Cybersecurity: Protecting Your Business

March 11, 2015
Agenda

• Introductions
  – Presenters

• Cybersecurity
  – Cybersecurity Trends
  – Cybersecurity Attacks
  – Incident Response
  – Industry Response
Learning objectives

• Assess how cybersecurity affects your business
• Explore strategic ideas to mitigate cybersecurity risk and review your own organization's protocols
• Discuss how to protect your company from a breach, including safeguarding credit cards and sensitive information
• Outline measures for protecting your business before and after a data breach
Chanson Ho  
Grant Thornton LLP  
Senior Manager, Business Advisory Services  
Tel: 213.596.8419  |  email: Chanson.Ho@us.gt.com

Chanson is a Senior Manager in Grant Thornton’s Southern California Business Advisory Services Practice. He is also the firm’s West Region Governance, Risk, and Compliance Solution leader.

In his 14 years of public accounting and advisory experience, including 9 years with a Big Four firm, he has worked with publicly-traded, private-equity held, and venture-backed companies including financial services, manufacturing, retail, technology, and healthcare industries. Chanson is a CPA and has earned his master’s degree in Accounting from University of Southern California, and his bachelor’s degree in Economics from University of California at Berkeley.
Jeff Cheung is a Manager in Grant Thornton’s Los Angeles Business Advisory Services practice. He is a licensed Certified Information Systems Auditor, as well as a Payment Card Industry – Qualified Security Assessor with extensive experience in security assessments related to the network, operating system, application and database layers. Jeff’s professional experience includes PCI Reports on Compliance, Penetration Testing, Physical Security, and technology audits.
Cybersecurity Trends
Cybersecurity Trends
Cybersecurity Trends

Let's talk about it…

• It will never happen to me
• I think our network is secure
• We are in compliance with industry standards
• We are not a big company
• We don't have any personal information so we aren't a target
• We have never been attacked
Data breaches can be **financially costly** to organizations and could amount to **millions in losses**. Additionally, organizations can be held liable for **breaches** and **losses**, which may result in **fines or litigation**.
Cybersecurity Trends
Data Breaches Are Common

- **Feb. 2015:** Anthem Blue Cross – 80 million current and former Anthem health care customers' personal information stolen including SSNs and medical ID numbers.

- **Jan. 2015:** GrillParts.com – Their e-commerce website was breached from Jan 2014 – Oct 2014 and exposed customer information, including names, addresses, and credit card numbers.

- **Dec. 2014:** ABM Parking Services – Vendor supplied and maintained POS terminals were hacked and exposed customer information including credit card data.

- **Nov. 2014:** Sony Pictures Entertainment - Network breached by alleged North Korean hackers citing Sony's "terrible racial discrimination" stemming from the impending release of 'The Interview'. Over 100 Terabytes of data stolen, including thousands of financial documents and emails revealing the film studio's inner secrets that were leaked to the public.

- **Sept. 2014:** Home Depot – 56 million credit cards compromised via POS Malware attack at 2,200 stores in the US and Canada.
Cybersecurity Trends

Data breaches are expensive

- Malicious or criminal attacks are the most expensive cause of data breaches and are on the rise. In 2013, **90% of data breach cases involved malicious attacks. Negligence and insider misuse accounted for 10% of reported breaches.**

- Direct costs include:
  - Forensic support
  - Lost record support services for impacted individuals, including credit monitoring services, and hotline support
  - Refunds or discounts on products or services

- Indirect costs include:
  - In-house investigation and remediation costs
  - Communications costs
  - Customer losses associated with turnover and diminished acquisition rates

- **DOES NOT INCLUDE FINES**
Cybersecurity Trends

Who is responsible?

Within your organization, who is responsible for cybersecurity?

- **CIO, 36%**
- **CFO, 38%**
- **CISO, 7%**
- **Other, 19%**
Cybersecurity Trends

Where do you view the risk?

What are your organization's top cybersecurity and data privacy concerns?
Cybersecurity Trends

How are you addressing?

Does your organization have a cybersecurity task force?

If yes, what areas of the business are represented on the task force?
Cybersecurity Attacks
Cybersecurity Attacks
Notable Statistics

• Reported complaints amounted to $781M in 2013
• State with most complaints was California (14.92%)
• State with highest losses was also California (18.30%) $105M
• Billions of Dollars are spent every year to repair systems
• High number of incidents are still not reported

"We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?"
## Cybersecurity Attacks
How cybersecurity affects your organization

*Threats and Trends (2014 Verizon Breach Report)*

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>POS INTRUSION</th>
<th>WEB APP ATTACK</th>
<th>INSIDER MISUSE</th>
<th>THEFT/LOSS</th>
<th>MISC. ERROR</th>
<th>CRIMEWARE</th>
<th>PAYMENT CARD SKIMMER</th>
<th>DENIAL OF SERVICE</th>
<th>CYBERESPIONAGE</th>
<th>EVERYTHING ELSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>75%</td>
<td>1%</td>
<td>8%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>10%</td>
<td>4%</td>
<td>7%</td>
</tr>
<tr>
<td>Administrative</td>
<td>56%</td>
<td>8%</td>
<td>27%</td>
<td>12%</td>
<td>43%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>7%</td>
</tr>
<tr>
<td>Construction</td>
<td>7%</td>
<td>13%</td>
<td>13%</td>
<td>7%</td>
<td>33%</td>
<td>1%</td>
<td>1%</td>
<td>13%</td>
<td>13%</td>
<td>7%</td>
</tr>
<tr>
<td>Education</td>
<td>&lt;1%</td>
<td>19%</td>
<td>8%</td>
<td>15%</td>
<td>20%</td>
<td>6%</td>
<td>&lt;1%</td>
<td>6%</td>
<td>22%</td>
<td>2%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>7%</td>
<td>22%</td>
<td>10%</td>
<td>7%</td>
<td>12%</td>
<td>2%</td>
<td>2%</td>
<td>32%</td>
<td>5%</td>
<td>10%</td>
</tr>
<tr>
<td>Finance</td>
<td>&lt;1%</td>
<td>27%</td>
<td>7%</td>
<td>5%</td>
<td>4%</td>
<td>22%</td>
<td>26%</td>
<td>&lt;1%</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
<td>3%</td>
<td>15%</td>
<td>46%</td>
<td>12%</td>
<td>3%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>&lt;1%</td>
<td>10%</td>
</tr>
<tr>
<td>Information</td>
<td>&lt;1%</td>
<td>41%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>31%</td>
<td>&lt;1%</td>
<td>9%</td>
<td>1%</td>
<td>16%</td>
</tr>
<tr>
<td>Management</td>
<td>11%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>4%</td>
<td>4%</td>
<td>42%</td>
<td>11%</td>
<td>6%</td>
<td>11%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>31.32.33</td>
<td>14%</td>
<td>8%</td>
<td>4%</td>
<td>2%</td>
<td>9%</td>
<td>24%</td>
<td>30%</td>
<td>9%</td>
<td>30%</td>
</tr>
<tr>
<td>Mining</td>
<td>25%</td>
<td>10%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>40%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>Professional</td>
<td>&lt;1%</td>
<td>9%</td>
<td>6%</td>
<td>4%</td>
<td>3%</td>
<td>3%</td>
<td>37%</td>
<td>29%</td>
<td>8%</td>
<td>4%</td>
</tr>
<tr>
<td>Public</td>
<td>&lt;1%</td>
<td>24%</td>
<td>19%</td>
<td>34%</td>
<td>21%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>10%</td>
<td>2%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>10%</td>
<td>37%</td>
<td>13%</td>
<td>20%</td>
<td>7%</td>
<td>3%</td>
<td>10%</td>
<td>10%</td>
<td>2%</td>
<td>10%</td>
</tr>
<tr>
<td>Retail</td>
<td>31%</td>
<td>10%</td>
<td>4%</td>
<td>2%</td>
<td>2%</td>
<td>6%</td>
<td>33%</td>
<td>&lt;1%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Trade</td>
<td>6%</td>
<td>30%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>9%</td>
<td>3%</td>
<td>3%</td>
<td>10%</td>
<td>27%</td>
</tr>
<tr>
<td>Transportation</td>
<td>48.49</td>
<td>15%</td>
<td>16%</td>
<td>7%</td>
<td>5%</td>
<td>15%</td>
<td>5%</td>
<td>3%</td>
<td>24%</td>
<td>8%</td>
</tr>
<tr>
<td>Utilities</td>
<td>39%</td>
<td>3%</td>
<td>1%</td>
<td>2%</td>
<td>31%</td>
<td>14%</td>
<td>7%</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>29%</td>
<td>13%</td>
<td>13%</td>
<td>10%</td>
<td>3%</td>
<td>9%</td>
<td>6%</td>
<td>17%</td>
<td>17%</td>
</tr>
</tbody>
</table>
Cybersecurity Attacks
Lessons learned related to the safeguarding of sensitive data


**Top Cybersecurity Threats**

- **POS Intrusion**
  - Use of stolen credentials
  - POS terminal vulnerabilities
  - RAM Scrapers

- **Web App Attacks**
  - Use of stolen credentials
  - Application weaknesses
  - DDoS
Top Cybersecurity Threats (Continued)

- **Insider and Privilege Misuse**
  - Privilege abuse
  - Unapproved hardware
  - Embezzlement

- **Physical Theft and Loss**
  - Tampering

- **Miscellaneous Errors**
  - Poor internal business process controls
Cybersecurity Attacks
Lessons learned related to the safeguarding of sensitive data


Top Cybersecurity Threats (Continued)

• Crimeware
  • Stolen credentials
  • Malware infections

• Payment Card Skimmers
  • Physical tampering of payment terminals

• Cyber Espionage
  • Hacking for political gain
  • Website defacement
  • Stolen intellectual property
Cybersecurity Attacks
Lessons learned related to the safeguarding of sensitive data

*Top Cybersecurity Threats (2014 Verizon Breach Report)*

Top Cybersecurity Threats (Continued)

- **DoS Attacks**
  - Botnets
  - Degradation of Service

- **Everything Else**
  - Phishing
  - Browser hacking
  - Social engineering
Incident Response & Risk Management
Incident Response & Risk Management
4 ways to prepare for a breach:

1. **Data mapping/classification**: Before you come up with a plan to protect your data, you need to figure out exactly what it is you are protecting.

2. **Conduct a vendor assessment**: You need to account for data held by business partners, vendors and other third parties.

3. **Create a risk profile**: There’s no good way to know just how vulnerable your systems are without having someone try to hack them.

4. **Create your incident response (IR) team and plan of action**: Know who does what and when.
Incident Response & Risk Management

What happens in a breach?

• In most organizations, breach notification will come from an external entity. Very few organizations have the required detective controls in place to know if data was read/copied by an unauthorized party.

• How do they know it's you? Determination of "Common point of purchase"

• **Forensic analysis** – Determining the extent of the losses

• **Compliance status** – Determining the compliance of organizations with applicable laws / regulations

• **Remediation** – Implementation of controls to prevent reoccurrence

• **Monitoring** – Continuous process of evaluating the effectiveness of those implemented controls.

• **Follow up / Fines** – Depends upon the severity of the breach, and "willful non-compliance"
Incident Response & Risk Management

What to do if a breach occurs?

Execute Your Plan

• Follow your Escalation Protocol
• Preserve affected machines and area
• Assemble your team and take inventory

Respond to the Breach…

MOVE QUICKLY & DOCUMENT YOUR WORK AS YOU:

• Preserve the Evidence
• Identify the Compromised Data
• Communicate Progress
Incident Response & Risk Management

What to do if a breach occurs?

- State breach notification laws (now in 46 states, DC, PR, and USVI) generally require notification of individuals if their “personal information” was, or is reasonably believed to have been, acquired by an unauthorized person.
- Different industries maintaining specific data types can also drive additional notification requires. For example, the HIPAA's breach notification rule.

✓ Have a breach incident response plan
✓ Communicate, communicate, communicate
Incident Response & Risk Management

What is *Not* a Breach?

- If de-identified information is disclosed
- If you believe, in good faith, that the unauthorized person could *not* reasonably have retained information
- If a worker accesses sensitive information without permission but in good faith, as long as there is *no* further unauthorized action
- If a worker reveals sensitive information to an unauthorized colleague, as long as there is *no* further unauthorized action
Industry Response
Industry Response

NIST Framework for Improving Critical Infrastructure Cybersecurity

• Created through collaboration between industry and government
• Consists of standards, guidelines, and practices to promote the protection of critical infrastructure
• Based on existing standards, guidelines, and practices - for reducing cyber risks
Industry Response

New Requirements of Payment Card Industry Data Security Standard (PCI DSS) 3.0

• **Increased Vendor Scrutiny**
  – Credit Card redirects do not remove you from PCI scope
  – Vendors restricted from reusing passwords between customers
  – Contractual descriptions of PCI controls handled by vendors

• **Increased ROC Reporting Requirements**
  – Increased descriptions of controls
  – Increased scoping requirements
  – Decreased likelihood of "checklist" audits
Industry Response

External/internal penetration assessment explained

- **External Assessment**
  - Perspective: Assessing from across the Internet
  - Example: Hackers from China, Attacker in their basement
  - Must break through firewalls and intrusion detection/prevention systems
  - External Threats – Largest Attack Population

- **Internal Assessment**
  - Perspective: Inside the corporate network
  - Example: Access an employee has
  - Already past the perimeter firewall
Industry Response

Increased due diligence

1. AICPA SOC 2 Audits – Trust Services Principles and Criteria (Security, Confidentiality, Availability, Processing Integrity, and Privacy)
2. GLBA Assessments
   - Review of Privacy Controls in place to protect customer financial information
3. FFIEC Audits
   - Review of Information Security Controls to protect bank operations
4. ISO 27001:2013 Assessments
   - Review of Information Security based on International best practices
Disclaimer

In accordance with certain professional standards, we inform you that this document supports Grant Thornton LLP’s marketing of professional services and is not written tax, accounting or other advice directed at the particular facts and circumstances of any person. We encourage you to discuss with us, or an independent tax advisor, legal counsel or other advisors the potential application of this document to your particular situation.

Nothing herein shall be construed as imposing a limitation on any person from disclosing the tax treatment or tax structure of any matter addressed herein. To the extent this document may be considered to contain written tax advice, any written advice contained in, forwarded with or attached to this document is not intended by Grant Thornton to be used, and cannot be used, by any person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.