Addressing the Evolving Cybersecurity Landscape

Tom Tollerton, CISSP, CISA, PCI QSA
Manager – Cybersecurity Advisory Services

DHG presenter

Tom Tollerton, Manager | DHG IT Advisory | 704.367.7061 | tom.tollerton@dhgllp.com

- Leader in Cybersecurity Advisory Services
- 12+ years cybersecurity experience
- Credentials: CISSP, CISA, PCI QSA
- Focus: Cybersecurity and privacy audits, PCI compliance audits, SOC 1 & 2 examinations, cyber forensics investigations
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

DHG Birmingham CPE Seminar

Cybersecurity Threat Environment

DHG Birmingham CPE Seminar

Cybersecurity Threat Environment

DHG Birmingham CPE Seminar

Cybersecurity Threat Environment

DHG Birmingham CPE Seminar

Cybersecurity Threat Environment

DHG Birmingham CPE Seminar

Cybersecurity Threat Environment
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

costs of a breach

- Forensic Investigation
- Regulatory or Industry Fines/Penalties
- Brand Damage
- Vulnerability Remediation (Capital Cost)
- Fraudulent Transactions
- Civil Litigation

What’s on the Line?

Average time to discover a breach: > 200 days
Average cost of a data breach: $4 million

1 IBM 2016 Cost of Data Breach Study - United States

• In over half of successful breaches, attackers can compromise an organization within minutes
• 60% of attacks target small and medium-sized organizations
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

top vulnerabilities

“The initial exploit is typically simple and easy to avoid.”

1. Poor user awareness
2. Weak and default passwords
3. Missing security patches and/or anti-malware
4. Poorly configured devices
5. Poor monitoring/alerting

evolving modes of attack

- Compromising weak vendors
- Anti-forensic tools and techniques
- Extortion vs. Exfiltration
- IoT and botnets
- **Social engineering**
  - Phishing
  - Social media
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

• **Commoditization of Malware**
  - Malware “Markets”
  - Cost Effective
  - Guaranteed Results

• **Malware-as-a-Service** - All-inclusive packages
  • Rent infrastructure!
Case Studies

case study 1 – “man in the middle” attack

- Weak passwords and lack of encryption lead to capture of sensitive information over the wire
- Example of poor configuration
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

case study 2 – social engineering

Sophisticated email phishing attack deceives authorized finance manager into wiring over $50,000

Example of lack of threat awareness by critical personnel

Virtually impossible to recover lost funds

Case study 2 – social engineering (data theft)

Phishing attempts to steal employee W-2s during tax filing season

Sophisticated tactics make the attacks appear innocuous

Source: krebsontsecurity.com
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

---

case study 3 - ransomware

- Simple business model
- Extortion vs. exfiltration
- Easy to acquire and deploy
- Multiple variants difficult to trace and block
- Becoming more sophisticated

#1 CYBER THREAT TO BUSINESSES IN 2017
ransomware - continued

Scenario:
- Internal user clicks phishing link; authorizes installation of CryptoLocker
- Ransom = .5 BTC ($817.48)

$817.48 \times 20 = $16,349.60
$817.48 \times 100 = $81,748
malware – how is it getting in?

**Phishing Emails:**

Rarely is there a piece of information that is not presented in an email. Here you have a phishing email that uses fake credibility to get users to click on a malicious attachment.

**Infected websites:**

Malware is often hosted on websites. Here you can see a phishing website that is meant to look like a legitimate PayPal page.
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

malware—how is it getting in?

Social Media:

LinkedIn

From: User Support
Date: May 16, 2013
Subject: Important Profile Changes

LinkedIn Important Profile Changes. Just click on the link or button below for further details.

View/Reply to this message

Don't want to receive e-mail notifications? Block your message forever.

This email was intended for: , shared

LinkedIn Corporation, 3999 Blueridge Blvd, Mountain View, CA 94043, USA

Takeaways
to-do’s – easy wins

1. Block Malware
   • Keep Windows patches up-to-date
   • Ensure consistent antimalware is installed on all systems/kept up-to-date

2. Use Strong Passwords
   • Change periodically
   • Use eight characters with complexity
   • Don’t reuse passwords
   • Use a password manager

3. Consistent System Configurations
   • Remove administrative privileges
   • White-list authorized applications

4. Encrypt sensitive data
   • Especially laptops and removable media

5. Back Up Sensitive Data
   • Know what your valuable data is and where it is
   • Offline backups
Identify
- Organizational Understanding of Cyber Risk & Business Context
- Identification:
  - Data types & location
  - Threats
  - Vulnerabilities
- Strategic Focus & Prioritization
Addressing the Evolving Cybersecurity Landscape

NIST Cybersecurity Framework

**Protect**
- Develop & Implement Appropriate Safeguards
- Limit & Contain Impact of Cyber Events
- Physical, Technical, Administrative Security Controls

**Detect**
- Monitoring & Event Logging Functions
- Automated Systems Common
- Requires Customization to Limit False Positives
Addressing the Evolving Cybersecurity Landscape

NIST Cybersecurity Framework

Respond
- Strong Response Capabilities Contain Impact
- Clearly Defined Roles & Responsibilities
- Establishes Appropriate Communications Channels

Recover
- Plans and Activities to Restore Business Services
- Determines an Organization’s Resilience
AICPA Cybersecurity Update

### aicpa soc suite of services

<table>
<thead>
<tr>
<th>Purpose</th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
<th>SOC for CRMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of Report</td>
<td>Restricted</td>
<td>Restricted</td>
<td>General Users</td>
<td>Restricted</td>
</tr>
<tr>
<td>Report Detail</td>
<td>Testing Detail Included</td>
<td>Testing Detail Included</td>
<td>Testing Detail Not Included</td>
<td>Testing Detail Not Included</td>
</tr>
<tr>
<td>Guidance</td>
<td>SSAE 1</td>
<td>AT 101, Trust Service Principles</td>
<td>AT 101, Trust Service Principles</td>
<td>SSAE 18, Description criteria</td>
</tr>
</tbody>
</table>
SOC report for cybersecurity risk management

• **What is it?**
  
  New guidance for examination and reporting of an organization’s cybersecurity risk management program

• **Why is this needed?**

  AICPA is responding to requests for an independent, industry agnostic assessments of how cybersecurity risk is handled by an organization

• **Who is this for?**
  
  - Boards of directors
  - Investors
  - Key stakeholders

• **Clarifications**

  - How does it differ from other SOC reports?
  - Does it replace other frameworks?
  - Integration of other compliance requirements?

• **Structure**

  - Description
  - Assertion
  - Opinion

• **Description Criteria**

  - 9 control categories addressing key risk areas
Addressing the Evolving Cybersecurity Landscape

August 17, 2017

DHG Birmingham CPE Seminar

DHG Cybersecurity Capabilities

DHG cybersecurity services

- Cybersecurity Risk Assessments
- Payment Card Industry (PCI) Assessments
- SOC 1 and 2 Examinations
- Penetration Testing and Vulnerability Scanning
- Security Policy Development Assistance
- Social Engineering Assessments
- Digital Forensics & Incident Response