When Business Process & Incident Response Collide

The Fine Tuning of the Incident Response Program

Reneaué Railton
Sr. Information Security Analyst,
Duke Medicine Cyber Defense & Response
Incident Response

What is the most importance component of an Incident Response Program?

Tools? Processes?
Governance? Policy?
Experience?
Risks to the Organization

- Poor user practices (phishing and insecure data storage)
- Inconsistent security practices (adherence to policy i.e., exceptions, patching)
- Failure to detect attacks (ineffective tools, lack of experience)
- Sprawl and amount of data (mobile, remote users, cloud services)
Risks lead to Incidents…
A Breach is imminent!

Our attack surface is increasing!

We're loosing visibility!

My controls aren't working!!

A Breach is imminent!
World’s Largest Data Breaches

Breaches by data sensitivity

Breaches by number of records stolen

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
<table>
<thead>
<tr>
<th>Totals for Category</th>
<th># of Breaches</th>
<th># of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking/Credit/Financial</td>
<td>30</td>
<td>403,531</td>
</tr>
<tr>
<td>Business</td>
<td>128</td>
<td>110,407</td>
</tr>
<tr>
<td>Educational</td>
<td>27</td>
<td>572,692</td>
</tr>
<tr>
<td>Government/Military</td>
<td>23</td>
<td>1,330,500</td>
</tr>
<tr>
<td>Medical/Healthcare</td>
<td>121</td>
<td>100,923,435</td>
</tr>
</tbody>
</table>

**Totals for All Categories:**

- # of Breaches: 329
- # of Records: 103,340,565
- % of Breaches: 100.0
- % of Records: 100.0

Identity Theft Resource Center

2015 Data Breach Category Summary
Report Date: 6/2/2015

Ponemon 2015 Benchmark Study on Privacy & Security of Healthcare Data

• 90% of Healthcare organizations in the study experienced a breach
• 40% had 5 or more data breaches over 2 years
• Estimated average cost of healthcare breach over $2.1 million
• Criminal attacks are the #1 cause of data breaches in Healthcare
• Attacks are up 125% compared to 5 years ago
Threats

What can we do?

• We’re under attack right now!
• Attackers are winning!
• It’s getting worse!

Hospital Medical Devices Used As Weapons In Cyberattacks

Criminal attacks in healthcare are up 125% since 2010

The healthcare industry is experiencing a surge in data breaches, security incidents, and criminal attacks—exposing millions of patients and their medical records, according to the Ponemon Institute.

Dark Reading, Posted June 8, 2015
What is our current focus?

**Compromised Accounts**
- Log Analysis with Splunk

**Vulnerable Systems**
- Vulnerability scanning and remediation

**Compromised Systems**
- Log analysis and network data

**Sensitive Data**
- Data loss prevention technologies and policy
Scaling the Response?

- Incident Response Program needs to be 24/7
- Automation only works on “known quantities”
- How do we make the argument for better tools or more resources?
Who Provides the Response?

Organizational CSIRT
- Costs to own and maintain equipment
- Salary & Benefits
- Training
- Localized, Site specific

Pros
- Understanding of network environment
- Reports are unique to situation

Outside Security Service
- Equipment provided and maintained by third party
- Data and Intelligence aggregation across multiple customers
- Identifies Priority events

Cons:
- Canned Responses
- Intel provided may not be site specific
Cisco MTD
Duke Medicine statistics 03/08 – 03/31

03/08-03/14 97,539 Security Events
03/15-03/21 135,515 Security Events
I don't see why I need MFA.

You've got Mail!

Oh No! My email account will be deleted unless I validate my account now!

My paycheck was deposited where?!

A virus encrypted my files and I don't have a backup!

CryptoWall ???

I guess that's one way to get user's to comply with data encryption policies!

Case Study
Email Attacks

Systems processed > 4.7M emails per day at peak; 4.5M malicious emails were deleted each day (>3000/minute)

Of 146M emails received in January only about 13% were legitimate (5% were spam, 82% were viruses, phishing, and other malware)
The Phish

• November, 2013: Phishing email sent to 380 users with the subject “Duke Alert” asking them to confirm login details.
• Link lead to Fake Duke Login Page:

• December, 2013: Employees who had fell for the Phish noticed their paychecks were not deposited on payday – two days before Christmas.
• Investigation found that direct deposits for these employees had been routed to a foreign banking institution in Mauritius.
Who bears the loss?

• The organization who owns the application that was accessed?
• The user who provided their credentials to the criminal.

Employees are paid monthly. If an employee makes 60K/year, that is $5,000 – taxes & insurance. If take home pay is $4000 x 6 employees the loss is minimal at $24000. But what if 100 employees had been affected? 1000?
Phishing Attack

Duke Security Controls

Protective Measures:
- Roll-out of MFA
- Auto-lock compromised accounts
- Any compromised account is required to enroll in MFA
- User Awareness & Training
- Free Software made available (Endpoint Protection, Lastpass, MFA)

Detective Measures:
- Monitor user logins from multiple locations
- Monitor multiple logins from a single external source
- Seed Phishing site with fake UserID, monitor for intel

Fake NetID
Did it Work?

Phishing attacks continue after new security measures implemented
Faculty, staff encouraged to enroll in multi-factor authentication service
MONDAY, MARCH 17, 2014

They're BACK! (and they're looking to pilfer your paycheck)
by Stephen O'Donnell on 7/21/2014 10:15 AM

Once again, our IT security login credentials for the phishing email promising other universities over the

Direct deposit phishing attacks continue 1 year later
This month marks the one-year anniversary of the start of a series of phishing attacks aimed at stealing the paycheck of Duke faculty and staff. From November 2013 through March 2014, attackers sent three messages asking Duke employees to provide their usernames and passwords. Several employees' paychecks were diverted to bank accounts controlled by the attackers. Duke was not the only target. According to REN-ISAC, a national group that promotes cybersecurity in research and higher education:
The message went to 617 people.

9 people fell for the message
Weighing the Costs

Before the Incident

• IR Tools
• Trained, experienced staff
• Regular Risk Assessment and Audits

After the Incident

• Third-party Consultants and Investigative Teams
• Technical & Awareness Training
• Recovery/Replacement of damaged assets
Indirect Costs

**Intangible Costs**
- Damage to Corporate Brand or reputation
- Loss of future customers/clients/investors

**Tangible Costs**
- Regulatory fines
- Loss of Revenue (Sales, productivity, etc.)
- Legal fees
- Identity Protection Services
Security Focus Areas

- Network Security
- System Security
- End User & Account Protection
- Logging & Analysis
- Risk & Governance
Security Defenses and Techniques: Network Security

- NGFW
- VRF Technology
- IPS/IDS utilizing CIF
- Managed Security Services & Threat Defense
Security Defenses and Techniques: Systems Security

- Automated Patching (IEM)
- Data Loss Prevention (DLP)
- Mobile Device Management
- Web Application Security
- Reduced Administrative Rights
Security Defenses and Techniques: End User and Account Protection

• Whole Disk Encryption
• Spam Filtering
• Endpoint Protection – it’s not just Anti-virus anymore
• Identity and Access Mgt (IAM)
• Secure Sign On Service
• Multifactor authentication (MFA)
• Password Escrow
Security Defenses and Techniques: The Incident Response Toolbag

- Security Information & Event Management (SIEM)
- Threat & Intel Feeds
- NetFlow Analysis
- Log Correlation and Analysis
- Forensics
- Open Source Toolkits
Security Defenses and Techniques: Risk & Governance

- Risk assessments, vulnerability scanning & penetration testing
- Compliance audits
- Policy updates
- Awareness, training and outreach