Using international standards to improve US cybersecurity

Wednesday, March 18, 2015

Alan Calder

IT Governance Ltd
www.itgovernanceusa.com

PLEASE NOTE THAT ALL DELEGATES IN THE TELECONFERENCE ARE MUTED ON JOINING AND WILL AUTOMATICALLY BE UNMUTED FOR THE START OF THE Q&A SESSION
Introduction

About Alan Calder…

• Acknowledged international cybersecurity expert
• Leading author on information security and IT governance issues
• Led the world’s first successful implementation of ISO 27001 (then BS 7799)
• Consultant on cybersecurity and IT governance strategies globally, including across the USA

© IT Governance Ltd 2015
Agenda

• **The current cyber threat** – Breaking down recent high-profile data breaches

• **Current legislation** – Reviewing the patchwork of state data breach notification laws

• **Proposed US legislation** – Learn about President Obama's proposed data breach notification law

• **International standard** – Discover how the cybersecurity standard, ISO 27001, will help get your business cyber secure

© IT Governance Ltd 2015
Current cyber threat
The current cyber threat

783
US data breach incidents in 2014

Health care and business
industries suffered most breaches in 2014

348.16 million
US records compromised

88%
believe cyber attacks are among the three biggest threats facing organizations

© IT Governance Ltd 2015
The current cyber threat

“This cyber threat is one of the most serious economic and national security challenges we face as a nation.”

“As a nation, we face constant cyber threats against our critical infrastructure and economy.”

“Companies that fail to adequately protect their networks will be at an increasing competitive disadvantage.”

46% of US companies have been asked for IT security credentials by customers in the past 12 months.
The changing threat landscape

• 87% of iPhone and 97% of Android top 100 Apps have been hacked
• 100% of companies experience virus attacks, and 97% have suffered malware attacks
• Every day, 156 million phishing emails are sent
• 15 million make it through spam filters
• The average global cost for each stolen record is $145 – in the USA it is $201
The changing threat landscape

Why did they fail to avoid a breach?

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaded existing preventive security controls</td>
<td>65%</td>
</tr>
<tr>
<td>Lack of in-house expertise</td>
<td>35%</td>
</tr>
<tr>
<td>Third-party vetting failure</td>
<td>20%</td>
</tr>
<tr>
<td>Poor leadership</td>
<td>15%</td>
</tr>
<tr>
<td>Incomplete knowledge of where sensitive data exists</td>
<td>12%</td>
</tr>
<tr>
<td>Lack of data classification</td>
<td>7%</td>
</tr>
<tr>
<td>Lack of accountability</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Root cause of data breaches

- Malicious or criminal attack: 42%
- System glitch: 29%
- Human error: 30%
Case study – Target

Data breach

- November/December 2013
- Hackers logged into the retailer’s network using credentials stolen from heating and ventilation firm Fazio Mechanical Services, which they stole through a sophisticated phishing attack
- Hackers were able to upload malware programs onto Target’s POS systems and remain undetected
- 110 million customers had their card data or personal information stolen
Case study – Target

Repercussions

• Target profits for the first six months of the fiscal year were down 41%
• Costs associated are estimated to have reached $148 million
• CEO Gregg Steinhafel and CIO Beth Jacob resign

What could Target have done differently?

• Properly secure third-party access to its network
• Segment network so third parties could not access payment systems/sensitive information
• Regular testing of their software to identify any vulnerabilities early on
Data breach

• September 2014
• Hackers used third-party credentials to break into network and installed POS malware through unpatched vulnerability
• Breach involved 56 million payment cards and 53 million customer email addresses
• Home Depot now facing at least 44 lawsuits
• Spending to deal with the breach has exceeded $43 million
Case study – Home Depot

What did Home Depot lack?

• The right attitude towards cybersecurity
  – When employees asked for security training, management response was: “We sell hammers”

• Up-to-date software
  – Allegedly used outdated Symantec antivirus software to protect its network

• Rigorous vetting of employees
  – Hired a computer engineer in 2012 who had been in prison for disabling computers at previous company
Case study – Sony Pictures

Data breach

- November 2014
- Hackers infiltrate Sony’s corporate computer network
- Torrents of unreleased Sony Pictures films appear online
- Personal information about employees (families, emails, salaries, etc.) is leaked
- Plaintext passwords are leaked online, along with other credential data
- Huge number of marketing slide decks are leaked
- Sony staff are kept from using computers for days
- Sony postpones release of upcoming film *The Interview*
Case study – Sony Pictures

Repercussions
• North Korea blamed, causing tension between the two nations
• Ex-employees seek to combine class action lawsuits against Sony
• Costs reach $100 million

How did the breach get so bad?
• Executives ignored ransom emails, treated as spam
• Failed to acknowledge breach until one week later
• General lax approach to online security
  – April 2011 - Sony’s PlayStation network hacked and 76 million gamers’ accounts compromised
  – Inappropriate spending? $250m budget still couldn’t keep them cyber secure
Small companies are at risk too

- Cyber criminals target indiscriminately
- 60% of breached small organizations close down within six months
- Often lack effective internal security practices
  - No dedicated IT security and support
  - Passwords, system access easily compromised
  - Out-of-date server hardware and software
  - Websites are built on common, open-source frameworks – weaknesses easily exploited
What is the board told?

- 32.5% of boards do not receive any information about their cybersecurity posture and activities
- 38% of the remainder receive reports only annually
- 29% of IT teams don’t report breaches for fear of retribution
Cybersecurity skills shortage

Shortage
- 209,000 unfilled cybersecurity positions in US
- 74% up on last five years

ISACA report
- 90% believe there is a shortage
- 41% expect difficulties finding skilled candidates
- 58% plan to increase staff training

Companies should be looking for
- Industry-recognized qualifications (IBITGQ)
Current legislation
Data breach notification laws

Consumer data is currently protected by a patchwork of state legislation

Industry-specific laws

- **FISMA** – requires federal agencies to implement appropriate information security programs

- **HIPAA** – aims to protect health care information

- **SOX** – improves accuracy and reliability of financial disclosures
Costs of a data breach in America

- Data breach notification cost = $509,237
- Post-data breach costs = $1,599,996
- Lost business cost = $3,324,959

- Ponemon Institute Cost of Data Breaches Report 2014

© IT Governance Ltd 2015
Proposed US data breach notification legislation
Personal Data Notification and Protection Act

- Single, strong, national standard
- Notify individuals within **30 days** of data breach
- Punishment could be up to **10 years in prison**
Reducing the cost of a breach

- A strong security posture
- An effective incident response plan
- A CISO appointment
- Implementing industry standards
ISO 27001 – the cybersecurity standard

ISO 27001 – a globally recognized standard that provides a best-practice framework for addressing the entire range of cyber risks

- Encompasses people, processes, and technology
- Systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives

© IT Governance Ltd 2015
Key elements of implementing ISO 27001

- Determine the scope of the ISMS
- Consider the context of the organization and interested parties
- Appoint a senior individual responsible for information security
- Conduct a risk assessment – identify risks, threats, and vulnerabilities
- Appoint risk owners for each of the identified risks
- Implement appropriate policies and procedures
- Conduct staff training
- Conduct an internal audit
- Implement continual improvement of the ISMS
How will ISO 27001 benefit your business?

- Increased/appropriate level of information security
  - Systematic approach to risks
  - Informed decisions on security investments: cost-effective security
- Better work practices that support business goals
- Good marketing opportunities
- Credibility with staff, customers, and partner organizations
- Due diligence
- Compliance with corporate governance requirements
  - Appropriate action to comply with law
  - Manage business risks
  - Industry best-practice security
  - Internationally recognized good security practice

© IT Governance Ltd 2015
Benefits of ISO 27001 registration

• Assurance to customers, employees, investors – their data is safe
• Credibility and confidence
• Internationally recognized
• Shows that you have considered all of the information security-associated risks
• Notably fulfilling fiduciary responsibilities
• Supports your adherence to multiple compliance requirements
ISO 27001 in the US

Number of ISO 27001-registered organizations in America*

Between 2012 and 2013 the number of ISO 27001-registered organizations jumped 36%.

* Source: ISO Survey 2013
Why some of the world’s most valuable brands pursue ISO 27001 registration

Google: “This certification validates what I already knew...that the technology, process and infrastructure offers good security and protection for the data that I store in Google Apps”

Amazon: “The certification confirms our longstanding commitment to the security of our services to our customers.”

Microsoft: “…provides external validation that our approach to managing security risk in a global organization is comprehensive and effective, which is important for our business and consumer customers.”

© IT Governance Ltd 2015
Fixed-priced, packaged solutions

The Basics
- $659
- You deliver the project independently
- Software and documentation templates
- Standards and books

Do It Yourself
- $3,160
- The project, calling on specialist tools and courses to aid efficiency and accelerate implementation

Get A Little Help
- $6,800
- Use tools and courses and benefit from the expert’s know-how

Get A Lot of Help
- $16,700
- $14,995
- The project, receiving hands-on guidance from us
- Mentor and coach
- IT Governance removes all the pain, delivering a registration-ready ISMS, aligned with ISO 27001

We Do It For You
- From $8,500
- $7,650

Find out more: www.itgovernanceusa.com/iso27001-solutions.aspx
IT Governance

• Helped over 150 organizations achieve ISO 27001 registration worldwide
• 15+ years’ experience
• Highly regarded within the industry
• Unique offering of tools, training, and consultancy unavailable elsewhere

© IT Governance Ltd 2015