More Bang for Your Buck: Maximizing Cyber Security
With a Minimal Budget

Monday, September 28, 2015

Deena Coffman
CEO
IDT911 Consulting
New York, N.Y.

Deena Coffman has more than 20 years of experience working with technology and data management programs in law firms, corporate law departments, and major consulting firms. She has provided guidance to clients that are adopting technology or building programs related to data privacy, data security, operational risk, and electronic discovery.

Deena is a former chief operating officer of Kroll Cyber Security and Information Assurance. She also managed international projects with the analytical and forensic technology group at Deloitte Financial Advisory Services. She held global responsibility as the discovery director for Johnson & Johnson.

Her educational background includes an MBA from Cornell University’s S.C. Johnson Graduate School of Management, an MBA from Queen’s University in Ontario, Canada, and a Bachelor of Arts in management from the University of Illinois. She also maintains certification as a CIPP, MCSE, and MCP+I.
Three Session Ideas
Tools or tips you learned from this session and can apply back at the office.

1. _____________________________________________________________

2. _____________________________________________________________

3. _____________________________________________________________
More Bang for Your Buck: Maximizing Cyber Security with a Minimal Budget

Deena Coffman

September 28, 2015
Information security doesn’t have to be expensive or burdensome.

I did not say it was easy.

What’s a CEO to DO?!

A lack of reliable estimates leads to a creative environment for decision making where:

- Under spending
- Overspending, and
- Useless spending invariably result.

Regrettably, there is a large and glaring Gap in the security industry when it comes to quantifying losses.

2015 Verizon Data Breach Investigation Report
No More “Security by Obscurity”

The Washington Post

Here’s what you find when you scan the entire Internet in an hour

ZMap Scans the Entire Internet in Under 45 Minutes

By Timothy Lee August 18, 2015 Follow @timothee

Until recently, scanning the entire Internet, with its billions of unique addresses, was a slow and labor-intensive process. For example, in 2010 the Electronic Frontier Foundation conducted a scan to gather data on the use of encryption online. The process took two to three months.

A team of researchers at the University of Michigan believed they could do better. A lot better. On Friday, at the Chaos security conference in Washington, they announced ZMap, a tool that allows an ordinary server to scan every address on the Internet in just 44 minutes.

Google for Hackers

SHODAN FINDS COMPUTERS

FROM WEB SERVERS TO INDUSTRIAL CONTROL SYSTEMS TO REFRIGERATORS AND ANYTHING ELSE CONNECTED TO THE INTERNET.

FREE SIGN UP

Or login using Google Twitter Facebook

© IDT911 Consulting, LLC. All Rights Reserved — Confidential
KH1  Added screenshot of youtube video
Kevan Humphrey, 7/28/2015
Low Hanging Fruit

- **75%** of victims were targets of opportunity
- **78%** of attacks were considered in the low to very low ‘difficulty level’
- **76%** of network intrusions exploited weak or stolen credentials

Source: Verizon, 2013 Data Breach Investigations Report

9 Steps to Improve Your Security on a Limited Budget

1. Sensitive data discovery
2. Policies and procedures
3. Training and awareness
4. Secure configurations and regular patching
5. Encryption
6. Incident response planning
7. Backup/recovery measures
8. Limited use of administrator accounts
9. Separation of duties, including third-party audits
What We’ll Cover Today

1. **Take Stock**: Sensitive Data Discovery — Know Where Your Assets (or Liabilities) Exist
2. **Policies and Procedures**: Handle the Assets Properly
3. **Training and Awareness**: Engaging Your Employees In Your Defense
4. **Secure Configurations and Regular Patching**: Keeping Up With the Joneses
5. **Encryption**: It is neither expensive nor difficult, despite rumors to the contrary
6. **Incident Response Planning**: You Wouldn’t Be Caught Without a Fire Safety Plan
7. **Backup and Recovery Measures**: Back to Basics
8. **Limited Use of Administrator Accounts**: Guard The Master Key
9. **Separation of Duties**: This means third-party audits
Take Stock

78% of breaches could have been avoided with:

• IT best practices
• Improved security policies and
• Better informed, engaged employees

- 2012 Bit9 Cyber Security Research Report

Non-Hacker Data Breach Events

• Mis-mailing (including email and fax)
• Erroneous posting of information onto the Internet
  – FTP server is indexed by Google
  – Old server with PII put into service with IIS enabled
  – Erroneous Web posting by Webmaster or employee using Dropbox, Box, GitHub, etc.
• Data theft by either an employee or a non-employee
  – Disgruntled or financially motivated employee with access to personnel records
• Stolen or lost laptop, portable drive, USB or smartphone
Non-Hacker Data Breach Events

Unsecure disposal of records (files, old computers, network printers)

- **Dumpster rather than shredder** (including electronic media)
- **End of lease return of equipment** containing electronic PII
- **Computer equipment sold** on eBay or donated

Information Asset Inventory

- **What is your sensitive data?**
  - PHI, PCI, PII, IP
- **Consider laws and contracts**
  - State, Federal, Intl PCI
- **Intake channels**
  - eMail
  - Internet
  - Walkup
- **Usage and Storage**
  - Transfer
  - Access
  - Storage
  - Retention
Risk Assessment

What are the internal and external threats?

What mitigation measures exist?

What audit is in place?

What risk transfer is needed? (Insurance)

---

“...lesson learned recently by Cogent Healthcare, based in Brentwood, TN, after a mistake by a contractor led to a possible breach of 32,000 patients' protected health information. The vendor, India-based M2ComSys, was hired to transcribe care notes dictated by doctors. The firm stored those notes on what was supposed to be a secure website. However, the information remained publicly accessible because M2ComSys failed to activate a firewall.
Policies and Procedures
Handle the Assets Properly

Ponemon 2015 State of Endpoint Risk

Figure 1. What are the biggest threats to endpoint security in your organization?
Five choices permitted:

- Negligent or careless employees who do not follow security policies: 78%
- There are more personal devices connected to the network (BYOD): 60%
- Employees’ use of commercial cloud applications in the workplace: 60%
- The number of employees and others using multiple mobile devices in the workplace has increased: 50%
- The number of insecure mobile devices used in the workplace has increased significantly: 45%
- Malware infections are more stealthy and difficult to detect: 32%
- More employees are working offsite and using insecure Wi-Fi connections: 16%

* FY 2014 * FY 2013
* This response was not available in all fiscal years
Policies and Procedures

Figure 1. What are the biggest threats to endpoint security in your organization?

<table>
<thead>
<tr>
<th>Threat</th>
<th>FY 2014</th>
<th>FY 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligent or careless employees who do not follow security policies</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>There are more personal devices connected to the network (BYOD)</td>
<td>68%</td>
<td>60%</td>
</tr>
<tr>
<td>Employees’ use of commercial cloud applications in the workplace</td>
<td>51%</td>
<td>60%</td>
</tr>
<tr>
<td>The number of employees and others using multiple mobile devices in the workplace has increased</td>
<td></td>
<td>60%</td>
</tr>
<tr>
<td>The number of insecure mobile devices used in the workplace has increased</td>
<td>45%</td>
<td></td>
</tr>
<tr>
<td>Malware infections are more stealthy and difficult to detect</td>
<td>33%</td>
<td>32%</td>
</tr>
<tr>
<td>More employees are working offsite and using insecure Wi-Fi connections</td>
<td>16%</td>
<td>32%</td>
</tr>
</tbody>
</table>

* FY 2014 * FY 2013
* This response was not available in all fiscal years

Training
Policy
Training/Policy
Policy
Secure Configuration
Training/Policy

Training and Awareness

Engaging Your Employees In Your Defense
Training is Critical

If you don’t tell them, how will they know?

- End-user
- Board/Executive
- IT
- InfoSec

Common Denominator

“…The common denominator across the top four patterns, accounting for nearly 90% of all incidents, is **people**. Whether it’s goofing up, getting infected, behaving badly, or losing stuff…”

- 23% of recipients now open phishing messages and 11% click on attachments.
- 50% open e-mails and click on phishing links within the first hour.

2015 Data Breach Investigations Report (DBIR)
“One of the most effective ways you can minimize the phishing threat is through **awareness** and **training.**”

Lance Spitzner, Training Director, SANS Securing The Human

Secure Configurations and Regular Patching

Keeping Up With the Joneses
Compliance or IT Does Not Guarantee Security

IT

Compliance

Security

Default Settings

Insecam Displays Unsecured Webcams From Around The World

Big bertha says: default passwords

Security Override - The Default Password List

Default Passwords | CRN.net

Wi-Fi arrest highlights security dangers

An odd site called Insecam purports to display 73,000 unsecured webcams from around the world, most of them CCTV and simple IP cameras. All of the cameras have two things in common - they’re streaming on publicly accessible network ports and they are still using the default passwords, thereby opening gaps into a web of great potential and the what'should-have-beens.

© IDT911 Consulting, LLC. All Rights Reserved — Confidential
Technology Tools

- **Inventory** your technology systems and monitor for vulnerabilities that impact your environment
- **Patch** as quickly as possible
- **Use 2FA** when available

Vulnerability Management

In the inaugural DBIR (vintage 2008), we made the following observation:

*For the overwhelming majority of attacks exploiting known vulnerabilities, the patch had been available for months prior to the breach [and 71% >1 year].*

This strongly suggests that a patch deployment strategy focusing on coverage and consistency is far more effective at preventing data breaches than “fire drills” attempting to patch particular systems as soon as patches are released.

2015 Data Breach Investigations Report (DBIR)
If You Must Prioritize

These 10 Common Vulnerabilities and Exposures (CVEs) accounted for ~97% of the 2014 breach events reported in Verizon’s 2015 report.

Secure Configuration

- Desktops
- Servers
- Mobile devices
- Routers
- Cloud services (often forgotten!)
Encryption

It is neither expensive nor difficult, despite rumors to the contrary

Encryption 101

• It’s free.
• It’s easy.
• Do it.
Incident Response Planning

You Wouldn’t Be Caught Without a Fire Safety Plan

Based on risk profile, security plan and employee guidelines, develop an Incident Response Plan.

- Define
  - Protected information
  - What constitutes an "incident"
  - What constitutes a “breach”
  - WHO does WHAT WHEN

- Communicate and train
- Practice
- Refine and update

Just like a fire safety plan, you hope not to use it, but you wouldn’t think of not having one.
Incident Response Planning
The Team

- Legal / Privacy
- Insurance Broker/Agent
- Compliance
- Security Professionals
  - Internal and External
- Information Technology
- Communications
- Sales / Customer Service
- Finance
- Executive Management

Testing, Auditing and Updating Your Plan

- Are you sure?

- How do you know?
  - Test
  - Audit / Sample after implementation

- What worked last year may not work in the current environment
Backup and Recovery Measures

Just In Case

- Back up
- Test your backup periodically
Ransomware Still A Growing Threat

Limited Use of Administrator Accounts

Guard the Master Key
Access Control

• For consultant accounts, **deactivate periodically** unless the manager sponsoring the project confirms the account should continue.

• **Enforce “least privilege”** and “need to know” access.

• Log to read-only media logon successes and failures.

Access Control

• Remove guest and other default accounts.

• **Change all default passwords (accounts, systems, software & devices)**.

• Limit, monitor and alert on privilege account usage.
  – Admin privileges should not be used even by systems administrators, for day-to-day duties.

• Coordinate closely with HR to remove access for terminated employees.

• Audit accounts monthly (or at least quarterly) for active accounts that should have been removed.
Separation of Duties

This means third-party audits

Manage Conflict of Interest

- Difficult when staff is small
- External audit
- Report to CEO or Board rather than to IT or CFO
- Alerting/logging
Still Think IT Has You Covered?

Of the data breach events caused by internal personnel:

Specifically, FTP servers:

60% of incidents were attributed to errors made by System Administrators — Prime actors responsible for a significant volume of breaches and records.

“…enterprise security assessment and consulting firm [reported] their team of threat intelligence analysts encounter publicly accessible FTP servers on a daily basis…. analysts are “tripping over” company and individual FTP sites requiring no authentication. Even worse, many of these sites contain large volumes of intellectual property and personally identifiable information (PII ).”

Free Tools

• SANS
• OWASP
• Microsoft
• CSO Online
• NIST documentation and standards
Questions

We’re Hiring!

Deena Coffman | Chief Executive Officer, IDT911 Consulting
917.891.1845
dcoffman@IDT911Consulting.com

1501 Broadway | Suite 1616 |
New York, NY
10036 www.IDT911Consulting.com