Prevention of Data Breach

April, 2014
Jeff Sanchez is a Managing Director in Protiviti’s Los Angeles office. He joined Protiviti in 2002 after spending 10 years with Arthur Andersen’s Technology Risk Consulting practice. Jeff has participated in technical consulting and audit projects primarily in the hospitality, gaming, financial services and retail industries. Jeff leads Protiviti’s global Data Security and Privacy practice and is a subject-matter expert in the Payment Card Industry Data Security Standard. For the last six years, Jeff has concentrated on the design and implementation of security and privacy solutions. Jeff is a CIA, CISM, CISA, PA-QSA, CIPP/US and PMP.

jeffrey.sanchez@protiviti.com
## Agenda

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach Overview</td>
<td>4</td>
</tr>
<tr>
<td>Data Breach Methodologies: Social Media and Mobile</td>
<td>11</td>
</tr>
<tr>
<td>Best Practices</td>
<td>14</td>
</tr>
<tr>
<td>Data Breach Incident Response</td>
<td>18</td>
</tr>
<tr>
<td>What You Can Do Today</td>
<td>20</td>
</tr>
<tr>
<td>Questions</td>
<td>24</td>
</tr>
</tbody>
</table>
Data Breach Overview
Large Data Breaches of the Decade

CardSystems Solutions: 40 million credit card accounts exposed. CSS, one of the top payment processors for Visa, MasterCard, American Express is ultimately forced into acquisition.

2005

AOL: Data on more than 20 million web inquiries, from more than 650,000 users, including shopping and banking data were posted publicly on a web site.

2006

Monster.com: Confidential information of 1.3 million job seekers stolen and used in a phishing scam.

2007

Wyndham Hotels: were sued by the US Federal Government after sensitive customer data, including credit card numbers and personal information, allegedly were stolen three times in less than two years.

2008

“Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated.”
— The IIA Research Foundation

2009

Google/other Silicon Valley companies: Stolen intellectual property

2010

VeriSign: Undisclosed information stolen

2011

Sony’s PlayStation Network: 77 million PlayStation Network accounts hacked; Sony is said to have lost millions while the site was down for a month.

2013

Target Credit and Debit Card data breach!!

Source: CNN, NBC, CSO Online

© 2014 Protiviti Inc.
CONFIDENTIAL: This document is for your company’s internal use only and may not be copied nor distributed to another third party.
Data Breach Overview

- 89 percent of data breaches could have been prevented and 40 percent of the largest data breaches were recorded in 2013.

- 2013 culminated with Target’s breach, which is estimated to impact upwards of 110 million credit and debit card accounts.

- As per Verizon, 2013 report:
  - 92 percent of data breaches were caused due to External threat actors
  - 14 percent were caused due to Internal threat actors
  - 1 percent were caused due to Partners

Source: Online Trust Alliance, Verizon 2013 Report
Data Breaches Statistics (1/2)

Number of Breaches in 2013

Overview:
- Targeted attacks increased in January, 2014 reaching their highest levels since August, 2013.
- Small companies of 250 employees or less were targeted in 39% of attacks through organizations with 2500+ employees were targeted more often.
- The .exe file type was the most common attachment, making up 24.7% of email-based targeted attacks that included file attachments.

Source: Symantec

© 2014 Protiviti Inc.
CONFIDENTIAL: This document is for your company's internal use only and may not be copied nor distributed to another third party.
Data Breach Statistics

Who’s Perpetrating Breaches?

- Perpetrated by outsiders: 92%
- Committed by insiders: 14%
- Implicated business partners: 1%
- Involved multiple parties: 7%
- Attributed to state-affiliated actors: 19%

How Do Breaches Occur?

- Hacking: 52%
- Network intrusions: 76%
- Malware: 40%
- Physical attacks: 35%
- Social tactics: 29%
- Privilege misuse and abuse: 13%

Percent of Total Breaches

In the last 12 months (February, 2013 – January, 2014), more than 500 million identities have been exposed.

A data breach in November, 2013 is now estimated to have exposed 110 million identities.

Source: Symantec, Verizon 2013 Report
## Profiling Threat Actors

<table>
<thead>
<tr>
<th>VICTIM INDUSTRY</th>
<th>ORGANIZED CRIME</th>
<th>STATE-AFFILIATED</th>
<th>ACTIVISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Manufacturing</td>
<td>Professional</td>
<td>Information</td>
</tr>
<tr>
<td>Retail</td>
<td>Professional</td>
<td>Transportation</td>
<td>Public</td>
</tr>
<tr>
<td>Food</td>
<td></td>
<td></td>
<td>Other Services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION OF OPERATION</th>
<th>ORGANIZED CRIME</th>
<th>STATE-AFFILIATED</th>
<th>ACTIVISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eastern Europe</td>
<td>Tampering (Physical)</td>
<td>Backdoor (Malware)</td>
<td>SQLi (Hacking)</td>
</tr>
<tr>
<td>North America</td>
<td>Brute force (Hacking)</td>
<td>Phishing (Social)</td>
<td>Stolen creds (Hacking)</td>
</tr>
<tr>
<td></td>
<td>Spyware (Malware)</td>
<td>Command/Control (C2)</td>
<td>Brute force (Hacking)</td>
</tr>
<tr>
<td></td>
<td>Capture stored data (Malware)</td>
<td>Export data (Malware)</td>
<td>RFI (Hacking)</td>
</tr>
<tr>
<td></td>
<td>Adminware (Malware)</td>
<td>Export data (Malware)</td>
<td>Backdoor (Malware)</td>
</tr>
<tr>
<td></td>
<td>RAM Scraper (Malware)</td>
<td>Password dumper (Malware)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloader (Malware)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stolen creds (Hacking)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMMON ACTIONS</th>
<th>ORGANIZED CRIME</th>
<th>STATE-AFFILIATED</th>
<th>ACTIVISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TARGETED ASSETS</td>
<td>ORGANIZED CRIME</td>
<td>STATE-AFFILIATED</td>
<td>ACTIVISTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>ATM</td>
<td>Laptop/desktop</td>
<td></td>
<td>Web application</td>
</tr>
<tr>
<td>POS controller</td>
<td>File server</td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td>POS terminal</td>
<td>Mail server</td>
<td></td>
<td>Mail server</td>
</tr>
<tr>
<td>Database</td>
<td>Directory server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DESIRED DATA</th>
<th>ORGANIZED CRIME</th>
<th>STATE-AFFILIATED</th>
<th>ACTIVISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment cards</td>
<td></td>
<td></td>
<td>Personal info</td>
</tr>
<tr>
<td>Credentials</td>
<td></td>
<td></td>
<td>Credentials</td>
</tr>
<tr>
<td>Bank account info</td>
<td></td>
<td></td>
<td>Internal organization data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trade secrets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>System info</td>
</tr>
</tbody>
</table>

*Source: Verizon 2013 Report*
Threat Actors’ Country of Origin

Source: Symantec, Verizon 2013 Report
Data Breach Methodologies: Social Media and Mobile
Social Media: Methodology

**Fake Plug-in Scams**

Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.

**Likejacking**

Using fake “Like” buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user’s newsfeed, spreading the attack.

**Fake Apps**

Applications provided by attackers that appear to be legitimate apps; however, they contain a malicious payload. The attackers often take legitimate apps, bundle malware with them, and then re-release it as a free version of the app.

**Manual Sharing Scams**

These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.

**Fake Offering**

These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

### Top Five Social Media Attacks

- **Fake Offering**: 82%
- **Likejacking**: 8%
- **Manual Sharing**: 5%
- **Comment Jacking**: 2%
- **Fake Apps**: 2%

Source: Symantec
Mobile: Malware by Type

- **Track User**: Risks that spy on the individual using the device, collecting SMS messages or phone call logs, tracking GPS coordinates, recording phone calls, or gathering pictures and video taken with the device.

- **Collect Data**: Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.

- **Adware/Annoyance**: Mobile risks that display advertising or generally perform actions to disrupt the user.

- **Send Content**: These risks will send text messages to premium SMS numbers, ultimately appearing on the bill of the device's owner. Other risks can be used to send spam messages.

- **Traditional Threats**: Threats that carry out traditional malware functions, such as back doors and downloaders.

- **Change Settings**: These types of risks attempt to elevate privileges or simply modify various settings within the operating system.

*Source: Symantec*
Best Practices
The attack can be disrupted at any point in the kill chain. Ideally, a company will have controls at each point to create a defense in depth strategy. “Cyber kill chain” model shows, cyber attacks can and do incorporate a broad range of malevolent actions, from spear phishing and espionage to malware and data exfiltration that may persist undetected for an indefinite period.
### Best Practices – Network Security

1. **Review firewall configurations and ensure that only allowed ports, services and Internet protocol (IP) addresses are communicating with your network.**

2. **Segregate payment processing networks from other networks.**

3. **Apply access control lists (ACLs) on the router configuration to limit unauthorized traffic to payment processing networks.**

4. **Create strict ACLs segmenting public-facing systems and back-end database systems that house payment card data.**

5. **Implement data leakage prevention/detection tools to detect and help prevent data ex-filtration.**

6. **Implement tools to detect anomalous network traffic and anomalous behavior by legitimate users (compromised credentials).**
Best Practices – Administrative Access

- Use two-factor authentication when accessing payment processing networks. Even if a virtual private network is used, it is important that 2FA is implemented to help mitigate key-logger or credential dumping attacks.

- Limit administrative privileges for users and applications.

- Periodically review systems (local and domain controllers) for unknown and dormant users.
Data Breach Incident Response
## The First 24 Hours Checklist

1. **Record the date and time** when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.

2. **Alert and activate everyone** on the response team, including external resources, to begin executing your preparedness plan.

3. **Secure the premises** around the area where the data breach occurred to help preserve evidence.

4. **Stop additional data loss.** Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.

5. **Document everything** known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.

6. **Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.

7. **Review protocols** regarding disseminating information about the breach for everyone involved in this early stage.

8. **Assess priorities and risks** based on what you know about the breach.

9. **Bring in your forensics firm** to begin an in-depth investigation.

10. **Notify law enforcement**, if needed, after consulting with legal counsel and upper management.

Source: Experian
What You Can Do Today
## What You Can Do Today

1. **Forensics analysis on sample of systems looking for malware and signs of intrusion**
   - If you are in retail, audit hosts for a rogue "POSWDS" service
   - Look for rogue applications in memory that may attempt to masquerade as svchost and/or other programs on terminals and servers
   - Look for a rogue data manager application on internal LAN servers

2. **Traffic analysis on sample of networks looking for suspicious traffic**
   - Audit networks for possible rogue PING messages that contain custom text messages
   - Look for unauthorized FTP exfiltration on Internet-accessible hosts/servers
   - Looks for Suspicious network traffic
What You Can Do **Today**

### Alignment to NIST, VISA, and Australian Signals Directorate best practices

At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies listed in their Strategies to Mitigate Targeted Cyber Intrusions:

- Use application whitelisting to help prevent malicious software and unapproved programs from running
- Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
- Patch operating system vulnerabilities
- Restrict administrative privileges to operating systems and applications based on user duties.

What You Can Do Today

Alignment to NIST, VISA, and BAMs best practices (Contd.)

- Logging and monitoring
  - Implement tools to detect anomalous network traffic and anomalous behavior by legitimate users (compromised credentials)
  - Offload logs to a dedicated server in a secure location where unauthorized users can’t tamper with them
  - Aggregates events and logs from network devices and applications
  - Uses intelligence to analyze and uncover malicious behavior on the network
- Network architecture – FW outbound restrictions
- Secure remote access
- Implement data leakage prevention/detection tools to detect and help prevent data exfiltration
- Incident Response Plans
  - Invest in a dedicated incident response team (IRT) that has the knowledge, training and certification to respond to a breach. For more information on IRT training, visit the SANS Institute website.
  - Test and document incident response plans to identify and remediate any gaps prior to an attack.
  - Plans should be updated periodically to address emerging threats.
  - Look at controls relative to Breach Kill Chain
Questions
Contact Us

Jeffery Sanchez
Managing Director
Los Angeles, CA

Phone: +1.213.327.1433
jeffrey.sanchez@protiviti.com

Powerful Insights. Proven Delivery.™