DATA BREACHES: WHEN COMPLIANCE IS NOT ENOUGH

Andy Watson
I HAVE A NEW HOBBY. IT’S CALLED PHISHING.

I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON’T DESERVE.

Dear Customer,
This is your bank. We forgot your social security number and password. Why don’t you send them to us so we can protect your money.

Sincerely,
I. B. Banker

LOOKS LEGIT.
SURVEY OF CHIEF AUDIT EXECUTIVES (CAEs)
Data privacy and security are top risks…

42% agree data privacy, security risks, and regulations have the potential to impact growth significantly.

Which of the following risk areas have the potential to impact your organization’s growth?

<table>
<thead>
<tr>
<th>Areas</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data privacy and security</td>
<td>42%</td>
</tr>
<tr>
<td>Regulation</td>
<td>38%</td>
</tr>
<tr>
<td>Execution of strategy</td>
<td>38%</td>
</tr>
<tr>
<td>Third parties/vendors</td>
<td>22%</td>
</tr>
<tr>
<td>Mobile technologies</td>
<td>19%</td>
</tr>
<tr>
<td>Fraud/anti-corruption</td>
<td>14%</td>
</tr>
<tr>
<td>Supply chain</td>
<td>14%</td>
</tr>
<tr>
<td>Business continuity</td>
<td>13%</td>
</tr>
<tr>
<td>Global expansion</td>
<td>13%</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>12%</td>
</tr>
<tr>
<td>Social media</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>
Data privacy and security are second most audited areas…

70% have data privacy and security included in their audit plans.

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Currently in scope</th>
<th>Will include in the next 12 months</th>
<th>No plans to include in the near future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud computing</td>
<td>24%</td>
<td>36%</td>
<td>45%</td>
</tr>
<tr>
<td>Mobile technologies</td>
<td>25%</td>
<td>45%</td>
<td>35%</td>
</tr>
<tr>
<td>Social media</td>
<td>19%</td>
<td>30%</td>
<td>56%</td>
</tr>
<tr>
<td>Data privacy and security</td>
<td>70%</td>
<td>41%</td>
<td>7%</td>
</tr>
<tr>
<td>Third parties/vendors</td>
<td>66%</td>
<td>36%</td>
<td>14%</td>
</tr>
<tr>
<td>Fraud/anti-corruption</td>
<td>69%</td>
<td>34%</td>
<td>15%</td>
</tr>
<tr>
<td>Supply chain</td>
<td>46%</td>
<td>31%</td>
<td>32%</td>
</tr>
<tr>
<td>Business continuity</td>
<td>52%</td>
<td>37%</td>
<td>22%</td>
</tr>
<tr>
<td>Regulation</td>
<td>73%</td>
<td>36%</td>
<td>10%</td>
</tr>
<tr>
<td>Execution of strategy</td>
<td>36%</td>
<td>36%</td>
<td>38%</td>
</tr>
<tr>
<td>Global expansion</td>
<td>21%</td>
<td>24%</td>
<td>61%</td>
</tr>
<tr>
<td>Other</td>
<td>12%</td>
<td>18%</td>
<td>75%</td>
</tr>
</tbody>
</table>
DATA BREACHES IN 2014
How do breaches occur?

- 52% Used some form of hacking
- 76% Exploited weak or stolen credentials
- 40% Incorporated malware
- 35% Involved physical access abuse
- 29% Leveraged social tactics
- 13% Resulted from privilege misuse and abuse

Source: Verizon 2014 Data Breach Investigations Report
CYBERSECURITY: THE MYSTERIOUS HOT TOPIC
CYBER SECURITY
WHAT EXACTLY IS IT?

• Preventive methods used to protect information or systems from being stolen, compromised or attacked.

• More than technology, it is a layered methodology of people, processes, communications and controls.

• Requires an understanding of potential threats such as malware, hackers and other malicious acts.
CYBERSECURITY PROGRAM METHODOLOGY
• Privacy is concerned with enabling individuals to have say over how their personal information is collected, used, retained, and disclosed.

• Security is concerned with protecting information from inappropriate access, modification, or destruction.

• Compliance is concerned with complying with government rules/regulations or contractual requirements.
Personally Identifiable Information (PII)

- Name, address, e-mail address
- Social Security Number
- Driver's license number or state-issued identification card number
- Financial account number, credit card number, or debit card number
- Credit records
- Buying history
- Employee record

Other Sensitive Information

- User credentials
- Age, gender, race, ethnicity
- Grades
- Salary or job position
- Criminal record
- Purchase history
- Pricing information
- Financial information
- Customer lists
CYBER SECURITY
DATA SECURITY LIFECYCLE

Create
- Data created and assigned metadata

Store
- Access Controls
- Encryption
- Rights Management
- Content Discovery

Use
- Activity Monitoring and Enforcement
- Rights Management
- Logical Controls
- Application Security

Destroy
- Crypto-Shredding
- Secure Deletion
- Physical Destruction

Archive
- Encryption
- Asset Management

Share
- DLP
- Encryption
- Logical Controls
- Interface Controls
CYBER SECURITY
PROGRAM METHODOLOGY

THE FRAMEWORK

IDENTIFY
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT
- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recovery planning
- Improvements
- Communications
COMPLIANCE DOES NOT EQUAL CYBERSECURITY
# Cyber Security Common Compliance Standards

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Objective</th>
<th>Limited Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCI DSS</strong></td>
<td><strong>Payment Card Industry Data Security Standard</strong></td>
<td>Protects cardholder data (i.e., credit cards, debit cards, etc.)</td>
<td>Cardholder data</td>
</tr>
<tr>
<td><strong>HIPAA</strong></td>
<td><strong>Health Insurance Portability and Accountability Act</strong></td>
<td>Governs the use and disclosure of Protected Health Information (PHI)</td>
<td>Protected Health Information (PHI)</td>
</tr>
<tr>
<td><strong>GLBA</strong></td>
<td><strong>Gramm-Leach-Bliley Act</strong></td>
<td>Governs the collection, disclosure, and protection of consumer’s non-public personal information by financial institutions</td>
<td>Consumer’s non-public personal information</td>
</tr>
<tr>
<td><strong>SOX</strong></td>
<td><strong>Sarbanes-Oxley</strong></td>
<td>Governs the adequacy of a company’s internal control on financial reporting</td>
<td>Internal controls over financial reporting</td>
</tr>
<tr>
<td><strong>SOC Reports</strong></td>
<td><strong>Service Organization Controls Report</strong></td>
<td>Documents and tests controls implemented by outsourced service providers.</td>
<td>Controls over outsourced services</td>
</tr>
</tbody>
</table>
## CYBER SECURITY

### COMMON COMPLIANCE STANDARDS:

### PCI DSS REQUIREMENTS

<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
</table>
| Build and maintain a secure network                      | 1. Install and maintain a firewall configuration to protect cardholder data  
|                                                          | 2. Do not use vendor-supplied defaults for system passwords and other security parameters                                                       |
| Protect cardholder data                                  | 3. Protect stored cardholder data  
|                                                          | 4. Encrypt transmission of cardholder data across open, public networks                                                                            |
| Maintain a vulnerability management program              | 5. Use and regularly update anti-virus software on all systems commonly affected by malware  
|                                                          | 6. Develop and maintain secure systems and applications                                                                                           |
| Implement strong access control measures                 | 7. Restrict access to cardholder data by business need-to-know  
|                                                          | 8. Assign a unique ID to each person with computer access  
|                                                          | 9. Restrict physical access to cardholder data                                                                                                   |
| Regularly monitor and test networks                      | 10. Track and monitor all access to network resources and cardholder data  
|                                                          | 11. Regularly test security systems and processes                                                                                                 |
| Maintain an information security policy                   | 12. Maintain a policy that addresses information security                                                                                         |
Phase 1: Determine Objectives

Phase 2: Assess Control Environment

Phase 3: Address Gaps
Phase 1: Determine Objectives

- What type of data does the Company want to protect?
- Where is the data located? Consider the Data Security Lifecycle
- Why does the Company want to protect the data?
- Who does the Company want to protect the data from?
- How could the data be compromised?
- What is the impact if the data was compromised?
- What price does the Company want to pay to protect the data?
• What Compliance Programs (i.e., PCI DSS, SOX, etc.) does the Company comply with?
• What Cyber Security risks are not addressed by these Compliance Programs?
• Who has access to the data?
• What controls does the Company have to protect the identified data?
• Are the controls documented and tested on a regular basis?
• What are the Company's Cybersecurity gaps?
Phase 3: Address Gaps

- Develop a layered Cyber Security approach to address the Cyber Security gaps at all layers of the Technology Model.
- Implement documented polices and procedures for protecting the Company's data.
- Implement a test plan and test your Cyber Security program.
- Educate employees on their responsibilities for protecting the Company's data.
- Implement a process to re-assess your Cyber Security program on a regular basis.
Ensure that all relevant layers and endpoints of the business and information technology environment are addressed during the Cybersecurity risk assessment process.

Consider what tools can be used to help analyze and address information security risks at all layers of the Technology Model:

- Data loss prevention software
- Perimeter security
- Scanning and monitoring tools
- Data encryption
- Identity and access controls
- Laptop/Mobile Security Tools
- Virus/spyware/malware protectors
CYBER SECURITY
PERPETRATORS

- Hackers
- Crackers
- Script Kiddies
- Corporate Spies
- Unethical Employees (Insiders)
- Cyber Extortionists
- Cyber Terrorists
- Jerks
CASE STUDY
TARGET CORPORATION
"In mid-December, we learned criminals forced their way into our system, gaining access to guest credit and debit card information. The investigation has recently determined that certain guest information was taken. That included names, mailing addresses, e-mail addresses, or phone numbers. We have partnered with a leading third-party forensics firm who is thoroughly investigating the breach."

- Target.com
What data was stolen?

The security breach is one of the largest breaches in U.S. retail history.

It included over **40 million credit and debit cards** and up to **70 million customers' Personally Identifiable Information**
What are the costs of the data breach?

Estimated losses between $1 billion and $4 billion in fraudulent charges.

The banking industry has already started to request payment from Target to recover some of the estimated loss of 30% to 50% of any fraud losses, along with stiff fines.

Several lawsuits have already been filed, including some from smaller banks that want a higher recovery.

Target's 2013 fourth-quarter profits were down 46%.

Sales fell 5.3%

Target's CIO resigned.

The Company is "enhancing the role" of the Chief Compliance Officer and the Chief Information Security Officer.
How did the breach occur?

The hackers used a malware phishing e-mail to compromise the user-id and password for one of Target's vendors, a HVAC company.

The vendor's user account was then used to access Target's internal network and deploy the Malware "Trojan.POSRAM".
CASE EXAMPLE
HOW THE BREACH OCCURRED

How did the Malware work?

The malware "Trojan.POSRAM" was consumed by Target's Point of Sale ("POS") payment programs to monitor the POS information that was processed in memory.

The POS processes authorization of data, including full credit card/debit card magnetic stripe data.

When data is processed, the application decrypts the transaction on the cash register system or backend server and stores the authorization data in random access memory ("RAM").

The hackers were able to access full track data when it was stored in RAM and using the RAM-Scraping malware to steal the data.

When the malware identified that it had obtained the correct data, it stored the data it to a file on the local system.

Then the malware transmitted the file through Target's network using the "Ping" command to an internal host server which was periodically accessed by the hackers using the stolen vendor's account.
CASE EXAMPLE
TIMELINE OF EVENTS

Trying Times
Target’s discovery that cybercriminals had stolen the credit and debit card numbers of about 40 million customers led to a series of difficult decisions.

$70 a share

**Nov. 27-Dec. 18** Unknown to Target, cybercriminals were stealing the numbers from credit and debit cards swiped at store registers.

**Dec. 18** Company says ‘strong start to its holiday season has continued.’

**Dec. 19** Target says the card numbers of 40 million customers were stolen between Nov. 27 and Dec. 18.

**Dec. 27** Target says PIN data also were stolen.

**Jan. 10** Target says up to 70 million more customers had personal information such as names and email addresses stolen.

**Jan. 13** CEO Gregg Steinhafel offers apology in full-page newspaper ads.

**Jan. 29** Target confirms that cybercriminals gained network access through an outside vendor.

**Feb. 4** CFO John Mulligan testifies before Congress about need to convert cards from magnetic strips to chip-enabled technology.

**Feb. 18** Stock closes at $56.39, down 11.3% since Target revealed that card numbers had been stolen.

Sources: WSJ Market Data Group; news reports
What are some takeaways from the Target breach?

1) Protect your organization’s reputation and bottom line with **fast, accurate breach assessment**. Doing so enables effective communication and response that limits reputational and perhaps financial damage. Target’s name was pummeled repeatedly as additional information came to light—first the breach of up to 40 million credit and debit cards, and then the theft of up to 70 million people’s personal information.

2) Operationalize your **cybersecurity risk assessment** and **breach response processes**. This moves your organization from the typical, knee-jerk reaction of incident response to a more strategic, daily approach.

3) **Upgrade** your risk analysis—and your technology—to meet changing threats. The Target breach happened at the point-of-sale, a place considered not as vulnerable. It appears that Target used an outdated algorithm to encrypt PIN data.
What are some takeaways from the Target breach?

4) Understand how quickly an attack can spread through a system. Large retailers such as Target should constantly be on guard for attacks because their networks have multiple access points that need to be monitored.

5) Never underestimate how motivated thieves are to break into a system—and how much is at stake. This is especially true for medical information, which, according to Kirk Herath, Nationwide Chief Privacy Officer, has a street value of $50—versus the $1 value of a stolen Social Security number.

6) **Never put sole reliance on compliance** when it comes to cybersecurity.
“Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we suffered a data breach [in November 2013]. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience.”

- Gregg Steinhafel, Target CEO
FINAL TAKEAWAYS
You must have a plan…

- Inventory compliance programs.
- Perform a Cyber Security Risk Assessment to identify gaps not covered by compliance programs.
- Work with management to develop a plan to address Cyber Security gaps.
Reminder: Sign the attendance sheet to ensure you receive CPE credit for this session.
CONTACT

Andy Watson
Advisory Services Senior Consultant
Grant Thornton
E andy.watson@us.gt.com
T (617) 848-5013