Plan of Attack | 5 Step Plan

- Naming those Digital Assets
- Practicing Digital Doomsday
- Training + Policies and Procedures
- Technology Tuning
- Security in the Supply Chain
### Next Steps | Sample Plan

<table>
<thead>
<tr>
<th>0 to 30 Days</th>
<th>30 to 90 Days</th>
<th>90+ Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Name your top 2 digital assets</td>
<td>- Update policies and procedures</td>
<td>- Establish a Cross Functional Security Council</td>
</tr>
<tr>
<td>- Implement Incident Response Framework</td>
<td>- Employee &amp; vendor education and awareness programs</td>
<td>- Work with Legal to discuss your data privacy and security standards</td>
</tr>
<tr>
<td>- Practice a Digital Disaster</td>
<td>- Acceptable use agreements (signed / dated)</td>
<td>- Work with your Insurance company to plan out the coverages you need for cyber liability</td>
</tr>
<tr>
<td></td>
<td>- Targeted assessments focused specifically on the top 2 digital assets</td>
<td></td>
</tr>
</tbody>
</table>
Name Those Critical Digital Assets

Executives Want to Know

What’s coming?
How will we know?
What does being prepared look like?
What’s our exposure?

Threat Awareness

Can YOU answer who, what, when, why – Who understands your exposure?

“We Have a Security Program…”

Approach

9 out of 10 employees admit they...break policy

- Threat Testing
- People & Process
- Open Source Intelligence
- Legal & Insurance Advice
Next Steps | Actions

Basics
• Top Digital Assets – What are they?
• Implement Awareness Training
• Policies and Procedures
• Patches for Operating systems
• Encryption of emails
• Encryption of data
Next Phase

• Those 5 Tech Trends and Your Top 2 Digital Assets – How do you protect those digital assets?
• Incident Management
• Disaster Recovery
• Digital Disaster
• Technology Tuning
• Supply Chain Review
Name Those Critical Digital Assets

From an industry perspective, there are two key tenants that must be understood:

1. Some organizations will be a target regardless of what they do but most become a target because of what they do.

2. Understand as much as you can about what your opponent is likely to do and how far they are willing to go.

Source: USSS and Verizon Data Breach Investigations Report 2013
Back at the Office | Next Steps
Name Those Critical Digital Assets

Commit Today

- Name your “POTUS and VP” of digital assets
- Practice a digital disaster
Here’s your next staff meeting agenda

**Current State Assessment – Spend Dedicated Time Discussing:**
- What security measures are in place? What do they protect?
- How vulnerable are you? How vulnerable are your clients?
- What client communication and response plans exist?
- Do you test incident management plans using plausible scenarios?

**Options Analysis**
- What could be done within the next 90 days to improve security?
- How would your company respond to losing intellectual property, internal emails posted on a public website, or worse?
- How can each security layer be enhanced, at what cost and at what impact to productivity?
Evolve Your Data Protection Strategy

- Think of your most valuable clients and digital assets
- There is no 100% method to avoid being hacked so the design needs to ask:
  - Can we store that sensitive & important data in different places?
  - Can we treat each element within the asset with different levels of access and protection?
  - Will we know if the data is being watched, touched, moved, copied?
Got Credit Cards?

• You Need Strict network segmentation – block off that PCI card data AND add two-factor authentication for access to the PCI environment.
• Tighten Up Privileged accounts: Very few people or systems should access PCI. Create several layers of access and DIFFERENT passwords
• Got Vendors? Lock off those endpoints! If you must have an active connection add additional behavioral monitoring and endpoint threat detection.
• Who Watches the Watchmen? Baseline activity and have alerts trigger when activity goes outside the norm. Monitor the monitoring systems to make sure any alarms or alerts are not being ignored
Got Credit Cards?

Pre PCI DSS Audit – Prep Questions

• Where do our PCI assets AND PCI relevant assets live? How are they created, transported, copied, and configured? What walls do we have around them?
• Who (people and systems) can touch them? Can we limit that access? Can we turn off the access? How do we monitor when the PCI assets and PCI relevant assets are accessed?
• What are the current systems vulnerabilities?
• What is our network and data traffic baseline? Do we know what “normal” looks like?
Got Credit Cards?

Penetration Test Methodology Changes

• NIST SP 800 – 115
• EVERYTHING you did in the past AND …
  – Test entire perimeter of CDE and all critical systems (have you defined critical?)
  – Validate all of the segmentation, user access controls and scope reduction controls
  – Test inside AND outside the network
  – Test all network components and the operating systems
Practicing Digital Doomsday

Naming Your Top Digital Assets

• List the 1-3 assets that, if compromised, your company would cease to exist:
Digital Disaster | Data Handling

Staff Meeting - Practice the Disaster
Name Your Worst Digital Nightmare:

• Digital death, what happened?
• Go around the room and ask the team to tell you the escalation plan and their list of actions.
• Do you know who to call? Do you know what to do?
• How do you stop the bad guys from taking more?
• Do you need outside help?
• Time yourself...how long does it take before you create a plan of action?
Training | Data Handling

Analysis: Industry Findings
Policies, Procedures, and Training is Key

87%
The percentage of breaches that could have been avoided through reasonable security controls

60%
The percentage of incidents where a policy was in place that would have prevented a breach but was not followed and a breach occurred

Teach Employees to Question

Do I really need to download this data?

If I email this data, is it secure?

If I put this data on a CD/DVD, thumb drive, or laptop how will I protect it?

Do I know how to dispose of the data safely when I don’t need it anymore?
Training | Data Handling

4 TIPS TO REMEMBER

- Timeout feature
- Password protect
- Treat old devices and back up information like gold
- Never loan devices or WiFi
Training - 80/20 Rule
2 Steps = Biggest Impact

• **Best Practices & Improved Security Policies**
  - 58%

• **Informed, Aware & Engaged Employees**
  - 20%

• **Technology Improvements**
  - 18%

• **Gov’t Regulation & Law Enforcement**
  - 4%

2012 Bit9 Cyber Security Research Report
Can you access more important assets on BYOD?

70% of the workforce that owns a personal smartphone ... accesses corporate data

AND...80% of those personally owned devices on the corporate networks are... inadequately managed by IT Departments
Training | Data Handling

• Vendors
  – Annual Requirement: Security training
  – Annual Requirement: Acceptable Use Policy; Confidentiality; Privacy and other agreements signed

• Your Staff
  – New Hires (same 2 bullets above) and...
  – Reminders – emails and staff meetings
  – Annual Refreshers
Training | Data Handling

- Posters
- Newsletters
- YouTube videos
- Play security games on websites
- E-mails
- Display Tables
- Contests
- “Mystery Shopping”
Human errors and systems glitches caused nearly $\frac{2}{3}$ of data breaches globally in 2012...

*2013 Cost of a Data Breach: Global Analysis*, Ponemon Institute and Symantec, June 2013
Too Much Data = Attractive Target
Total number of records containing sensitive personal information involved in security breaches in the United States is 608,087,870 in 3,763 data breaches since January 2005.

*A Chronology of Data Breaches*, Privacy Rights Clearinghouse, June 2013
Laptop encryption does help

The average value of a lost laptop is $49,246 and the data breach costs represent 80 percent of the total cost of a lost laptop compared to two percent for replacing the computer. Encryption on average can reduce the cost of a lost laptop by more than $20,000.

The Billion Dollar Lost Laptop Study, Ponemon Institute and Intel Corp., December 2010
Next Steps | Training

5 Things…

• Training – just say NO to CBT only
• Document IT AND End User policies and procedures
• Where will your team get stuck during the digital doomsday exercise?
• 90% of our clients last year had the core technology they needed but…it was not tuned to the top digital assets
• Not sure where to start for training? Try internet safety games at OnGuardOnline.gov
Next Steps | Cloud in your future?

Draw up the Pre-Nup First!

- When you “break up” what are their sanitization policies so you get your data back and they don’t have your digital footprints?

Need a “Go to guide”? Try NIST:
NIST Cloud Computing Reference Architecture SP 500-292
Cloud?

Start with these questions:
1. What is your data encryption strategy and how is it implemented?
2. What is the infrastructure patching schedule?
3. What is the drive-wiping standard?
4. Describe the endpoint security
5. During a breach, how do you isolate and safeguard our data from other customers?
6. How is user access monitored, modified and documented?
7. Are you in compliance with my company’s required regulatory requirements – for example - PCI, HIPAA, SOX, SSAE16?
8. What is your resiliency, reliability, back-up and disaster recovery strategy?
9. If there is a subpoena for data on your cloud, how do you ensure that legal actions taken will not affect the privacy of our data?
Next Steps  |  Vendor Guidelines

Supply Chain Security – 8 Vendor Checkpoints

• Information Security
• Identity Management
• Endpoint and Server Security
• Gateway and Network Security
• Web and Application Security
• Physical and Personnel Security
• Security Management
• Intellectual Property, Customer Information, and Financial Transaction Security
Next Steps | Vendor Guidelines

Supply Chain Security – Vendor Must Answer:
• Chain of Custody
• Least Privilege Access
• Separation of Duties
• Tamper Resistance and Evidence
• Persistent
• Compliance Management
• Code Testing and Verification
• Trusted and Vetted Staff
“A partner’s lax security practices and poor governance – often outside the victim’s control or expertise – are frequently catalysts in security incidents.”

Verizon 2012 Data Breach Investigations Report
Hidden Risks of Outsourcing

- Almost all companies outsource some component of their Data/Information management to third parties, but most companies have not measured the risks associated therewith. Companies use third parties for everything from web hosting to payroll outsourcing to credit card processing.
- For the last 3 years, Verizon has observed in its annual study findings that there has been a steady increase in the proportion of externally-hosted and/or externally managed data assets involved in privacy breaches.
- Outsourcing function = Loss of Control, but does NOT release the “data owner” from liability for privacy violations/breaches.
- FTC Act, Dodd-Frank, Red Flags Rule, PCI Compliance, NERC CIP, HIPAA/HITECH, and many other state and federal regulations extend to not only you but the vendors you use as well, putting the responsibility for compliance (and the reputation risk) squarely on your shoulders.
  - FTC Act gives broad ranging authority around “unfair or deceptive trade practices” regarding use of vendors, enforcement of appropriate privacy and security policies.
- Outsourcing can greatly increase your “contingent” business interruption risk.
Next Steps | Vendor Guidelines

Hidden Risks of Outsourcing

- **Ask Your Technology Team Or Outside Experts to:**
  - Analyze your top 2 critical digital assets
  - Identity the protection strategies around those assets
  - Fine tune existing technology to protect those assets
  - Develop end user and vendor management awareness programs targeted at protecting those assets
  - Assist in the categorization of vendors and redevelopment of contract protocols
  - Review insurance for cyber and/or E&O provided by those vendors for adequacy
  - Design custom insurance solutions for you and your vendors
Next Steps | Resources

Free internet safety games:  OnGuardOnline.gov

NIST Cloud Computing Reference:  Architecture SP 500-293

ODNI's document on foreign spies stealing U.S. information:

Carnegie Mellon's Insider Threat team's Common Sense Guide to Mitigating Insider Threats

OMB's (104-pages) guidance on mobile phone security controls

Ponemon's Cost of Cybercrime study:

USSS and Verizon Data Breach Investigation report:
http://www.verizonenterprise.com/DBIR/2013/

Mandiant's cyber security trends (fill out info form and then you can download report):
http://connect.mandiant.com/mtrends2013-eml

Free security training resources, including webcasts, are available at the Multi-State ISAC website:
http://msisac.cisecurity.org/resources/videos/free-training.cfm
Next Steps | Resources

Training - Data Handling

Free Training Resources:

• Social Networking

• Phishing
Next Steps | Resources
Training - Data Handling

Free Training Resources:

• National Security Briefing (NISPOM)
  – http://www.youtube.com/watch?v=UP01b84U0qY

• Wireless Security

• Spyware
  – http://onguardonline.gov/media/game-0002-beware-spyware
New Book!

Reviewed on Jon Stewart’s “Daily Show” January 21, 2014
Let’s keep the conversation going…

Are you naked online?
PROTECTING YOUR INTERNET IDENTITY

Ted Claypoole & Theresa Payton
Foreword by Chris Swecker, Former FBI Agent

tp@fortalicesolutions.com
@FortaliceLLC
Fortalice-LLC
877.487.8160

Offices: Charlotte & Greater Metro MD/VA/DC area