Security Frameworks

What are they for?
May 13, 2015
Presenters & Trusted Advisors

• **Brian Serra**
  - VP, PCI Advisory Solutions
  - 20 years of InfoSec experience
  - CISSP, PCIP, ASV

• **Jeff Hall**
  - Senior Security Consultant
  - 30+ years of technology and security experience
  - CISSP, CISM, CGEIT, PCI QSA, PCIP
Agenda

• What is a security framework?
• Common security frameworks
• The control triad
• Where security frameworks fit
• Deeper dive
What Is A Security Framework?

- Shared security knowledge base
- What works to secure infrastructure, systems and data
- Frequency of review and assessment
Security Frameworks Timeline

1995
BS 7799

1996
ISACA COBIT

1994
FIPS 140-1

2000
ISO 17799

2002
Visa USA CISP FISMA

2003
MasterCard SDP

2006
PCI DSS

2005
ISO 27001:2005

2009
HIPAA HITECH

2011
SSAE 16 SOC2/3

2013
ISO 27001:2013
Common Security Frameworks

• **NIST/FIPS**
  – General security framework

• **ISO/IEC 27000**
  – General security framework

• **Payment Card Industry**
  – Focused on the security of payment card data
Common Security Frameworks

• Health Information Technology for Economic and Clinical Health (HITECH)
  – Focused on protected health information (PHI)

• Federal Information Systems Management Act (FISMA)
  – Focused on security of all government information systems
Common Security Frameworks

• ISACA COBIT
  – Overall IT audit framework with sections on security and privacy
Common Security Frameworks

• Statement on Standards for Attestation Engagements (SSAE) 16
  – Service Organization Controls 3 (SOC 3)
  – Service Organization Controls 2 (SOC 2)
Just A Quick Comment

• SSAE 16 SOC 2/3 is not a security framework per se
  – Specifies security domains
  – Controls and testing are dependent on the customer and auditor defining those components
  – Need to review report in detail to determine if it is usable and what is usable
The Control Triad

Protection
Detection
Correction
The Control Triad

• **Protection**
  – Stops an attack or abuse

• **Detection**
  – Identifies an attack or abuse when protection fails

• **Correction**
  – Identifies changes to correct the control failure(s)
Where Security Frameworks Fit

• Define what
  – Infrastructure
  – Operating systems
  – Applications
  – Data
Where Security Frameworks Fit

• Define why
  – Threats
  – Risks
  – Vulnerabilities
Where Security Frameworks Fit

• Define how
  – Techniques for securing infrastructure and systems
  – Mitigation of risks
Where Security Frameworks Fit

• **Define when**
  – Real time
  – Daily
  – Weekly
  – Monthly
  – Annually
  – Periodically
Where Security Frameworks Fit

• Periodically
  – Periodically ≠ annually
  – Defined by your organization’s risk assessment
  – May vary by device or application
What Security Frameworks Do Not Do

• **Security is not perfect**
  – Compliance does not mean you cannot be breached or have a security incident

• **Stop mistakes**
  – Human errors still occur
  – Security frameworks use “defense in depth” to minimize impact of those errors
What Security Frameworks Do Not Do

• Security frameworks are bare minimums
A Bit Deeper Dive

• PCI DSS
  – Build and maintain a secure network and systems
    • Requirement 1 - Install and maintain a firewall configuration to protect cardholder data
    • Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters
A Bit Deeper Dive

• **PCI DSS**
  
  – Protect cardholder data
    • Requirement 3 - Protect stored cardholder data
    • Requirement 4 - Encrypt transmission of cardholder data across open, public networks
  
  – Maintain a vulnerability management program
    • Requirement 5 - Protect all systems against malware and regularly update anti-virus software or programs
    • Requirement 6 - Develop and maintain secure systems and applications
A Bit Deeper Dive

• PCI DSS
  – Implement strong access control measures
    • Requirement 7 - Restrict access to cardholder data by business need to know
    • Requirement 8 - Identify and authenticate access to system components
    • Requirement 9 - Restrict physical access to cardholder data
A Bit Deeper Dive

• PCI DSS
  – Regularly monitor and test networks
    • Requirement 10 - Track and monitor all access to network resources and cardholder data
    • Requirement 11 - Regularly test security systems and processes
  – Maintain an information security policy
    • Requirement 12 - Maintain a policy that addresses information security for all personnel
## A Bit Deeper Dive

<table>
<thead>
<tr>
<th>NIST CATEGORY</th>
<th>PCI DSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categorize</td>
<td>Open PCI Scoping Toolkit</td>
</tr>
<tr>
<td>Select</td>
<td>Process, store or transmit cardholder data or “connected to” systems</td>
</tr>
<tr>
<td>Implement</td>
<td>Requirements 1, 2, 3, 4, 5, 6, 12</td>
</tr>
<tr>
<td>Assess</td>
<td>Qualified Security Assessor, Internal Security Assessor or self-assessment</td>
</tr>
<tr>
<td>Authorize</td>
<td>Requirements 7, 8, 9</td>
</tr>
<tr>
<td>Monitor</td>
<td>Requirements 10, 11</td>
</tr>
</tbody>
</table>
Thank You!