Data Breach Strikes - Nerds & Geeks Unite: Effective Cooperation Between Privacy and Technical Experts

Presented by:
Paul H. Luehr, Managing Dir.
Stroz Friedberg

Gerard M. Stegmaier, Esq.
Wilson Sonsini Goodrich & Rosati
2011 Average Loss to Organization = $5.5 million

- Down from $7.2 million in 2010
- Not including organizations in excess of 100,000
- Low of $566K, High of $20.9 million

2011 Average Loss per Victim = $194

- Cost per Malicious Attack = $222
- Cost per Negligent Employee = $174

2011 Malicious Attacks, up over 3x

- Up from 12% to 24% to 31% to 37% (2008-2011)

Source: Ponemon Institute/Symantec, 2011 U.S. Cost of a Data Breach Study (49 organizations across 14 sectors)
### Data Breach Trends

**Figure 10. Per capita cost differences for six attributes or conditions**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party flub</td>
<td>$26</td>
</tr>
<tr>
<td>Quick response</td>
<td>$33</td>
</tr>
<tr>
<td>Lost or stolen device</td>
<td>$22</td>
</tr>
<tr>
<td>First time</td>
<td>$37</td>
</tr>
<tr>
<td>External consulting support</td>
<td>$(41)</td>
</tr>
<tr>
<td>CISO leadership</td>
<td>$(80)</td>
</tr>
</tbody>
</table>

*Source: Ponemon Institute/Symantec, 2011 U.S. Cost of a Data Breach Study*
Data Breach Trends

**Figure 4. Per capita cost by industry classification of benchmarked companies**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Per Capita Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications</td>
<td>$334</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>$276</td>
</tr>
<tr>
<td>Financial</td>
<td>$247</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$240</td>
</tr>
<tr>
<td>Industrial</td>
<td>$235</td>
</tr>
<tr>
<td>Consumer</td>
<td>$203</td>
</tr>
<tr>
<td>Transportation</td>
<td>$196</td>
</tr>
<tr>
<td>Services</td>
<td>$185</td>
</tr>
<tr>
<td>Retail</td>
<td>$174</td>
</tr>
<tr>
<td>Education</td>
<td>$142</td>
</tr>
<tr>
<td>Technology</td>
<td>$134</td>
</tr>
<tr>
<td>Public</td>
<td>$134</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$116</td>
</tr>
<tr>
<td>Media</td>
<td>$89</td>
</tr>
</tbody>
</table>

Source: Ponemon Institute/Symantec, 2011 U.S. Cost of a Data Breach Study
96% of Health Companies Surveyed had a Breach
  • Average of 4 over past 2 years
  • 46% had more than 5 in past 2 years

$2.2 million = Average Financial Impact
  • Up 10% from 2010

Discovered through:
  Employees (55%), Audit (45%), Patients (35%)

Source: Ponemon Institute/ID Experts, 2nd Annual Benchmark Study on Patient Privacy and Data Security (2011)(72 organizations surveyed)
Responding to Data Breaches

PREPARE
PRESERVE
SEARCH
ASSESS
COMMUNICATE
PREPARE for Disaster

- Develop a Response Plan
- Organize your Network Data
- Build Your Team
PREPARE: Develop a Plan

- Management endorsement
- Contact Lists
- Legal Analysis and Timeline
- Categories of adverse events
- “First steps” checklist
- Facilities and equipment lists
- Outreach plan

Develop a Response Plan

Organize your Network Data
Build Your Team
PREPARE: Organize your Data

Map your critical assets
Record backup schedules and inventories
Update user lists
Centralize logging functions
Synchronize network times

“Where’s your stuff?”

Develop a Response Plan
Organize your Network Data
Build Your Team

© Stroz Friedberg, LLC 2012
PREPARE: Build your Team

Outside Counsel
Client and Media Relations
Human Resources
Business Unit
In-House Counsel
In-House IT
CPO, CSO Compliance
Outside Incident Response Experts

Develop a Response Plan
Organize your Network Data
Build Your Team
Data Breach – Types

Examples:

- **Hacking**
  - Phishing/spear phishing
  - Brute force attack
  - SQL injection
  - Advanced Persistent Threat (APT)

- **Data theft or loss**
  - Media stolen (e.g. laptops, thumb drives, tapes)
  - Data stolen (e.g. by current or former employee)
  - Data lost (e.g. in taxi or during data migration)

- **Data leakage**
  - Exposure to public (e.g. via web site)
  - Exposure to unauthorized person (e.g. wrong employee)
  - Sensitive data sent via unencrypted channel
Response Team (Internal Threat)

Counsel

IR Team Lead

CPO/CSO Lead

Evidence Team Lead

Forensic Analysis Team Lead

Physical Investigation Team Leader

- Hard drive, devices, volatile data preservation
- Log file & backup acquisition
- Media analysis
- Network log analysis
- Interviews & video/keycard/fingerprint collection
- Law enforcement liaison

© Stroz Friedberg, LLC 2012
- Unhook infected machines *(leave power on).*
  - Do **NOT** poke around.
  - Insert clean and patched machines.
- Call forensic experts to image infected machines.
- Save off log files *(e.g., web, firewall, IDS).*
- Pull needed backup(s) out of rotation.
- Save keycard data and surveillance tapes.
- Start real-time packet capture.
- Force password change.
Coordinating IT and Forensic Activity

- **IT needs to secure data environment**
  - Pull network connection, save backups and logs, prepare clean “builds,” force password change, update antivirus

- **Forensic needs to review active/latent data**
  - Image servers and report findings

Business Continuity

- Migrate data after forensic imaging
SEARCH and ASSESS – Internal Threats
Internet Activity

**Banking activity**
- http://www.google.com/search?source=ig&hl=en&rlz=&q=resignation letter examples&
- http://www.victorypharmacy.com
- https://online.wellsfargo.com
- http://webmail.aol.com
- http://www.facebook.com/login.php?email=jdoe@aol.com
- file:///O:/Projects/2010/Wind Leases/Pow... Lease2.doc
- http://embassysuites...US/es/hotel/MSBPRES...es-Minnea
- http://www.brothersoft...erase-deleted-files.html
- http://www.google.com/search?source=ig&hl=en&rlz=&q=erasing deleted files&aq=0&o
- javascript:onSubmitToolBarItemClicked(‘DeleteMessages’,”);

**Employment activity**
- Internal server access
- https://online.wellsfargo.com
- http://webmail.aol.com
- http://www.facebook.com/login.php?email=jdoe@aol.com

**Web access**
- (email, social media, cloud)

**Data deletions**
- http://www.google.com/search?source=ig&hl=en&rlz=&q=resignation letter examples&
- http://www.victorypharmacy.com
- https://online.wellsfargo.com
- http://webmail.aol.com
- http://www.facebook.com/login.php?email=jdoe@aol.com
- file:///O:/Projects/2010/Wind Leases/Pow... Lease2.doc
- http://embassysuites...US/es/hotel/MSBPRES...es-Minnea
- http://www.brothersoft...erase-deleted-files.html
- http://www.google.com/search?source=ig&hl=en&rlz=&q=erasing deleted files&aq=0&o
- javascript:onSubmitToolBarItemClicked(‘DeleteMessages’,”);
CD/DVD Burning

INSERT DISK

Please insert a CD/DVD

Target type: 
Target location: 
Target:

Start in:
Shortcut key: None
Run: Normal window
Comment:

For Help, press F1

© Stroz Friedberg, LLC 2012
Removable Devices
A Link file shows this document was accessed on a particular date and time...

And where the file was located when accessed.
### Deletion and Wiping Activity

| 000000210 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000220 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000230 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000240 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000250 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000260 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000270 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000280 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000290 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 0000002a0 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 0000002b0 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 0000002c0 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 0000002d0 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 0000002e0 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 0000002f0 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000300 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000310 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000320 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000330 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000340 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000350 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000360 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000370 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000380 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
| 000000390 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ................................................ |
Spear Phishing

From: johnsmith985@yahoo.com
To: Joyce.associate@lawfirm.com
Subject: Please read the attachment for tomorrow’s meeting.

Attachment: one document
Dear Joyce,

Please excuse the personal email address, I’m working from home and I can’t get access to the network.

Can you please open the attached document and review for tomorrow’s meeting.

Many thanks,

John
 Analyze log files.
 Review memory/virtual memory.
 Analyze hard drives.
 Analyze and reverse malware code.
 Review live traffic captures.
 Run behavioral profiling.
### Deleted Files: Hacker’s Toolkit

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>EraseLog.vbs</td>
<td>VBScript Script File</td>
<td>1,109</td>
</tr>
<tr>
<td>FindPass.exe</td>
<td>Application</td>
<td>17,408</td>
</tr>
<tr>
<td>Letmein.exe</td>
<td>Application</td>
<td>18,432</td>
</tr>
<tr>
<td>ListAdmins.vbs</td>
<td>VBScript Script File</td>
<td>1,213</td>
</tr>
<tr>
<td>Netsvc.exe</td>
<td>Application</td>
<td>14,336</td>
</tr>
<tr>
<td>NETVIEWX.EXE</td>
<td>Application</td>
<td>40,960</td>
</tr>
<tr>
<td>Pseexec.exe</td>
<td>Application</td>
<td>90,112</td>
</tr>
<tr>
<td>PsKill.exe</td>
<td>Application</td>
<td>26,624</td>
</tr>
<tr>
<td>Psloggedon.exe</td>
<td>Application</td>
<td>45,056</td>
</tr>
<tr>
<td>pspassword.exe</td>
<td>Application</td>
<td>57,344</td>
</tr>
<tr>
<td>Pulist.exe</td>
<td>Application</td>
<td>55,296</td>
</tr>
<tr>
<td>rasmon.dll</td>
<td>Application Extension</td>
<td>4,608</td>
</tr>
<tr>
<td>rasmon.exe</td>
<td>Application</td>
<td>16,384</td>
</tr>
<tr>
<td>Sqlcmd.asp</td>
<td>ASP File</td>
<td>4,004</td>
</tr>
</tbody>
</table>
Volatile Data Capture

Capturing physical memory may reveal processes not normally seen by user or IT.

<table>
<thead>
<tr>
<th>Proc#</th>
<th>PPID</th>
<th>PID</th>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Idle</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>8</td>
<td>System</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>156</td>
<td>smss.exe</td>
</tr>
<tr>
<td>3</td>
<td>144</td>
<td>164</td>
<td>winlogon.exe</td>
</tr>
<tr>
<td>4</td>
<td>144</td>
<td>168</td>
<td>csrss.exe</td>
</tr>
<tr>
<td>5</td>
<td>156</td>
<td>176</td>
<td>winlogon.exe</td>
</tr>
<tr>
<td>6</td>
<td>156</td>
<td>176</td>
<td>winlogon.exe</td>
</tr>
<tr>
<td>7</td>
<td>156</td>
<td>180</td>
<td>csrss.exe</td>
</tr>
<tr>
<td>8</td>
<td>176</td>
<td>228</td>
<td>services.exe</td>
</tr>
<tr>
<td>9</td>
<td>176</td>
<td>240</td>
<td>lsass.exe</td>
</tr>
<tr>
<td>10</td>
<td>1112</td>
<td>284</td>
<td>dd.exe</td>
</tr>
<tr>
<td>11</td>
<td>820</td>
<td>324</td>
<td>helix.exe</td>
</tr>
<tr>
<td>12</td>
<td>228</td>
<td>408</td>
<td>svchost.exe</td>
</tr>
<tr>
<td>13</td>
<td>228</td>
<td>436</td>
<td>spoolsv.exe</td>
</tr>
<tr>
<td>14</td>
<td>228</td>
<td>464</td>
<td>Avsynmgr.exe</td>
</tr>
<tr>
<td>15</td>
<td>228</td>
<td>480</td>
<td>svchost.exe</td>
</tr>
<tr>
<td>16</td>
<td>228</td>
<td>540</td>
<td>regsvc.exe</td>
</tr>
<tr>
<td>17</td>
<td>228</td>
<td>552</td>
<td>MSTask.exe</td>
</tr>
<tr>
<td>18</td>
<td>228</td>
<td>592</td>
<td>dfrws2005.exe</td>
</tr>
<tr>
<td>19</td>
<td>464</td>
<td>612</td>
<td>VsStat.exe</td>
</tr>
<tr>
<td>20</td>
<td>464</td>
<td>628</td>
<td>Avconsol.exe</td>
</tr>
<tr>
<td>21</td>
<td>600</td>
<td>668</td>
<td>UMGR32.EXE</td>
</tr>
<tr>
<td>22</td>
<td>228</td>
<td>672</td>
<td>WinMgmt.exe</td>
</tr>
<tr>
<td>23</td>
<td>800</td>
<td>820</td>
<td>Explorer.exe</td>
</tr>
<tr>
<td>24</td>
<td>820</td>
<td>964</td>
<td>Apoint.exe</td>
</tr>
<tr>
<td>25</td>
<td>820</td>
<td>972</td>
<td>HKserv.exe</td>
</tr>
<tr>
<td>26</td>
<td>820</td>
<td>972</td>
<td>HKserv.exe</td>
</tr>
<tr>
<td>27</td>
<td>820</td>
<td>988</td>
<td>DragDrop.exe</td>
</tr>
<tr>
<td>28</td>
<td>820</td>
<td>1008</td>
<td>alogserv.exe</td>
</tr>
<tr>
<td>29</td>
<td>820</td>
<td>1012</td>
<td>tgcmd.exe</td>
</tr>
<tr>
<td>30</td>
<td>820</td>
<td>1048</td>
<td>PcfMgr.exe</td>
</tr>
<tr>
<td>31</td>
<td>408</td>
<td>1064</td>
<td>JogServ2.exe</td>
</tr>
<tr>
<td>32</td>
<td>864</td>
<td>1072</td>
<td>Apltex.exe</td>
</tr>
<tr>
<td>33</td>
<td>820</td>
<td>1076</td>
<td>cmd.exe</td>
</tr>
<tr>
<td>34</td>
<td>592</td>
<td>1096</td>
<td>nc.exe</td>
</tr>
<tr>
<td>35</td>
<td>324</td>
<td>1112</td>
<td>cmd2k.exe</td>
</tr>
</tbody>
</table>
Malware Review
SEARCH and ASSESS – Challenges

Timing

- Estimate per Server
  - Initial Breach Analysis = 7 to 10 days
  - Identification of PII or PHI = 2 to 30 days
  (structured DB v. unstructured xls, doc, pdf, txt, jpg)

Desire for Certainty

- Regulators
- Consumers
- Company Officers/Managers
SEARCH and ASSESS – Challenges

Investigation Paradox

- More careful analysis takes time
- More careful analysis increases certainty
  - Can locate lost/stolen data
  - Can account for malware changes, attacking IP’s
  - Can run scans across entire network
  - Can better account for PII and PHI sources
- More careful analysis reduces cost
- 2010 Ponemon Findings:
  - Quick Responder* Cost = $268 per record
  - Later Responder Cost = $174 per record

*notification within 30 days

© Stroz Friedberg, LLC 2012
SEARCH and ASSESS – Challenges

PII, PHI Variations:

- **Social security number:**
  
  ```
  === - == - ====, === == ====, ==========
  “SSN, Social Security Number, socsec,” etc.
  ```

- **Account number:**

  5411222233334444 = 5.41122E+15 in scientific notation

- **Unsearchables:**

  ```
  SSN  000-00-1234
  SSN  000-00-5678
  ```
Breach Response – a Dynamic Process

BREACH DEFINITIONS
Did an unauthorized party:
- Access*
- Acquire
- Misuse
- Disclose PII/PHI

Does investigation show:
- Material compromise
- Actual loss or injury to consumer
- Material risk of ID theft or fraud
- Significant risk of financial, reputational, other harm*
Internal Stakeholders

- Team Members – Counsel, Compliance, HR, IT, Business Managers, Public Affairs, Experts
- Board/CEO, Executives
- Employees
- Shareholders
- Customers
Notification Clock

- When did earliest/original breach occur?
- What is the notification due date?
- When will we “know” whether we need to notify?

Reporting Formats

- What are the needs of the response team?
- What does IT, Board, counsel need to know?
- Should reports be oral or written?
- What is covered by privilege?
Best Practices

- Assemble response team immediately
- Discourage blame, data hoarding, and avoidance
- Communicate often, but not constantly
- Coordinate investigative findings across teams
- Limit strategic discussions to key managers & counsel
RESOURCES

HHS Health Information Privacy - www.hhs.gov/ocr/privacy

NIST Computer Security Resource Ctr – csrc.nist.gov

State Data Breach Laws – www.ncsl.org

FTC Privacy Actions – www.ftc.gov/privacy

Privacy Rights – www.privacyrights.org

Open Security Foundation, Data Loss DB – datalossdb.org
QUESTIONS?

Paul H. Luehr
Managing Director, CPO
Stroz Friedberg

720 Northstar Center West
625 Marquette Ave South
Minneapolis, MN 55402

612.605-3007 direct
pluehr@strozfriedberg.com

Gerard M. Stegmaier, Esq.
Wilson Sonsini Goodrich & Rosati, P.C.

1700 K Street, NW
Fifth Floor
Washington, DC 20006-3817

202-973-8809 direct
gstegmaier@wsgr.com