Defending Against Data Beaches: Internal Controls for Cybersecurity

Presented by:
Michael Walter, Managing Director
and
Chris Manning, Associate Director
Protiviti Atlanta Office
## Agenda

- **Defining Cybersecurity**
- **Priorities for Cybersecurity**
- **NIST Cybersecurity Framework**
- **The Cyber Kill Chain – Attack, Defense and Internal Controls**
- **Defensive Enhancements and Audits**
Evolution of Cybersecurity Definition

Original Definition

Stop cyber threats from getting into our environment.

Old Definition

Try to stop cyber threats from getting into our environment and detect systems that get infected with viruses and/or malware.

Current Definition

Threats continually navigate through our environment. Ultimately we need to be able to...

Prevent  Detect  Respond
Cybersecurity Threats Methods and Countermeasures

Data is increasingly getting digitized and internet is being used to save, access and retrieve vital information. Protecting this information is not just a priority, but has become a necessity for most companies and government agencies around the world.

**Types of Cyber Threats**
- Information Warfare
- Cyber Espionage
- Cyber Crime
- Cyber Terror
- Hactivism
- Cracking

**Methods**
- Spam
- Identity theft
- Malicious code such as Viruses, Worm, Trojan Horse
- Phishing attacks
- Spyware
- Denial-of-service attacks
- Packet spoofing

**Security Measures for Protection**
- Personal Security
- Legal Compliance
- Incident Reporting
- Continuity Planning
- System Protection
- Physical & Environmental Protection
- Communications Protection
- Access Controls

Sources: Secondary Research
Cybersecurity Trends
### The Cyber/Data Breach Landscape

<table>
<thead>
<tr>
<th>2014</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2000</strong></td>
<td>Number of Breaches</td>
</tr>
<tr>
<td><strong>700m</strong></td>
<td>Records compromised</td>
</tr>
<tr>
<td><strong>$400m</strong></td>
<td>Financial losses</td>
</tr>
<tr>
<td><strong>&gt;200 days</strong></td>
<td>The average time from breach until discovery</td>
</tr>
<tr>
<td><strong>&gt;60%</strong></td>
<td>Companies learn they have been breached from a third party (customer, partner, vendor etc.)</td>
</tr>
<tr>
<td><strong>60%</strong></td>
<td>Cases where hackers were able to compromise an organization within minutes.</td>
</tr>
<tr>
<td><strong>40%</strong></td>
<td>Controls determined to be most effective fall into the “quick win” category.</td>
</tr>
</tbody>
</table>

**Most recorded attacks stem from external threat actors but internal threat actors are on the rise.**

**Breaches increasingly from “unknown” “unknowns” – almost every breached organization had up-to-date anti-virus.**

Source: Verizon, 2015 Data Breach Investigations Report
A Sample of World's Biggest Data Breaches

Source: http://www.informationisbeautiful.net/
Boards of Directors Attention

Boards of Directors are increasingly inquiring about cybersecurity as they see news of breaches, hear about increased regulatory scrutiny, and grow more concerned about cybersecurity risks.

NACD Guidance

The National Association of Corporate Directors (NACD) recently released guidance encouraging the full Board (not just the audit committee) to receive regular briefings on information security and provided five principles for Board involvement.

Cybersecurity Responsibilities

Responsibilities Include:

- **Board of Directors**
  - Commitment of resources
  - Policy approval
  - Monitoring
  - Metrics
  - Trend Analysis
  - Risk Assessment and Business Impact Analysis
  - Due care (governance)
  - Oversight

- **Executive Management**
  - Implement directives of the board
  - Regulatory compliance
  - CISO will usually perform information security on behalf of executive management

- **Cybersecurity Manager / CISO**
  - Cybersecurity strategy development
  - Overseeing the security program and initiatives
  - Coordinating with business process owners for ongoing alignment of cybersecurity with business objectives
  - Ensure RA and BIA are done
  - Developing risk mitigation strategies
  - Enforcing policy and regulatory compliance
  - Monitoring the utilization and effectiveness of security resources
  - Developing and implementing monitoring and metrics
  - Directing and monitoring security activities
  - Managing cybersecurity incidents and their remediation, as well as incorporating lessons learned
What Are Organizations Doing?

- Evaluating security risks from key vendors and partners
- Employing tools to help answer the questions “are we already breached?” and “how would we know if a breach occurs?”
- Identifying critical data (the “crown jewels”) and how it is being controlled
- Assessing internal and external vulnerabilities and performing periodic penetration tests
- Training and awareness to raise education of employees
- Evaluating the “Breach Kill Chain”
- Developing (and testing) breach response plans
- Wrapping all of this into a holistic security program – continuous and on-going
Priorities for Cybersecurity
5 Quick Wins *(SANS 20 Critical Security Controls)*

The *SANS Institute* is an American Cyber Security training company.

1. Application Whitelisting (CSC2)
2. Use Common, Secure Configurations (CSC3)
3. Patch Applications (CSC4)
4. Patch Systems (CSC4)
5. Reduce the Number of Users with Administrative Privileges (CSC3, CSC12)
SANS 20 Critical Security Control Catalogue

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
SANS 20 Critical Security Control Catalogue (cont.)

11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises
NIST Cybersecurity Framework
NIST Cybersecurity Framework (CSF) Background

• In February 2013, President Barack Obama signed an Executive Order launching the development of a Cybersecurity Framework

• Individuals and organizations around the world provided their thoughts on the kinds of standards, best practices, and guidelines that would meaningfully improve critical infrastructure cybersecurity.

• NIST published it on February 12th, 2014.


• Major differences include:
  - The inclusion of a maturity model definition to express security readiness.
  - The intention to outline an organization’s current state of security maturity as well as a “desired state”.
  - A framework to compare/contrast an organization’s security maturity to other organizations.

• Benefits
  • For organizations that don’t know where to start, the Framework provides a road map.
  • For organizations with more advanced cybersecurity, the Framework offers a way to better communicate their cyber risks internally and externally.
Cybersecurity Framework (CSF) – Functions and Categories

The **Framework Core** is a set of cybersecurity activities and informative references that are common across critical infrastructure sectors. The cybersecurity activities are grouped by five functions that provide a high-level view of an organization’s management of cyber risks.
Cyber Kill Chain – Attack, Defense and Internal Controls
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.
Cyber Kill Chain – Attack, Defense and Internal Controls

**Attacker Steps**

- Harvest information about the target (email addresses, IP addresses, system information, applications used, etc.)
- Pairing an exploit or exploits with a payload that will grant access
- Sending the exploit to the target through one or more means

**Defender Countermeasures & Internal Controls**

- Security Logging & Monitoring
- Malware Detection
- Boundary Defense
- Security Outside the Firewall
Cyber Kill Chain – Attack, Defense and Internal Controls

Attacker Steps

- Attacker performs actual exploit of vulnerable target systems
- Malicious software / malware is installed on the exploited systems, establishing a foothold

Defender Countermeasures & Internal Controls

- System Hardening and Patch Management
- File Integrity Monitoring
- Application Whitelisting
- Host-based Intrusion Detection & Prevention
- Security Logging & Monitoring
Cyber Kill Chain – Attack, Defense and Internal Controls

**Attacker Steps**

- Establish communications channel between compromised systems and the attacker’s systems
- Strengthen footholds, establish additional backdoors into target network
- Obtain sensitive data, exfiltrate it from the target

**Defender Countermeasures & Internal Controls**

- Intrusion Detection Systems
- Anti-malware devices and software
- Egress Filtering
Defensive Enhancements and Audits
Defensive Enhancements and Audits

Engage Executive Leadership through reporting and visibility

- Governance Review
  - Ensure Security is aligned to the business
  - Establishing a strong control environment as well as decision-making authorities and accountabilities

Are we doing the right things?
Are we getting the benefits?
Are we doing them the right way?
Are we doing them well?
Defensive Enhancements and Audits

**Cybersecurity Audits**

- **Server Configuration Reviews**
  - Do we have a defined (and documented) standard for all of the servers in our environment?
  - Are we running the appropriate security software?
  - Are all of our systems up to date? (Not just the Operating System)

- **Network Architecture Reviews**
  - Attackers don’t “win” unless they get your data out of your network.
  - Are we enforcing strong egress/outbound filtering?
  - Do we have internal segmentation of systems that store, process and transmit sensitive data?
  - Are there any back doors into the network? (e.g. Rogue Wireless)
  - Can we see what’s happening on the network?
Defensive Enhancements and Audits

Cybersecurity Audits

• Application Configuration Reviews and Whitelisting
  – What you don’t know can kill you – Only execute what you know is good.
  – Requires detailed partnership with IT, but results can prevent many types of attacks – particularly malware and custom malware.
  – Do we effectively manage compliance with Privacy choices we give our consumers, even if not required by regulation?

• Accounts and Privileges Audit
  – What is our organization’s policy on access and need-to-know?
  – Have we appropriately restricted access to powerful credentials?
  – Are administrators in the organization sharing accounts and passwords?
  – Don’t forget those local user accounts!
Defensive Enhancements and Audits

Review Logging and Monitoring Capabilities

• Logging Device Configuration Review
  • Most straight-forward method to testing
    – Log input sources
    – Filters / monitoring settings
    – Alerting capabilities
    – Validation of reports / data
    – Completeness testing

• Technical Considerations
  – Lots of manual activities
  – Can be burdensome for technicians
  – May require training / knowledge of the tools reviewed
  – Specific configuration settings may not be obvious
  – Recommendations may not be meaningful without detailed analysis
Defensive Enhancements and Audits

Review Logging and Monitoring Capabilities

• SIEM Pre/Post Implementation Review
  • Did we define goals / did we accomplish goals:
    – Verify use cases with technicians and end users?
    – Assess log sources successfully added to SIEM?
    – Are reporting and alerting configured and functioning?
    – Are supporting processes in place?
  • Technical Considerations
    • Involves both technical and non-technical team members.
    • Potentially challenging to perform post implementation if goals were not defined up front.
  • Reporting Considerations
    • May outline steps that were missed during the implementation.
    • Helps to refine processes and enforce completeness of implementation.
Defensive Enhancements and Audits

**Incident Response Testing and Training**

- **Tabletop Testing**
  - Can be executed quickly
  - Testing requires a low technical impact
  - Suite of technical tools (automated and manual tools) are not required
  - Quality of the testing depends on attendance / participation of the tabletop exercise
  - Recommendations tend to focus on process improvement

- **Technical Testing**
  - May require more coordination with IT, Information Security and other departments
  - Testing requires more technical impact and involvement
  - Suite of technical tools (automated and manual tools) are required
  - Quality of the testing depends on attendance / participation of the tabletop exercise
  - Recommendations tend to focus on technical improvement
Defensive Enhancements and Audits

Awareness Training

- Program Review
  - How much awareness training does your average employee receive annually?
  - Does the program include techniques for both Prevention and Detection?
  - We can't properly respond if we don't know we are being attacked.
  - Enhancements through gamification of security training.
  - Periodic testing through social engineering campaigns.
Thank You

**Michael Walter**  
Managing Director, Protiviti  
Atlanta, GA  
303.898.9145  
michael.walter@protiviti.com

**Chris Manning**  
Associate Director, Protiviti  
Atlanta, GA  
770.363.4897  
chris.manning@protiviti.com
Rethinking our Strategy
Rethinking our Strategy

1. Most Cybersecurity Controls are Preventative in Nature

Preventative Controls
- Firewalls / Next-Gen Firewalls
- Intrusion Prevention Systems (IPS)
- Antivirus / Antimalware
- Internet Proxy
- Web Content Filter
- Data Loss Prevention
- Network Admission Control (NAC)

Detective Controls
- Intrusion Detection Systems (IDS)
- Security Monitoring and Response
Rethinking our Strategy

2. Cybersecurity is still a people problem

- Organizations must focus on high impact vulnerabilities and high likelihood risks
- Security is not “Fire and Forget”
- Preventative controls are not 100% effective. When they fail, we need a detective control in place
- We can't respond to attacks we don't see coming
Rethinking our Strategy

3. Prevention is ideal but detection is a must

If the **Time** we can **Protect** our assets and/or environments is greater than the time it takes to **Detect** and **Respond** to threats, then life is good.

\[ Pt > Dt + Rt = \text{😊} \]

Otherwise, life is bad.

\[ Pt < Dt + Rt = \text{:致力} \]

*Source: Time Based Security by Winn Schwartau*
Rethinking our Strategy

4. Shift focus from preventing attacks to preventing attacker *success*

- Moving to a goal-oriented defense strategy
- Assess your risk / know your environment and know what attackers are after
- Detect attackers moving toward their goals and execute a rapid response
- Increase Threat Intelligence (know your enemy)
- Leverage security methodologies to your advantage