Threat and Vulnerability Management (TVM)
Protecting IT assets through a comprehensive program

Chicago IIA/ISACA 2nd Annual Hacking Conference

October 2015
Introductions

Paul Hinds
Managing Director
Cybersecurity and Privacy Practice
Chicago, IL
paul.hinds@pwc.com

David Eccles-Ambrose
Senior Associate
Cybersecurity and Privacy Practice
Chicago, IL
david.eccles-ambrose@pwc.com
Agenda

1. Changing Risk and Protection Models
2. Threat and Vulnerability Management Programs
3. Questions
Changing Risk and Protection Models
Data Privacy & Information Security Risks

- Compliance with government or industry regulations (HIPAA, PCI, GLBA, COPPA, FTC Act)
- Compliance with self-regulatory frameworks (i.e., U.S.-EU Safe Harbor, TRUSTe, DMA OBA Principles)
- Negative impact to the brand
- Loss of employee, customer, & investor confidence
- Companies face several financial risks associated with a breach:
  - Federal or state regulatory fines
  - Stock price decline
  - Remediation efforts
- Companies are experiencing increasing lawsuits from:
  - Employees
  - Customers
  - Investors
- Enforcement actions from federal and state agencies
- Regulatory inquires may require long-term third party remediation in order to verify regulatory compliance

Threat and Vulnerability Management (TVM)  
PwC  
October 2015
## What kinds of questions should you be asking?

| 1 | Company Culture | • What are the company’s compliance requirements?  
• What is the culture of the company and what is the philosophy regarding data privacy and security?  
• Who will lead the efforts for information security & privacy (e.g., Steering Committee)?  
• How does the company ensure alignment between the management and staff?  
• What is the company trying to achieve with its information security/privacy program? |
|---|---|---|
| 2 | Sensitive Information | • What sensitive data does the company collect, use, disclose, dispose, etc.?  
• Is there a process to ensure customers are provided proper notice, choice, and consent with respect to the company’s data collection, use, and disclosure practices?  
• How does the company ensure data practices comply with customer privacy notices/policies?  
• Has the company classified and inventoried that data? |
| 3 | Threats | • Has the company's data been exposed – and would management know if it were?  
• Does the company know what breach indicators it should be monitoring?  
• Has the company released any new products that collect PII/SPI (i.e., websites, mobile apps, etc.)?  
• Has the company introduced any new technologies that access or store sensitive information (i.e., mobile devices, social media sites, cloud service providers, etc.)? |
| 4 | Building Protections | • Has the company established formal governance and controls around the data privacy lifecycle (i.e., notice, consent/choice, collection, access, disclosure, use, retention, disposal, security, etc.)?  
• Are such controls and safeguards periodically tested and monitored?  
• Have the controls and safeguards been updated to respond to changing business models? |
| 5 | Responding to Incidents | • Has the company established formal plans to respond to privacy and security incidents when they occur?  
• Is there a cross-functional team in place to monitor, investigate and respond to incidents?  
• Is the company prepared to respond to legal actions?  
• If a regulator were to inquire or investigate, would the company be prepared to respond? |
Having a Program In Place to Protect Data

A comprehensive program is needed to address the myriad of compliance requirements, and to protect consumer information and sensitive company information.
<table>
<thead>
<tr>
<th>Industry practice or tool</th>
<th>Percent of respondents using the respective practice or tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have an overall information security strategy</td>
<td>81%</td>
</tr>
<tr>
<td>Employ Chief Information Security Officer</td>
<td>74%</td>
</tr>
<tr>
<td>Employ security information &amp; event management (SIEM) technologies</td>
<td>66%</td>
</tr>
<tr>
<td>Established security baselines/standards for external partners/customers/suppliers/vendors</td>
<td>64%</td>
</tr>
<tr>
<td>Security strategy for employee use of personal devices on the enterprise</td>
<td>62%</td>
</tr>
<tr>
<td>Intrusion-prevention tools</td>
<td>60%</td>
</tr>
<tr>
<td>Vulnerability scanning tools</td>
<td>60%</td>
</tr>
<tr>
<td>Intrusion-detection tools</td>
<td>60%</td>
</tr>
<tr>
<td>Active monitoring/analysis of information security intelligence</td>
<td>59%</td>
</tr>
<tr>
<td>Vulnerability assessments</td>
<td>54%</td>
</tr>
</tbody>
</table>
Threat and Vulnerability Management (TVM) Programs
Breach Indicator Methodology

1. Baseline Network Scan
   - Acquire running state information from information technology network using WMI/Linux shell scripts
   - Configure scanning tools to network specifications
   - Use initial scan data to represent current state of network
   - Customize and tune our solution for the client network

2. Analysis of Running Processes
   - Review and analyze collected running process information for workstations and servers
   - Analyze for statistical anomalies and compare against our proprietary list of known breach indicators
   - Determine present state deviation from baseline

3. Network Log Analysis
   - Review collected information for network connections
   - May request certain log data from monitoring technologies for analysis (firewall, proxy, Web server, Intrusion Detection System, etc.)
   - Provide a thorough picture of the state of the network
   - Correlate end-point results with expanded network knowledge

4. Output Analysis / Threat Intelligence Review
   - Work with internal information technology teams to determine business justification for processes and network connections that exist within environment
   - Establish baseline limited to authorized system or network activity
   - Validate technical results and build threat profile

5. Report Findings
   - Categorize the assessment observations by risk in a detailed observations matrix for leadership to review
   - Business impact discussion with key stakeholders
   - Document results for stakeholder remediation decisions

Why?

- Customize and tune our solution for the client network
- Determine present state deviation from baseline
- Correlate end-point results with expanded network knowledge
- Validate technical results and build threat profile
- Document results for stakeholder remediation decisions
Components of a TVM Program

Defining program ownership, policies and procedures, and integration with enterprise risk management program

Evaluating threats and vulnerabilities and establishing communication and tracking mechanisms

Detecting breaches, rogue technologies, and malicious activities.

Actively identifying asset weaknesses before they can be exploited by an attack

Actively monitoring and enhancing the TVM program

Isolating and resolving asset security issues once identified

Threat and Vulnerability Management Program

Security, Information Management & Sustainability

Threat and Vulnerability Evaluation

TVM Security Strategy & Planning

Vulnerability Detection

Threat Detection
TVM Program – 20 Integrated Capabilities

- Program ownership
- Policy and procedures
- Integration with risk management
- Intrusion monitoring
- Malicious program detection
- Rogue technology discovery
- Log activity analysis
- Compliance testing
- Vulnerability scanning
- Penetration testing
- Intelligence analysis
- Security intelligence
- Communication and tracking
- Controls effectiveness evaluation
- Security infrastructure implementation
- Threat awareness
- Reporting
- Security remediation
- Incident response
- Threat and Vulnerability Evaluation
- Threat and Vulnerability Management
- Security, Information Management & Sustainability
- Threat and Vulnerability Management Program
- TVM Security Strategy & Planning
- TVM Security Strategy & Planning
- TVM Security Strategy & Planning
- TVM Security Strategy & Planning
- TVM Security Strategy & Planning
- TVM Security Strategy & Planning
TVM Program – Scorecard

Program ownership
Policy and procedures
Integration with risk management

Intrusion monitoring
Malicious program detection
Rogue technology discovery
Log activity analysis

Compliance testing
Vulnerability scanning
Penetration testing
Intelligence analysis

Security intelligence
Communication and tracking
Controls effectiveness evaluation

Threat and vulnerability management program

Security infrastructure implementation
Security remediation
Incident response
Threat and Vulnerability Evaluation

Threat and information management & Sustenance

Threat awareness
Reporting

Program maturity enhancement

TVM Security Strategy & Planning
**TVM Security Strategy & Planning Assessment**

**Program ownership**
The governance structure must ensure that designated individuals have the capacity to hold asset owners accountable.

**Policy and procedure**
Management’s intent and directives are documented in the relevant policies and procedures, but must be enhanced with additional security awareness training.

**Integration with risk management**
An integrated TVM program which enhances the overall enterprise information security risk management program.
Threat Detection Capabilities Analysis

Intrusion monitoring
There’s lots of options- host based like OSSEC, or network based like SNORT, but how do you assess the effectiveness of the intrusion monitoring?

Malicious program detection
Rogue security software, adware, and spyware.

Rogue technology discovery
It can be difficult to detect, prevent, and control rogue technologies in most enterprise environments. Network Access Control (Cisco ISE), detect unapproved wireless device with Cisco CleanAir®.

Log activity analysis
How do you effectively manage your log monitoring and anomaly detection capabilities? SIEM tools like AlienVault, LogRythm, and Splunk?

Breach indicator analysis
Immature organizations lack basic capabilities to identify indicators of a security breach.

Actively identifying and isolating threats to minimize their impact upon assets
Vulnerability Detection Analysis

Compliance testing
How do you evaluate conformance with established security guidelines and policies and compliance monitoring techniques? Unreliable scanning or time consuming audits?

Vulnerability scanning
Enhance vulnerability scanning capabilities by assessing factors such as tools, techniques, scope and frequency. *Nessus, Nexpose, QualysGuard.*

Penetration testing
Penetration testing assesses factors such as methodology, attack scenarios, scope and frequency.

Intelligence analysis
Security intelligence should be gathered from multiple sources and effectively leveraged through use of intelligence tools.

Actively identifying asset weaknesses before they can be exploited by an attack
**Threat and Vulnerability Evaluation Analysis**

**Security intelligence**
Big data analytics approach (*ArcSight* or *QRadar*) ensures assimilation and correlation of security information and the process of responding to the identified issues.

**Communication and tracking**
How are identified threats and vulnerabilities being communicated and tracked until closure?

**Controls effectiveness evaluation**
Assess the process of evaluating the controls and mitigating mechanisms.

---

Evaluating threats and vulnerabilities and establishing communication and tracking mechanism
**Threat and Vulnerability Remediation and Response Analysis**

**Security infrastructure implementation**
Enforce change management and configuration management processes to ensure infrastructure and controls are implemented consistently with the company’s security standards, such that they achieve the desired benefits and functionality.

**Security remediation**
Security remediation of the vulnerabilities detected should be a key performance indicator for the security program.

**Incident response**
Adopt mature IT service management (ITSM), i.e. ITIL.
Security Information Management and Sustenance Analysis

**Program maturity enhancement**
Continually monitor and enhance the program’s maturity.

**Threat awareness**
Enhance the organization’s defenses with security awareness activities to educate relevant users on threats.

**Reporting**
Identify key performance and key risk indicators for reporting the status of the TVM program and the actions taken in response improve the current capabilities.