



Cyber Security and Breach Response: What Board Members and Executive Leadership Need to Know

**ALSTON
& BIRD** L.L.P.

KPMG



Size and Scope? Is it Contained?

THE WALL STREET JOURNAL. **SUBSCRIBE NOW** and get **3 MONTHS** for the **PRICE OF 1** **SUBSCRIBE NOW**

U.S. EDITION Tuesday, May 24, 2011 As of 1:46 PM EDT [Subscribe](#) [Log In](#)

[Home](#) [World](#) [U.S.](#) [New York](#) [Business](#) **[Tech](#)** [Markets](#) [Market Data](#) [Opinion](#) [Life & Culture](#) [Real Estate](#) [Careers](#)

[Digits](#) [Personal Technology](#) [What They Know](#) [All Things Digital](#) [CIO Journal](#)

TOP STORIES IN WSJ

1 of 12 **The Facts About Assault Weapons and Crime**

2 of 12 **Death Toll Mounts in Algeria Siege**

3 of 12 **Obama at the Pinnacle**

Armstrong Describes Toll of Family

ASIA TECHNOLOGY | May 24, 2011, 1:46 p.m. ET

Sony Discovers Data Breach in Greece

[Article](#) [Stock Quotes](#) [Comments \(1\)](#) [MORE IN TECH »](#)

Email Print [Save](#) [facebook](#) [twitter](#) [google](#) [plus](#) [linked in](#) A A

What Type of Data?

The screenshot shows the NCSL (National Conference of State Legislatures) website. The header includes the NCSL logo and the tagline 'The Forum for America's Ideas since 1975'. A navigation menu lists various sections like 'About Us', 'Legislatures & Elections', 'Issues & Research', etc. The main content area is titled 'State Security Breach Notification Laws' and includes a 'Last update: August 20, 2012' notice. Below this, a paragraph states that forty-six states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. A 'Related information' section lists various state laws, such as Alaska Stat. § 45.48.010 et seq. and Ariz. Rev. Stat. § 44-7501. On the right side, there are sections for 'RESOURCES', 'Related Documents', and 'Issues & Resources', along with a 'Learn' button featuring a magnifying glass icon.

State Security Breach Notification Laws

Last update: August 20, 2012

Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

Related information: Security breach legislation, data disposal laws, consumer report security freeze laws, and more.

Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36a-701b
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. § 817.5681
Georgia	Ga. Code §§ 10-1-910, -911
Hawaii	Haw. Rev. Stat. § 487N-2
Idaho	Idaho Stat. §§ 28-51-104 to 28-51-107
Illinois	815 ILCS 530/1 et seq.
Indiana	Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.
Iowa	Iowa Code § 715C.1
Kansas	Kan. Stat. 50-7a01, 50-7a02
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq.

Find the NCSL [staff member](#) who handles the issue in which you are interested.

NCSL provides access to current state and federal legislation and a comprehensive list of state documents, including state statutes, constitutions, legislative audits and research reports.



Where Was the Data?

ico.

Information Commissioner's Office

Home

For the public

For organisations

What we cover

 Français  Español  Cymraeg

Accessit

Quick links

Search

[select a destination]

Penalty highlights need for encryption of sensitive data

News release: 25 October 2012

The Information Commissioner's Office (ICO) is reminding organisations that sensitive personal information should be encrypted when being stored and sent electronically.





Communications Issues

SEC Asks Companies to Disclose Cyberattacks, Data Breaches

Matt Liebowitz, SecurityNewsDaily Staff Writer
October 14 2011 03:28 PM ET



CREDIT: Twentieth Century Fox
[View full size image](#)

The Securities and Exchange Commission (SEC) has formally asked publicly traded companies in the U.S. to disclose when they've been hacked or suffered a data breach. The request could drastically alter how corporations traditionally handle cybercrime attacks and the amount of staff and effort they use to prevent such incidents.

The SEC [guidance](#), issued yesterday (Oct. 13), calls for corporations to disclose



Dealing with Law Enforcement



ision

Releases • 2011 • Hacker Pleads Guilty to Infiltrating AT&T Servers, iPad Data Breach

cebook (28) Share

Hacker Pleads Guilty to Infiltrating AT&T Servers, iPad Data Breach

Defendant Stole E-Mail Addresses and Personal Information Belonging to 120,000 Apple iPad 3G Subscribers

ney's Office
011

District of New Jersey
(973) 645-2888



TERRORISM LAW & ORDER FOLLOW THE MONEY VIDEO ABOUT

WATCH LIVE Notre Dame officials comment on Manti Te'o hoax reports



GALLERY
Manipulated photography before Photoshop



SPORTS
Regular NFL refs return, get standing ovation

April 4, 2011 5:13 PM

Secret Service investigates Epsilon data breach

comments 2 Like 368 Tweet 84 +1 0 Share 41 More +

By Laura Strickler Topics News

About Us

- Our People & Capabilities
- What We Investigate
- Our Partnerships

ALSTON & BIRD L.L.P.





Kim Peretti

ALSTON & BIRD LLP

THREAT LEVEL | [crime](#) | [hacks and breaches](#) | [breaches](#)

TJX Hacker Gets 20 Years in Prison

BY KIM ZETTER 03/25/10 2:02 PM
[Follow @KimZetter](#)

[Like](#) 265
[Tweet](#) 4
[+1](#)
[Share](#)

UNIVERSITY | PRO BONO | CAREERS | OFFICES
PROFESSIONALS | **RESOURCES**

BOSTON — Convicted TJX hacker Albert Gonzalez was sentenced to 20 years in prison on Thursday for leading a gang of cyberthieves who stole more than 90 million credit and debit card numbers from TJX and other retailers.

The sentence for the largest computer-crime case ever prosecuted is the longest ever imposed in the United States for hacking or identity-theft. Gonzalez was also fined \$25,000. Restitution, which will likely be in the tens of millions, was not decided Thursday.

Clean-cut, wearing a beige jail uniform and wireframe glasses, the 28-year-old Gonzalez sat motionless at his chair during Thursday's proceedings, his hands folded in front of him.

Before the sentence was pronounced, Gonzalez



ces: [Washington](#)



Partner

T: 202-239-3720 F: 202-654-4976

kimberly.peretti@alston.com | [VCard](#) | [PDF Bio](#)

Kimberly (Kim) Kiefer Peretti is a partner in the firm's White Collar Crime Group and co-chair of our [Security Incident Management and Response Team](#). Ms. Peretti is also a former director of PricewaterhouseCoopers' cyber forensic service practice and a former senior litigator for the Department of Justice's Computer Crime and Intellectual Property Section. She focuses her practice on managing complex, technical electronic investigations and responses, often resulting from cyber intrusions and data breaches. She also services a wide range of clients in matters of cybersecurity; privacy; financial crime, fraud and regulation; payment systems compliance and risk mitigation; economic espionage; and intellectual property theft.

While at the Department of Justice, Kim led several benchmark cybercrime investigations and prosecutions, including the prosecution of the infamous TJX hacker Albert Gonzalez, currently serving 20 years in prison for his role in the largest hacking and identity theft case ever prosecuted by the department.

Related Services

[Privacy & Data Security](#)

[Security Incident Management & Response Team](#)

ALSTON & BIRD LLP





Customer Issues

 SSAE-16.COM

[Find an SSAE 16 Provider](#)



[Home](#) [Type I](#) [Type II](#) [Preparation](#) [ISAE 3402](#) [Contact Us](#)

The SSAE16 Auditing Standard

December 22nd, 2012

[Which SOC Is Right](#)

ALSTON & BIRD L.L.P.





Insurance

« WSJ.com

CIO Journal Home

CIO Report : [Consumerization](#) [Big Data](#) [Cloud](#) [Talent & M](#)

CIO Report

May 29, 2012, 7:37 PM ET

As Flame Spreads, Most Companies Lack Cybersecurity Coverage

Article

Comments

Get full access to CIO Journal now.

LEARN MORE »

ALSTON & BIRD L.L.P.





Plaintiff's Exhibit A

OFFICE OF INADEQUATE SECURITY

YOUR INFO, THEIR SCREW-UPS.

[Home](#)

[About](#)

[Breach Laws](#)

[Privacy Policy](#)

Nov
17
2012

Data Breach Class Action against Popular Video Game Developer Dismissed for Failure to Plead Adequate Damages

[Breach Incidents](#), [Business Sector](#), [Hack](#)

An update on the [Valve/Steam breach...](#)



Regulators

Washington State Office of the
ATTORNEY GENERAL

SEARCH >

News > News Releases > 2009

FOR IMMEDIATE RELEASE
June 23, 2009

Attorney General McKenna calls TJX's data breach a costly lesson

Company to pay \$9.75 million to states to support data protection efforts

CONTACT US > CONSUMER COMPLAINT >

PCWorld

WHAT'S HOT REVIEWS

Office hardware • Business

BUSINESS

FTC Settles Data Breach Charges Against Two Firms

By [Grant Gross](#), IDG News Service

May 3, 2011 11:40 AM



ALSTON & BIRD L.L.P.





Personnel Dynamics

The Register[®]

[Data Center](#) [Cloud](#) [Software](#) [Hardware](#) [Networks](#) [Security](#) [Jobs](#) [Business](#) [Policy](#) [Science](#) [Bootnotes](#)

[Financial News](#) [Small Biz](#) [CIO](#) [Media](#) [Tech Panel](#)

 [Print](#)

 [Like](#) 3

 [Tweet](#) 41

 [Alert](#)

Sony hack boss Schaaff quits

New CEO Kazuo Hirai makes his mark

By **Phil Muncaster** • [Get more from this author](#)

Posted in [Business](#), 9th November 2012 04:25 GMT

[Free whitepaper – Shutterfly and Cleversafe: The Path to a Picture Perfect Data Storage Solution](#)



Live-Fire Exercise






Legal Obligations of the Board

- Fiduciary Duty
 - No legal duty on board to monitor for business risk.
 - Business Judgment Rule generally applies to board's management of cyber risk.
 - Board does have duty to “monitor” corporate controls and processes to prevent fraudulent or illegal actions.



Post-Breach Obligations

- Directors should treat a material breach as a “red flag” requiring director oversight.  Let the lawyers argue over the correct standard later.
- At the early stages of a breach, it is better for the board to assume that a breach implicates duty of oversight. A breach may raise issues of corporate compliance with rules and regulations regarding maintaining personal data and notifying regulatory authorities. It also raises challenging disclosure issues.
- The board should be informed and provide oversight with respect to management’s handling of the breach.



Practical Considerations for Board Oversight

- The board must gain understanding of the scope of the breach and the business and legal implications of the breach.
- Board Involvement
 - All board members need to become informed—be thoughtful about note-taking and communications among board members and management.
 - Consider using a committee for daily or more regular communications.
 - Consider what discussions should be privileged.
 - Consider having a third party engaged in the investigation or remediation speak directly to the board or committee.
 - Help the directors understand what they are being told. Breach technology is complex and can be daunting to the uninitiated.



Issues to Consider

- Has the breach been contained? (APT) Is it safe to operate the business?
- Whether the hacker has obtained personal data or personal health information about employees, customers or vendors
- Legal obligations to disclose the breach to persons affected by the breach
- Other legal reporting obligations
 - Securities and Exchange Commission (October 2011 Disclosure Guidance)
 - State Regulators
 - FTC
 - Foreign Regulators
 - Etc.
- General Media Interaction
- Trading Windows



Document What You Know

- A breach generally creates a dynamic situation where knowledge of the scope and impact of the breach change during the course of the investigation and remediation.
- Plaintiffs, the SEC and privacy regulators (among others) will inquire into what the company/board knew at the time of its disclosures.
- It is critical to thoroughly document what knowledge you have at the time you make a disclosure. Consider privilege issues.
- It is difficult to reconstruct events 1-2 years later without a good record.
- Confirm your information with third-party experts who are working on the breach to make sure that you have current information.
- Avoid “spinning the story” to minimize the impact of a breach, particularly where investigation is not complete and you may have to correct or update your prior disclosure.



New “Vectors” of Threats for Data Breaches

YESTERDAY

Bad “Actors”

- Isolated Criminals
- “Script Kiddies”

“Target of Opportunity”

Targets

- Identity Theft
- Self-promotion Opportunities
- Theft of Services

TODAY

Bad “Actors”

- Organized Criminals
- Foreign States
- Hactivists

“Target of Choice”

Targets

- Intellectual Property
- Financial Information
- Strategic Access

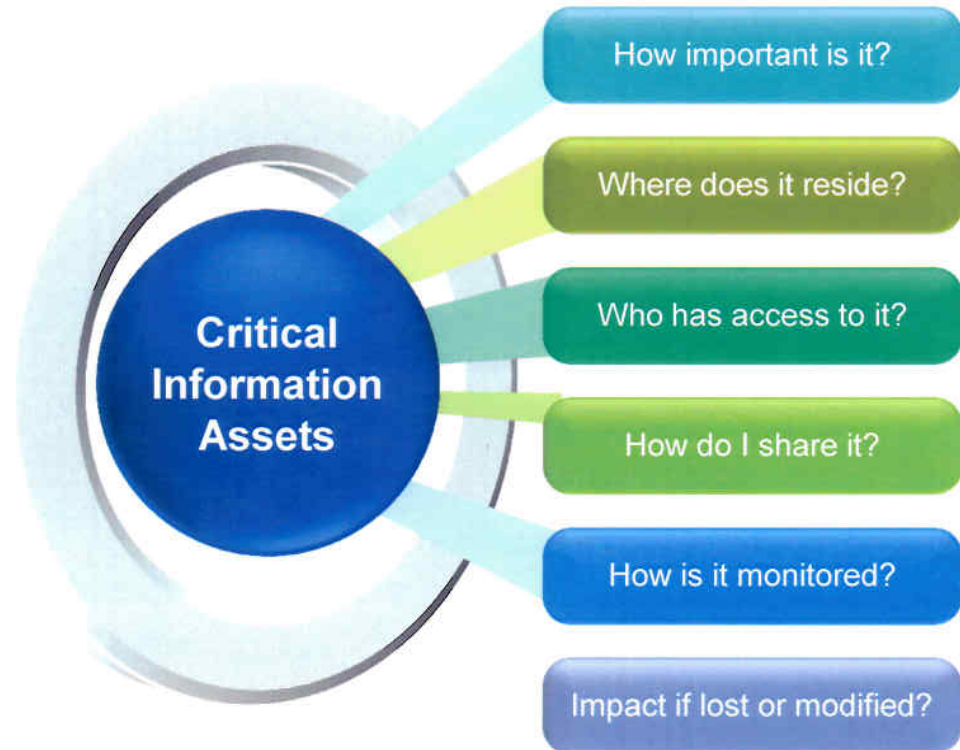


Thinking about Information Assets Differently

Information assets drive business value but there are key questions to consider when planning how to govern critical information:

- Do we know which data is most valuable?
- Do we know how to maximize the use of it or the impact of loss to our organization?
- How do we control the information in alignment to the value it provides?

Leading organizations are focusing on implementing information governance programs to answer these questions.





Advanced Persistent Threat = The New “State of the Art”

Most organizations have invested in information security and protection. They have **established programs, policies and technical controls** to protect information assets. The challenge is that these programs often **cannot keep pace** with the advanced new approaches and technical “attack vectors” that the bad actors are using.

Once a bad actor has identified your organization, they will continue to attempt multiple approaches and consider many different types of attacks to gain access to your information. They will often use **cutting-edge, state-of-the-art technologies** or prey upon **common lapses in security**, such as social engineering. They will continue multiple variations until they gain access. This approach is commonly referred to as Advanced Persistent Threat, or APT.

To combat APT, organizations must be prepared to **continually evolve, adjust and update** their information protection program to react to changes driven by new business drivers, new technology solutions, or driven by approaches to newly discovered threats. Security budgets are expected to increase over time rather than plateau or eventually shrink. This is the new reality.



Framework for Board Discussions about Cyber Risk

Business Layer

Geopolitical Drivers

Industry Leading Practices

Corporate Objectives

Business Process

Enablement Layer

Application

Data

Infrastructure Layer

Servers/Hosts

Networks

Physical Environment

AREAS OF DYNAMIC CHANGE

- Slow Economic Recovery
 - Driving Growth & Profitability
 - New Products/Services
 - Mergers/Acquisitions
 - Globalization
 - Strategic Sourcing
 - Competitive Differentiation
 - Increased Regulatory Scrutiny
-
- Mobile & Cloud Deployments
 - “Big Data,” BI & Analytics
 - Self-Service & Consumerization
-
- Virtualization & Cloud Platforms
 - Internetworking/VPNs
 - New Operating Systems
 - Low-Cost Computing Models
 - Changing DataCenter Models

A blue-tinted image showing a globe on the left and a padlock on the right, symbolizing global security and risk management.

Some Questions to Consider from the Board's Perspective

■ Portfolio Risks

- What are our major IT risks? Where do these compare against other significant enterprise risks?
- Who is responsible for the governance and oversight of these risks?
- What is the ongoing mechanism to review these risks and their impact? How often is this updated?

■ Execution Risks

- Do we have a formal data strategy?
- Do we have a set of controls to protect our critical information?
- Do we have a formal plan for cloud computing adoption? Are we piloting cloud? What is the approach to cloud governance?



Some Questions to Consider from the Board Perspective

■ **Competitive Risks**

- Do we have a social media policy? Are all employees training on the policy? How do we monitor use?
- How are we protecting our mobile devices? Have there been issues of loss or theft?

■ **Service & Security Risks**

- Do we have a dedicated resource responsible for information security?
- Have we evaluated our risk of security attack? How about our supply chain? Are we considered “Critical Infrastructure” by the U.S. government?
- What’s our response plan if we were attacked? How would we respond?
- When was the last time we updated our business continuity program? When was the last time the disaster recovery was plan tested?



Cyber Security and Breach Response: What Board Members and Executive Leadership Need to Know

ALSTON
& BIRD LLP

KPMG