



STROZ FRIEDBERG

DIGITAL RISK MANAGEMENT & INVESTIGATIONS

Cybersecurity: New Expectations for Marketers and their Counsel

Harriet Pearson, Partner, Hogan Lovells

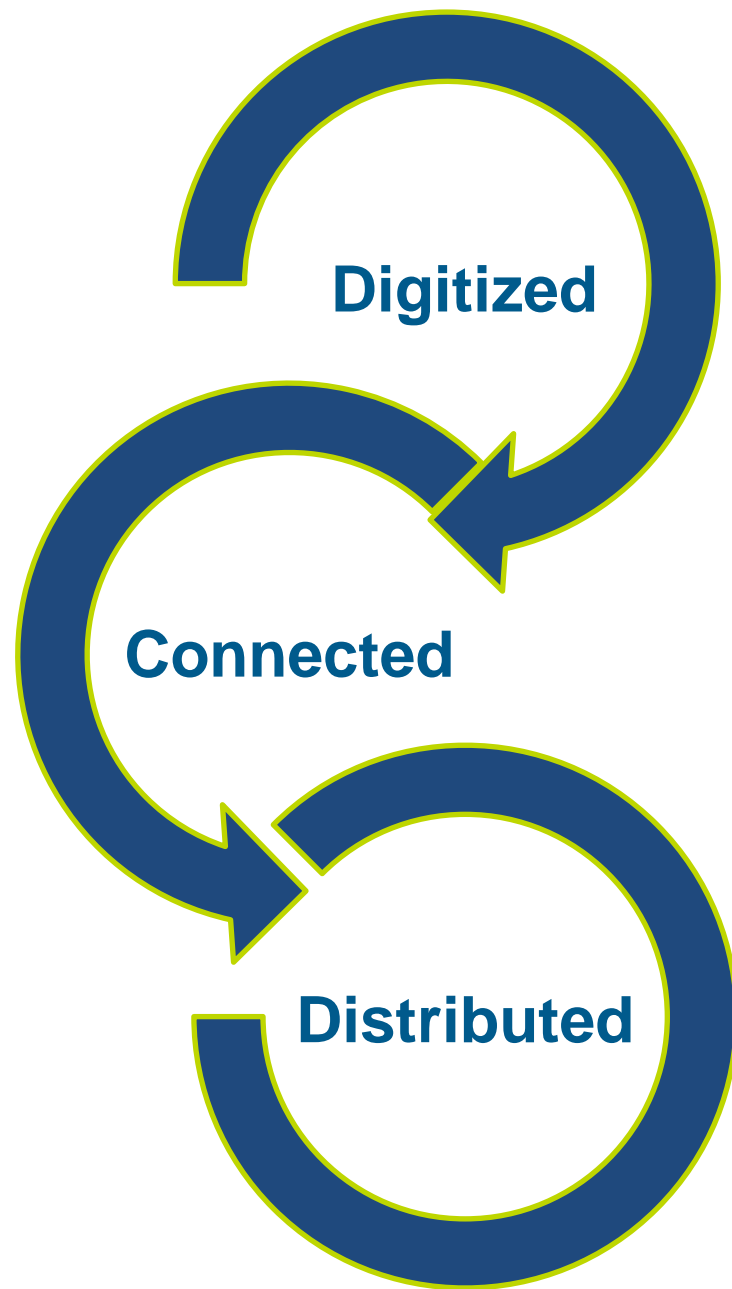
Thomas Hibarger, Managing Director, Stroz Friedberg

ANA Advertising Law & Public Policy Conference

Washington, D.C.

March 19, 2013

Cyberspace =



Cybersecurity Is Grabbing Headlines

The New York Times

January 30, 2013

Hackers in China Attacked The Times for Last 4 Months

NICOLE PERLROTH

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

After surreptitiously tracking the intruders to study their movements and help erect better defenses to block them, The Times and security experts have expelled the attackers and kept them from breaking back in.

THE NATIONAL
LAW JOURNAL

February 1, 2013

A Cybersecurity Blanket: New Executive Order Means a Broad Review for Lawyers, Clients

TODD RUGER

The federal government's new push to bolster cybersecurity will create an array of legal questions and potential pitfalls for companies in the coming months.

The New York Times

February 1, 2013

Twitter Hacked: Data for 250,000 Users May Be Stolen

NICOLE PERLROTH

Twitter announced late Friday that it had been breached and that data for 250,000 Twitter users was vulnerable.

The company said in a blog post that it detected unusual access patterns earlier this week and found that user information — usernames, e-mail addresses and encrypted passwords — for 250,000 users may have been accessed in what it described as a “sophisticated attack.”

Data Security is #1 concern of GCs

Legal Risks On the Radar

Figure 1
Top 10 concerns for directors and general counsel:

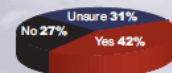
Directors

Data security	48%
Operational risk	40%
Company reputation	40%
M&A transactions	37%
Investor relations	30%
Executive compensation	30%
SEC/regulatory compliance	28%
Disaster recovery	27%
Internal controls	26%
Global business expansion	26%

General Counsel

Data security	55%
Operational risk	47%
Management of outside legal fees	38%
Company reputation	35%
Disaster recovery	35%
E-discovery	33%
FCPA	30%
Global business expansion	29%
Internal controls	26%
Executive compensation	26%

Figure 2
Directors who say their company has a crisis management plan in place to respond to a cyber attack.



Introduction

Each year, Corporate Board Member and FTI Consulting, Inc. conduct research to gain insight on which current legal issues raise concern for public company directors and corporate general counsel and to analyze related legal and governance events and trends. In early 2012, the organizations gathered data by surveying 11,340 directors and 1,957 general counsel. Questions were asked of both groups to compare and contrast their perspectives; other queries were specifically targeted toward either directors or GCs. The 2012 Law and the Boardroom survey results that follow once again offer interesting insight into the thoughts and opinions of these two critical governance groups.

Executive overview

Several key themes emerged from the 2012 Law and the Boardroom study that reflect changes taking place within corporate America. During the past decade, for example, U.S. businesses have expanded globally and stepped up the use of online communication as well as web-based products and delivery channels. Thus, increasingly, corporate America is operating in a world where connectivity is high and there are few physical barriers. Accordingly, for the first time, data security was earmarked by the largest percentage of responding directors (48%) and general counsel (55%) as an issue of concern. The second most prevalent response for both directors and GCs centers on operational risk, which topped directors' list in 2011 and moved up several places for general counsel this year. Finally, on the risk/concern spectrum, directors and GCs flagged loss of reputation as an issue of critical concern in 2012.

A significant number of directors are also worried about risks related to mergers and acquisitions and their relationship with investors, while a significant number of general counsel

noted concern with the management of outside legal fees and disaster recovery. Also resonating this year are issues involving compliance and investigations (Figure 1).

In addition to this barometer, the 2012 Law and the Boardroom study delved into opinions relative to proxy access and other shareholder-related matters. In particular, the study homed in on respondents' opinions regarding the nomination of director slates and subsequent actions taken as a result of 2011 say-on-pay votes. Also, for the first time, the survey queried respondents about the use of corporate social media and the risks and policies surrounding it. And finally, because the board/management relationship is a critical factor in the performance of the company, we asked directors and GCs to rate each other in several key aspects of effectiveness, as well as how well they work in tandem with each other.

The following report, a supplement to *Corporate Board Member* magazine's third quarter 2012 issue, presents highlighted data and examines each of these topics in fuller detail.

Cyber strategy and IT risk

Today, there is arguably no more insidious threat to a public company than that of cyber risk; it's invisible, ever-changing, and pervasive—making it very difficult for boards to manage. On top of that, it's costly. *Corporate Board Member* magazine recently reported that the median annualized cost of cyber crime per company averaged \$5.9 million—a serious bottom-line expense. Thus, it comes as no surprise that this year, more than half (55%) of general counsel rated data security as a major concern and 48% of directors feel likewise. Interestingly, this level of concern has nearly doubled in the last four years: In 2008, only 25% of directors and 23% of GCs noted data security as an area of high concern.

Figure 1

Top 10 concerns for directors and general counsel:

Directors

Data security	48%
Operational risk	40%
Company reputation	40%
M&A transactions	37%
Investor relations	30%
Executive compensation	30%
SEC/regulatory compliance	28%
Disaster recovery	27%
Internal controls	26%
Global business expansion	26%

CORPORATE BOARD MEMBER®
An NYSE Euronext Company

2012 SPECIAL SUPPLEMENT

General Counsel

Data security	55%
Operational risk	47%
Management of outside legal fees	38%
Company reputation	35%
Disaster recovery	35%
E-discovery	33%
FCPA	30%
Global business expansion	29%
Internal controls	26%
Executive compensation	26%

Agenda

- What is the current cyber risk landscape?
- What is current legal and regulatory landscape?
- What is likely to happen in Washington in 2013?
- What is corporate counsel's role?

FBI Director Mueller at 2012 RSA Conference

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

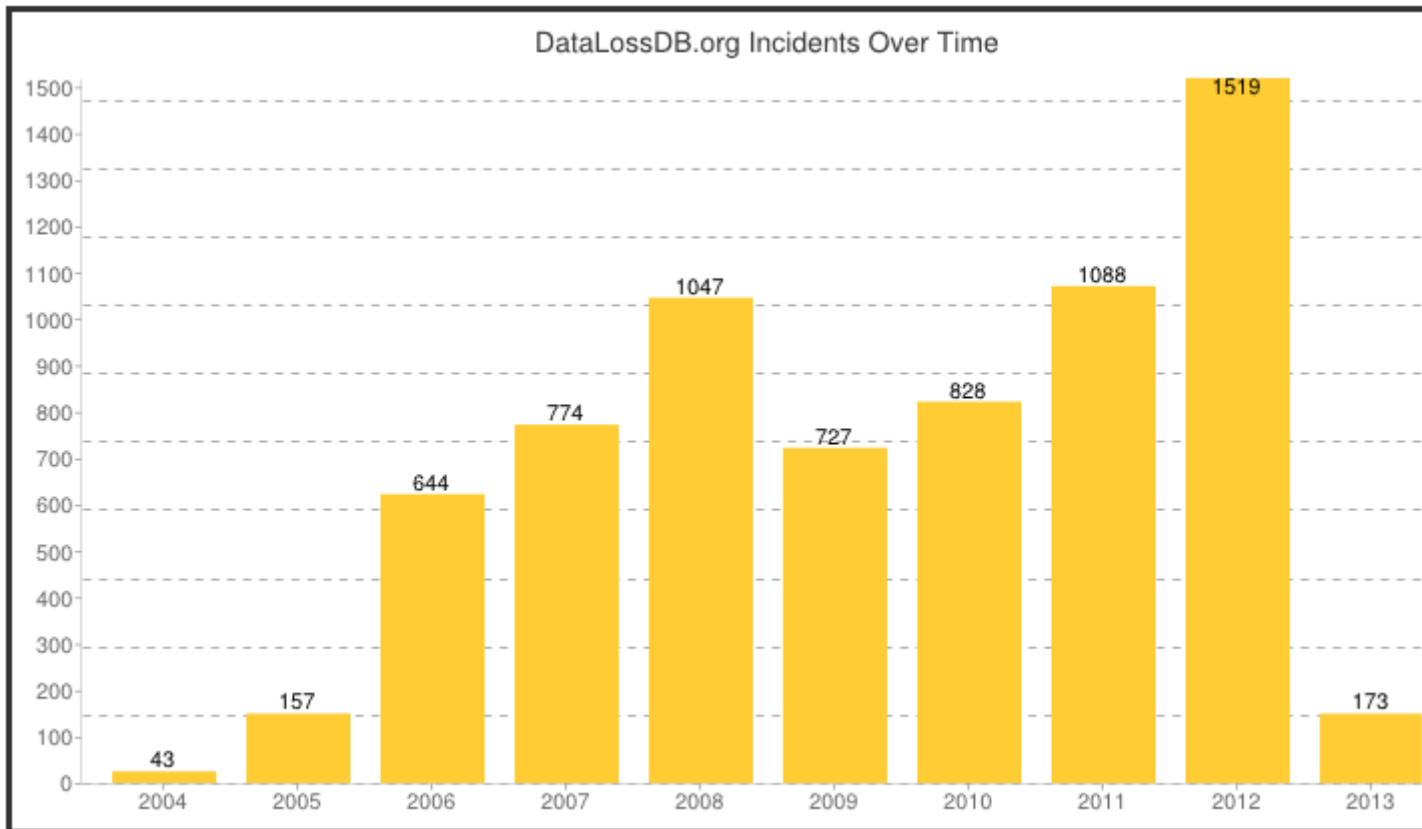


- *"State-sponsored hackers are patient and calculating," Mueller said. "They have the time, money and resources to burrow in and wait. You may discover one breach only to find that the real damage has been done at a much higher level."*

Source: CNNMoney http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm?iid=EL; last accessed 10.24.12

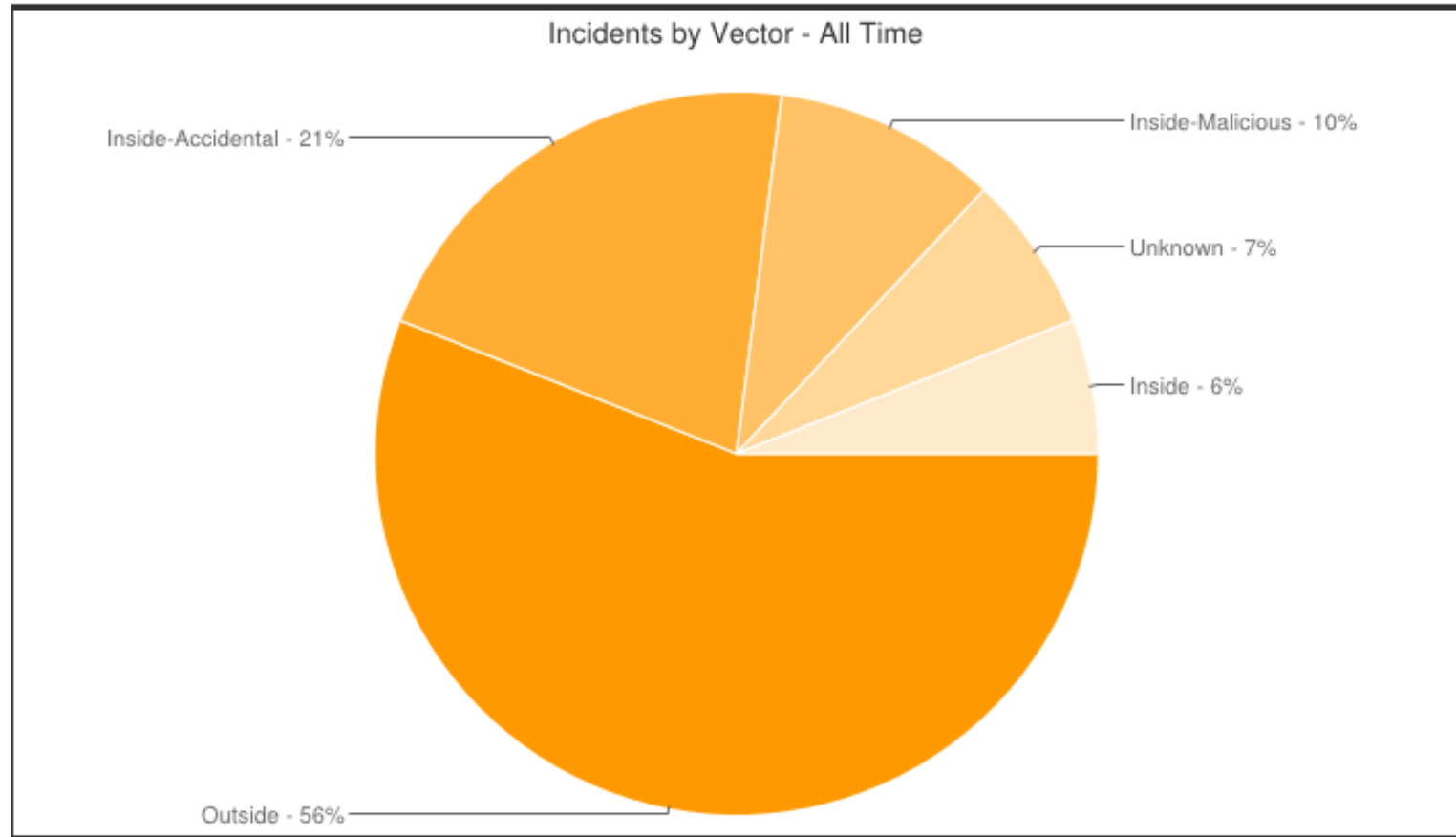
Data Breach Trends

Number of DataLossDB.org Incidents Over Time



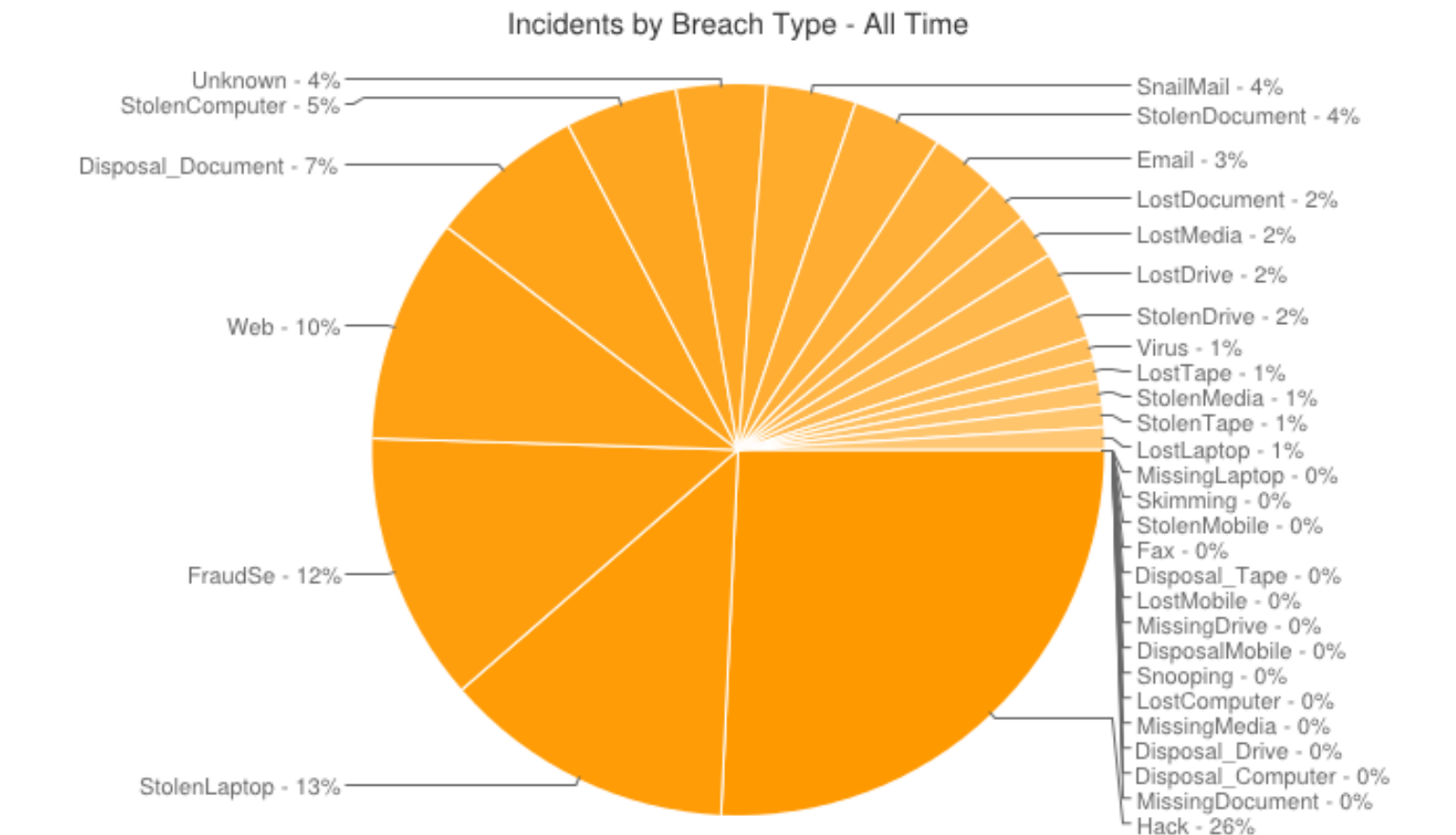
Source: <http://datalossdb.org/statistics>, last accessed 3/2/2013

Data Breach Trends



Source: <http://datalossdb.org/statistics>, last accessed 3/2/2013

Data Breach Trends



Source: <http://datalossdb.org/statistics>, last accessed 3/2/2013

Data Breaches Abound

State of South Carolina

**AN URGENT MESSAGE FOR ALL
SOUTH CAROLINA RESIDENTS TO
PROTECT AGAINST IDENTITY
THEFT**

**Please click for further
information.**

Source: <http://www.sctax.org/security.htm>; last accessed 11/6/2012

Data Breaches Abound

State of South Carolina

PROTECT YOURSELF AGAINST IDENTITY THEFT

As you have probably seen on the news, in October, the South Carolina Department of Revenue learned that it was the victim of a cyber attack in mid-September. Because of this criminal hack, South Carolina residents who have paid state taxes since 1998 may have had their personal information compromised.

Source: <http://www.sctax.org/security.htm>; last accessed 11/6/2012

Data Breaches Abound



News Topics

E-Government

Emerging and Sustainable
Technology

Health and Community
Services

IT Policy/Mgmt/Enterprise Tech

Justice and Public Safety

Products

Transportation and
Infrastructure

Wireless/Mobile/Broadband

[View All News Topics...](#)

» South Carolina Encrypts Records After Breach



Photo from Shutterstock

November 5, 2012 By [News Staff](#)

Officials in South Carolina have had a busy month. On Oct. 26, Gov. Nikki Haley announced a [data breach](#) that data security experts said

could lead to widespread bank fraud, identity theft, bogus tax refunds and fraudulent loans. The breach, initiated in August and discovered on Oct. 10, is being blamed on overseas hackers. Personal information for 3.6 million taxpayers was leaked from the state's Department of Revenue.

Tweet 5

Recommend 0

+1

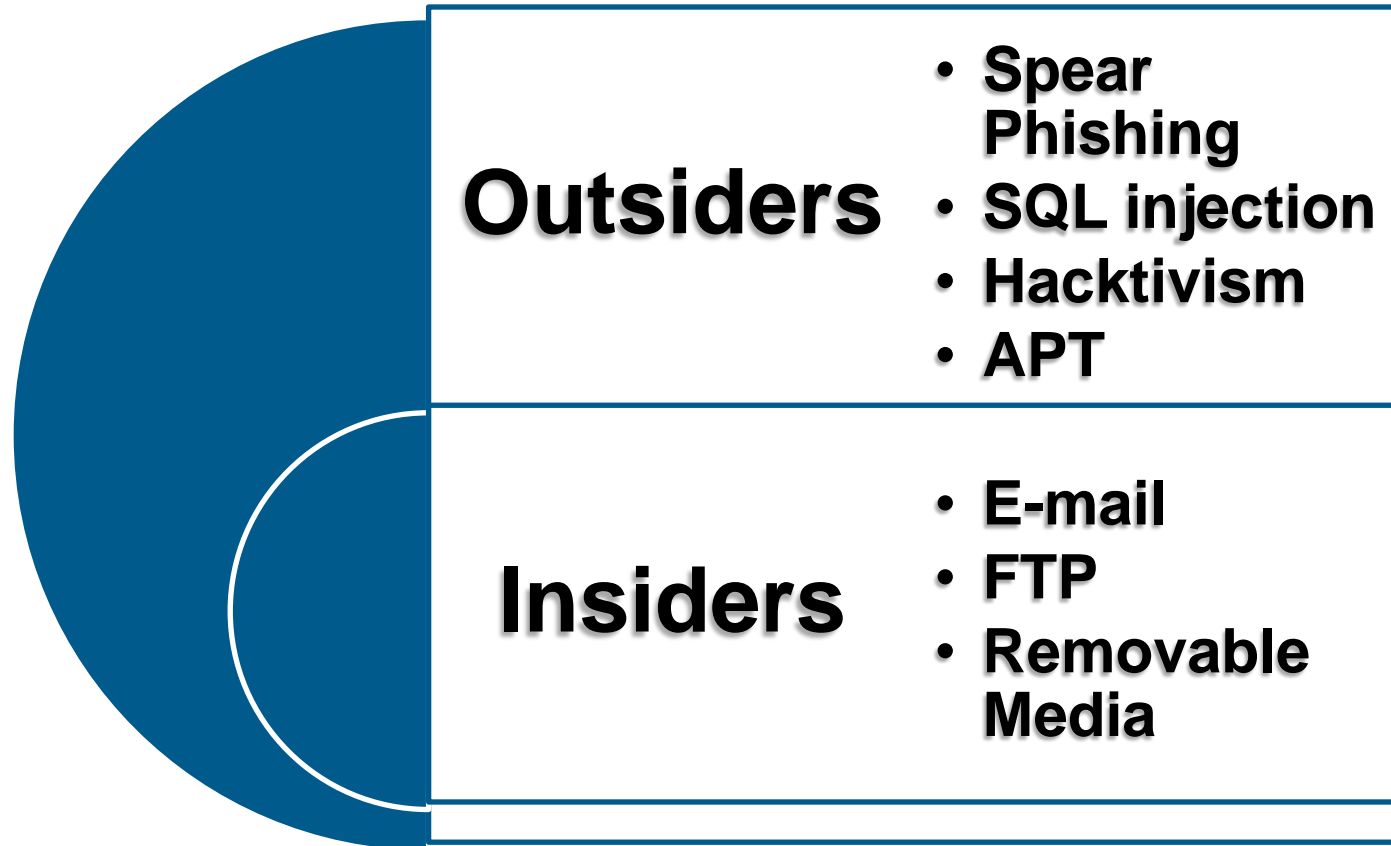


You May Also Like

[South Carolina Breach Compromises Millions of Records](#)

Source: <http://www.govtech.com/South-Carolina-Encrypts-Records-After-Breach.html> ; last accessed 11/6/2012

Attack Vectors



Outsider Threats – Spear Phishing

SECURITY Aug 5, 2011 9:50 am

As Targeted E-mail Attacks Proliferate, Companies Wince

By Jeremy Kirk, IDG News

The strange e-mails arrived in executives' inboxes around the same time that the Australian oil company was negotiating a deal with a Chinese energy company.

SIMILAR ARTICLES:

[Hack Attacks Proliferate with CIA, State of Alabama Latest Victims](#)
['Massive' Epsilon E-Mail Breach Hits Citi, Chase, Many More](#)
[How Do I Make Web Mail My Default Email, Part 1](#)
[How to Email Like a Pro](#)
[Cybercrime Fight Costing](#)

The e-mails had the same structure and format as those sent around the company and were baited with text that appeared to refer to a supposed continuing discussion between executives. The messages looked authentic from a nontechnical perspective, just part of normal electronic communication within a company.

But the corporate IT administrator felt something wasn't quite right. Upon closer examination, the administrator found the e-mails, while appearing to come from internal company

**“Companies in pharmaceutical, chemical, energy and oil industries are at the highest risk for encountering malware on the web, the report said.”
(PC World Aug. 5, 2011).**

In response to the targeted attacks against the Australian oil company, the IT administrator said he built a tool that automatically strips out links in e-mails that come from outside his company. That may be inconvenient for some users, but “we can do without the links but we can't do without security,” he said.

Fundamentally, the administrator said many executives still regard computer security as a hindrance and that “these geeks are just trying to make their life hard.”

“I still think they think this is a nuisance and that the security guy will take care of it,” the IT administrator said. “They are not elected [to the board] for IT savvy. They're old-school business people.”

From: **Express Mail Service** <el-915@baltimore.com>
Subject: Tracking Number (N)GHF45 213 213 2126 2126
Date: January 11, 2013 10:10:36 AM EST
To: [REDACTED]
Reply-To: Express Mail Service <el-915@baltimore.com>

Fed Ex

Order: JN-5584-49069383

Order Date: **Thursday, 3 January 2013, 11:23 AM**

Dear Customer,



Your parcel has arrived at the post office at January 6. Our courier was unable to deliver the parcel to you.

To receive your parcel, please, go to the nearest office and show this receipt.

GET & PRINT RECEIPT

[http://turbopercussion.com.br/
CTVTMCRWYE.php?receipt=799_642977493](http://turbopercussion.com.br/CTVTMCRWYE.php?receipt=799_642977493)

Best Regards, The FedEx Team.

From:  THibarger@StrozFriedberg.com
To:  'Pearson, Harriet P.'
Cc:
Subject: RE: REMINDER - Materials For ANA Advertising Law & Public Policy Conference 2013

Sent: Fri 3/1/2013 3:04 PM

badguy@gmail.com

Harriet,

Check out these changes to our slide deck and let me know what you think! Just click on the link to see the deck.



www.strozfriedberg.com/ana_slide_deck

www.badguyproxy.ru

Tom

Thomas Hibarger
Managing Director

Tel: 202.464.5803
Mobile: 202.754.2815
Fax: 202.464.5700

1150 Connecticut Avenue, NW, Suite 700, Washington, DC 20036
 thibarger@strozfriedberg.com  www.strozfriedberg.com

STROZ FRIEDBERG

SQL Injection



SQL Injection

In an SQL injection, the intruder sends intentionally malformed requests to a company's Website in the hope that the server will malfunction and either return non-public data in response to the request or grant the attacker deep administrative access to the server.

Hactivism: LulzSec and Anonymous



Advanced Persistent Threat (APT)

- State-sponsored hacking
- Most corporations and law firms are underprepared
- The ramifications are significant enough that this is no longer simply an IT problem
- The front office, CEOs, and Boards need to partner with IT to understand and strategize for APT defense and response
- APT defenses
 - Corporate governance – create a culture of digital security
 - Technological competencies
 - Cutting edge tools for zero day malware identification

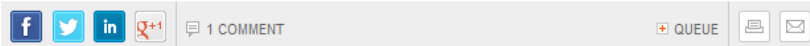
Advanced Persistent Threat (APT)

Bloomberg Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABLE

China-Based Hacking Of 760 Companies Shows Cyber Cold War

By Michael Riley and John Walcott - Dec 14, 2011 8:47 AM ET



[Google Inc. \(GOOG\)](#) and [Intel Corp. \(INTC\)](#) were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyber spies on iBahn, a provider of Internet services to hotels, takes some explaining.

iBahn provides broadband business and entertainment access to guests of [Marriott International Inc.](#) and other hotel chains, including multinational companies that hold meetings on site.

Breaking into iBahn's networks, according to a senior U.S. intelligence official familiar with the matter, may have let hackers see millions of confidential e-mails, even secreted ones.


“In the biotechnology sector, their victims include Boston Scientific, (BSX) the medical device maker, as well as Abbott Laboratories (ABT) and Wyeth, the drug maker that is now part of Pfizer Inc. (PFE).”
(Bloomberg, Dec. 13, 2011).

The hackers also rifled networks of the Parkland Computer Center in Rockville, Maryland, according to documents provided to Bloomberg News by a person involved in government tracking of the cyberspies, who declined to be identified because the matter isn't public. Parkland is the computing center for the Food and Drug Administration, which has access to drug trial information, chemical formulas and other data for almost every important drug sold in the U.S.

Lawyers Are Not Immune...

Bloomberg News

China-Based Hackers Target Law Firms to Get Secret Deal Data

By Michael A. Riley and Sophia Pearson on February 08, 2012 |     | 0 Comments



(Updates with IT officer's comment in 16th paragraph.)

Jan. 31 (Bloomberg) -- China-based hackers looking to derail the \$40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.

China-based hackers looking to derail the \$40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.

as Canada's Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based

Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms....

(Businessweek.com; 2-8-12)

for natural resources, Tobok said. Such stolen data can be worth tens of millions of dollars and give the party who possesses it an unfair advantage in deal negotiations, he said.

Policy, Regulatory & Legal Landscape

Intensifying Government Response...

.com

Congress

- 2012:
 - House Passed: CISPA and FISMA
 - Senate Considered: Cybersecurity Act and SECURE IT Act
 - Rockefeller letter to 500 CEOs
- 2013:
 - House: A repeat of 2012 so far
 - Senate: Commerce & Homeland Security

.gov

Administration

- Executive Order on critical industry security
 - “Voluntary” standards
 - Procurement incentives
 - Information-sharing
- Support for legislation
- SEC and other agencies active

.mil

Europe and other nations

...Occurs Alongside Consumer Protection Agenda

- State breach notification and other data security laws
- Federal data and software security enforcement
 - Federal Trade Commission (FTC v. Wyndham Worldwide; HTC settlement)
 - Health & Human Services
- NAAG – Top 2013 Priority

Key Cybersecurity Policy Issues

- Information-sharing incentives (e.g. liability protection)
- Commercial critical infrastructure regulation or standards
- Harmonized breach notification
- Privacy & civil liberties
- Cyber doctrine and international collaboration

Counsel's Role*

1. Establish and guide to **standard of care**
2. Guide compliance with **disclosure obligations**
3. Identify and guide **partnership strategy & governance**
4. Ensure **regulatory compliance**
5. Counsel on **cybersecurity program risks and obligations**
6. Ensure proper incident **preparation & management**
7. Identify and mitigate cybersecurity-related **transactional risk**
8. Advise on **cyber insurance strategy**
9. Monitor and engage **public policy and industry standards** developments
10. Discharge **ethical obligations**

*Cybersecurity: The Corporate Counsel's Agenda, BNA
Privacy and Security Law Report (Dec. 12, 2012)

<http://www.hldataprotection.com/files/2012/12/BloombergBNA-Cybersecurity-Pearson.pdf>



Incident Planning

PRE-BREACH PLANNING CHECKLIST

- ☐ Create your data breach incident response team and plan
- ☐ Define team roles and responsibilities
- ☐ Outline steps necessary in the first 72 hours
- ☐ Establish clear action items and checklists to keep parties focused
- ☐ Train staff to identify and report breaches
- ☐ Consult security experts to audit and review your security assessment
- ☐ Examine third parties' security protocols
- ☐ Track fast-changing data breach laws, privacy rules and notification mandates
- ☐ Encrypt sensitive data
- ☐ Map locations of critical data
- ☐ Restrict access to information on a "need to know" basis
- ☐ Review employee lists and purge old user accounts
- ☐ Follow a data retention policy with a plan to destroy or dispose of unneeded data
- ☐ Identify and secure computer systems from vulnerabilities like common attack vectors
- ☐ Implement appropriate electronic and physical security

Incident Planning

BREACH INCIDENT RESPONSE CHECKLIST

- ☐ Seek expert forensic advice on the nature and scale of the incident
- ☐ Ensure data is no longer being compromised
- ☐ Secure all data and systems
- ☐ Isolate and preserve compromised data
- ☐ Leave the computer's POWER ON; disconnect from the network, if possible
- ☐ Identify the types of compromised data, affected parties, and scope of the breach
- ☐ Attempt to retrieve or neutralize compromised data
- ☐ Change encryption keys and passwords immediately
- ☐ Identify the time frame for who needs to be contacted and how
- ☐ Adhere to regulatory notification mandates and timeframes
- ☐ Document your work
- ☐ Work quickly; the clock starts ticking for potential notification rules upon first discovery of the breach
- ☐ Consider notifying law enforcement if you suspect criminal activity

Incident Planning

POST-BREACH CHECKLIST

- ☐ Assess gaps and evaluate effectiveness of plans, procedures and staff training
- ☐ Adjust security and response plans and processes; communicate and train
- ☐ Stay current; test your plan often and stay aware of changing threats and laws
- ☐ Maintain a breach report in accordance with regulatory standards
- ☐ Continue to restore customer relations; monitor crisis communications and if applicable, effectiveness of identity fraud monitoring vendors

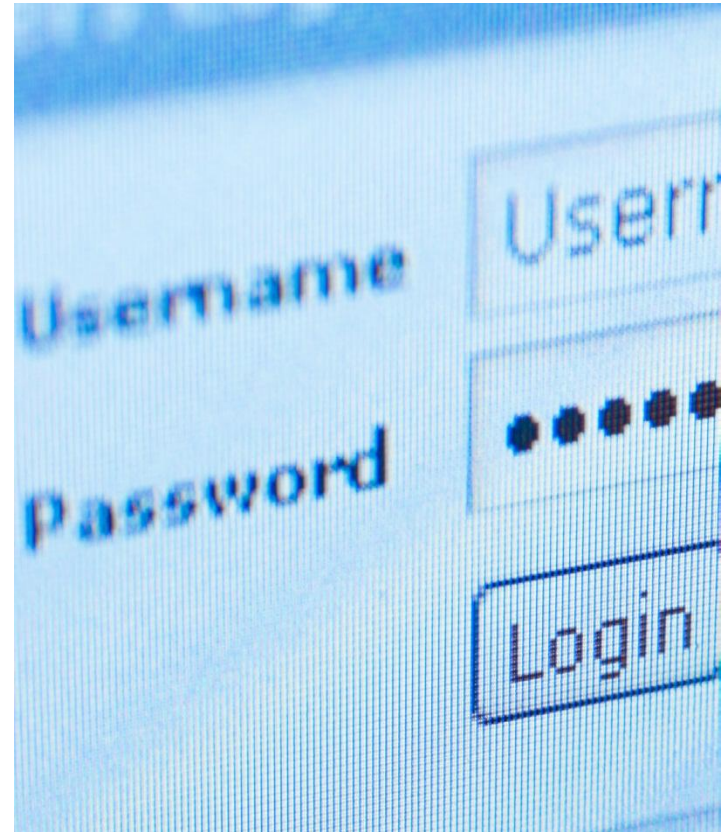
Conclusion

Cybersecurity will remain on agenda for foreseeable future

Still early in policy & regulation cycle

Stakes are high for companies in almost all sectors

Proactive measures, informed by 360-degree view of developments, will reduce risk and demonstrate good faith



Thank You!

Thomas Hibarger

Managing Director, Stroz Friedberg

thibarger@strozfriedberg.com

202.464.5803

Harriet Pearson

Partner, Hogan Lovells US LLP

harriet.pearson@hoganlovells.com

202-637-5477

Blog: hldataprotection.com