee made, such as accidentally sending an email with sensitive information to someone outside the company.

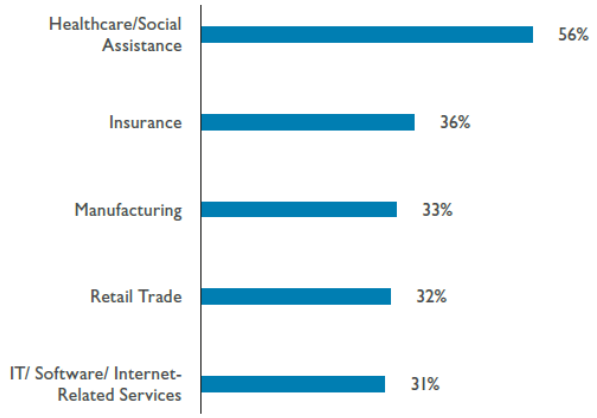
http://blogs.wsj.com/law/2015/12/09/employee-error-leading-cause-of-data-breaches-new-survey-says/

KUTAK ROCK LLP

http://www.acc.com/legalresources/resource.cfm?show=1416928

KutakRock.com

Data Breaches by Industry



Industries with highest percentage shown

2015 ACC Foundation: State of Cybersecurity Survey - Key Findings

In-House Counsel: Fighting the Good Fight

- Legal counsel
- Problem solvers
- Risk managers
- Relationship builders
- Budget minders
- Defenders of the universe

Boards that choose to ignore or minimize the importance of cybersecurity responsibility do so at their own peril.

--Luis Aguilar, SEC Commissioner (June 10, 2014)

How Much Do I Need to Know?

1. Do I understand the nature of cyber threats as it applies to our company?
2. Do the board processes and structure support high-quality dialogue on cyber issues?
3. What is our company doing to stay current as the cyber threat landscape evolves?

RISK

=

Threat

X

Vulnerability

KUTAK ROCK LLP

KutakRock.com

KUTAK ROCK LLP

KutakRock.com

What Is Your Security Framework?

- Cybersecurity Framework (NIST)
- HIPAA/HITECH
- PCI DSS
- ISO 27001
- Etc. . . .

What Do Regulators Request To See?

- Policies and procedures governing privacy and security. *These must be consistent with laws if your organization is regulated*
- Risk assessments conducted by the company over a several-year period
- Risk mitigation plans and responses developed as a result of the risk assessments

What Do Regulators Request To See? cont'd

- Evidence of:
  - education and awareness training, including attendance logs
  - vendor or business associate agreements in place regardless of whether third party caused breach
  - disaster recovery and business continuity plans
  - past security incident records
  - Incident response plans and testing

Fiduciary Duties of Directors

- **Wyndham - *Palkon v. Holmes*, No. 2:14-cv-01234 (D. N.J.)** – alleges board breach fiduciary duties by failing to ensure that the company and its subsidiaries implemented adequate information security policies, arguing the company failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner (**case dismissed**)
- ***Kulla v. Steinhafel*, (Target Corporation), No. 2014-cv-00203 (D. Minn.)** – alleges board breached fiduciary duties by failing "to maintain proper internal controls" related to data security and misleading affected consumers about the scope of the breach after it occurred (case pending)
- **Home Depot, No. 1:15-cv-02999-TWT (N.D. Ga.)** – directors were "complacent" leaving in place "vulnerabilities that not only allowed hackers to enter the system undetected but permitted them to continue siphoning customer cardholder and personal data for almost five months without detection" (case pending)

Case Study: *Palkon v. Holmes*

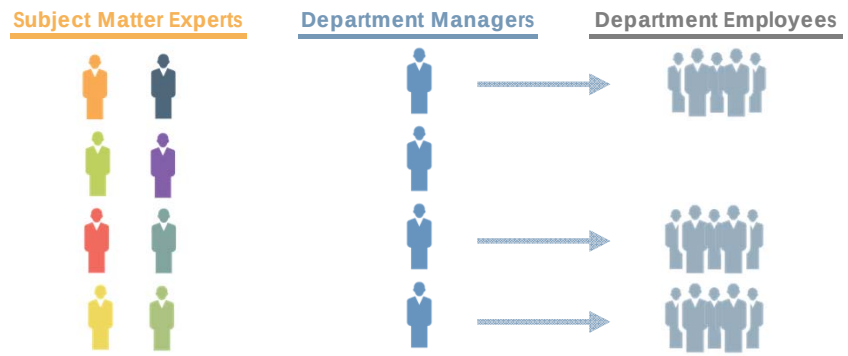
- Wyndham's board of directors discussed cyber-attacks at 14 meetings during the relevant time frame
- Company's general counsel gave a presentation regarding the data breaches or data security at each meeting
- Audit committee discussed these issues during at least 16 meetings over the same time period
- Company had retained third-party technology firms to investigate each breach and recommend enhancements to Wyndham's systems; the court reasoned that the board had conducted a reasonable investigation
- Board's quick response to the demand was not unreasonable, given that the FTC investigation filed a year earlier had enhanced the board's understanding of the issues raised in the demand

Pragmatic Advice

KUTAK ROCK LLP

Conduct cybersecurity risk assessments across the entire organization at least annually

Get an Enterprise-Wide Perspective



KUTAK ROCK LLP

KutakRock.com

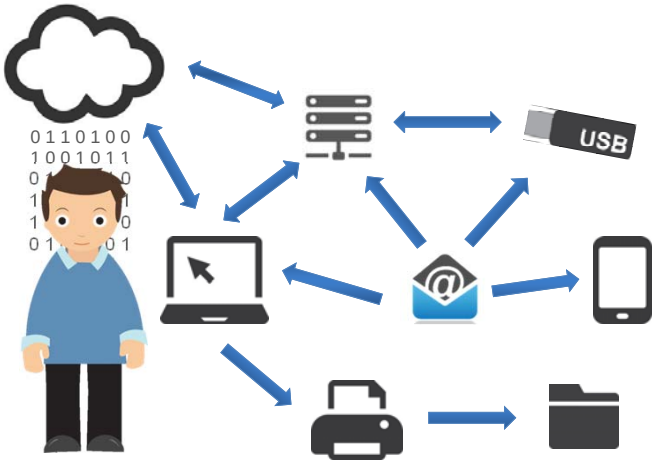
Pragmatic Advice

KUTAK ROCK LLP

Identify and map out where information exists and get rid of what you don't need

KutakRock.com

Where Is Our Information?



KUTAK ROCK LLP

KutakRock.com

Pragmatic Advice

KUTAK ROCK LLP

Assess your third-party vendors at least annually

KutakRock.com

KUTAK ROCK LLP

KutakRock.com

Assess Your Vendors' Practices

KUTAK ROCK LLP

KutakRock.com

Best Practices — Board Involvement

- Adequate time during board meetings to review and discuss cyber security issues; Quarterly, at minimum
- Full board engagement or dedicated committee
- At least one board member has specialized IT and/or cyber security knowledge
- Board understands how security resources are managed and monitored
- Assure there is direct reporting to C-Suite on key security risks
- Assure appropriate insurance that has been reviewed by risk management and annually thereafter

The Evolving Threat to Corporate Cyber & Data Security

KUTAK ROCK LLP

Presented by:
Sara English, CIPP/US
Sara.English@KutakRock.com

Cyber Insurance – Tip Sheet

Don't be fooled - insurance underwriting is not lagging behind the cybersecurity race. When in doubt – Read The Policy

Cyber insurance policies have key distinctions:

- *Determine whether your organization needs first- and/or third-party insurance*
- *Review liability limits closely*
- *Beware of exclusions*
- *Does your coverage include acts by third parties?*

Cyber insurance policies often have built-in support for risk management and data breach. Your insurer is usually an excellent resource in finding forensics teams, public relations, call centers, notifications, ID theft protection, and legal counsel.

Beware of cybersecurity exclusions and other loopholes. Note, for example, Columbia Casualty v. Cottage Health System, *2:15-cv-03432-DDP-AGR (M.D. Cal.). Insurer seeking declaration that Insurer not obligated to pay Cottage's settlement of a class action due to Cottage's failure to follow the minimum required cybersecurity practices that Cottage represented in its application for insurance.*

Cyber insurance policies coverages include:

Litigation
Regulatory
Notification
Crisis management
Credit monitoring
Media liability
Privacy liability
Theft of policy holder data
Forensic investigation costs
Business interruption
Extortion
Computer data loss and restoration

A CGL policy is usually insufficient

Bibilography

The State of Cybersecurity Report: An In-House Perspective. ACC Foundation. December 9, 2015. Available for purchase at http://www.acc.com/legalresources/resource.cfm?show=1416923. Key Findings may be downloaded for free.

Director's Handbook Series: Cyber Risk Oversight. National Association of Corporate Directors. 2014. Available* at https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=10688.

Cybersecurity: What the Board of Directors Needs to Ask. The Institute of Internal Auditors Research Foundation (IIARF). 2014. This publication was co-sponsored by Institute of Internal Auditors (IIA) and ISACA. Available* at http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cybersecurity-what-the-board-of-directors-needs-to-ask.aspx.

2015 Cost of Data Breach Study: United States. Ponemon Institute, May 2015. Available* at http://www-03.ibm.com/security/data-breach/.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. National Institute of Standards and Technology (NIST). February 12, 2014. Referred to as the "Cybersecurity Framework." Available at http://www.nist.gov/cyberframework/. The Cybersecurity Framework was released in response to President Obama's Executive Order 13636, titled *Improving Critical Infrastructure Cybersecurity*, which required NIST to develop a new voluntary framework of standards and best practices for cybersecurity.

* These resources are available free of charge, but registration is required prior to download.