Emerging Network Security Threats...
...and what they mean for internal auditors

December 11, 2013
John Gagne, CISSP, CISA
Objectives

• Emerging Risks
  – Distributed Denial of Service (DDoS) Attacks
  – Social Engineering
  – Malware
  – User Technology Awareness & BYOD

• Understand the Following
  – What is it?
  – What are the risks TODAY?
  – What should an internal auditor do about it?
    • Non-Technical
    • Technical
Distributed Denial of Service (DDoS) Attack

What is it?

• Internet Service Interruption Attack

• Key Terms
  – Malware
  – Botnet
  – Bandwidth
  – Command & Control Server

• DDoS Methods
  – Flooding
  – Session Overflow
  – Specially Crafted Packet
Distributed Denial of Service (DDoS) Attack

What are the risks TODAY?

- **Motivation**
  - Social
  - Political
  - Fraud

- **Reputation**

- **Resource Distraction**

- **Business Interruption**
  - Internal (Network, VOIP)
  - External (SaaS)

- **Centralized Third Party Service Providers** (DNS, Mail Host, Proxy, Payment Gateways)
What should an internal auditor do about it?

**Non-Technical**
- Formal Internal & External Communication Plan
- Business Continuity Planning (Alternative Processing)
- Third Party Service Provider Due Diligence

**Technical**
- IDS / NetFlow Monitoring
- Firewall Filtering
  - Geo Filtering
  - Protocol Filtering
- DDoS Mitigation Technology or Third Party Provider
Social Engineering

What is it?

• Psychological manipulation of an individual to divulge confidential information.
What are the risks TODAY?

• Social Media
  – Attack Pre-Intelligence
  – Account Compromise
  – Malware Distribution
  – Reputation Risk

• Phishing
  – Spear Phishing
  – Credential Harvesting
  – Privilege Escalation
  – Data Loss
Social Engineering

What should an internal auditor do about it?

Non-Technical
- Social Media Policy
- End-User Security Awareness Training
- Reporting / Whistleblower Channels
- Identity Verification Procedures

Technical
- Social Engineering Testing
  - Performance Metrics
  - Effectiveness
- Proxy / Web Filtering Testing
- Host Based Controls / Group Policy
- Layered Security Testing
Malware

What is it?

• Unauthorized software used for malicious purposes including:
  – Disruption of normal system operation
  – Gathering of sensitive information
  – Unauthorized control of a system

• Emerging Malware Types
  – Watering Hole Attack
    • 61% of Malware is Hosted on Legitimate Sites
  – Drive-by Download
  – Mobile Malware
Malware

What are the risks TODAY?

• Customer Facing Concerns
• Third Party Patching
• AV Inadequacy
• Active Risks
  – Data Loss
  – System Processing Interruption
• Passive Risks
  – Botnet Building
  – Activity Reconnaissance
    • Future Attacks
    • Sale of Data
Malware

What should an internal auditor do about it?

Non-Technical

• Focus on customer complaint trends and fraud reports

Technical

• Multi-factor authentication
• Vulnerability Scanning
• What monitoring control are in place?
  – Anomaly Detection
  – Where is data moving?
User Technology Awareness & BYOD
What are the risks TODAY?

• Technology Awareness
  – Remote Connectivity
  – Configuration Parameters
  – Third Party Software
  – Policy Bypass

• BYOD
  – Tethering
  – Mobile Malware
  – Removable Media

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Number of Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android malware</td>
<td>103</td>
</tr>
<tr>
<td>Symbian malware</td>
<td>3</td>
</tr>
<tr>
<td>Windows Mobile malware</td>
<td>1</td>
</tr>
<tr>
<td>iOS malware</td>
<td>1</td>
</tr>
</tbody>
</table>
What should an internal auditor do about it?

Non-Technical
• Up-to-date User Policies
  – Acceptable Use
  – Removable Media
  – Mobile Device
• Lost Device Reporting Channels

Technical
• Systemic Mobile Device Policies
• System Hardening
• Data Loss Prevention Technologies
• Mobile Device Encryption
Trends

- “Everything is connected”
- Social Engineering > DDoS
- “We’re not in Kansas Anymore”
- Assume we’ve been hacked
- Points of centralization
Open Discussion

Image Sources

- 2013 Symantec Internet Security Threat Report
- 2013 IBM X-Force Mid Year Trend and Risk Report