Compliance Is Security

Presented by:

Jeff Hall
Optiv Security
Agenda

• The mantra heard round the world
• Compliance defined
• Official requirements
• Compliance is never done
• Defense in depth
• “A surprise”
• Compliance really is security

Tweet along: #Sec360
www.Secure360.org
The Mantra Heard Round The World

“Compliance does not equal security”

Or … does it?

Tweet along: #Sec360

www.Secure360.org
The Breaches Do Not Bear That Out

• 2015 Verizon Data Breach Report
  • 40% of attacks are using stolen credentials
  • 25% of attacks using RAM scrapers
  • 25% of attacks using phishing
  • 10% of attacks using keyboard logging

• Do these attack vectors sound like they are coming from “compliant” organizations?
  • Verizon’s analysis says they were NOT compliant

Tweet along: #Sec360
www.Secure360.org
“Conformity in fulfilling official requirements.”
Official Requirements

- NIST
  - FedRAMP
- ISO 27K
- PCI
  - Data Security Standard (DSS)
  - Payment Application Data Security Standard (PA-DSS)
  - Payment Terminal Security (PTS)
- HIPAA HITECH
  - HITRUST
NIST vs ISO 27K

• NIST
  • Focused on all of information security and all systems
  • Multiple standards
    • Some standards are very high level and others are very detailed
    • Basis for most other information security standards

• ISO 27K
  • Focused on all of information security and all systems
  • Multiple standards
    • General standard (27001)
    • More detailed standard (27002)
HITECH vs PCI DSS

• HIPAA HITECH
  • Focused on the processing, storage and transmission of personal health information (PHI)
  • Goes into detail on protection of PHI and its recovery
  • Scope only covers systems that process, store or transmit PHI

• PCI DSS
  • Focused on the processing, storage and transmission of sensitive authentication data (SAD) and cardholder data (CHD)
  • Goes into detail on protection of SAD/CHD
  • Scope only covers systems that process, store or transmit SAD/CHD
Caveats On Official Requirements

• They are all only baselines
  • Collection of “best practices” or “shared knowledgebase” for ensuring information security
  • The bare minimum for being secure
  • Some more in-depth than others

• Scope of each framework is not equivalent

• They are not the “be all to end all” in information security
  • Need to be tweaked for your environment/equipment/architecture
  • May need to be enhanced/changed if your environment does not lend itself to their practices
Caveats On Official Requirements

• HITRUST
  • An admirable attempt to map various security standards to reduce assessment overlap and fatigue
    • HITECH, NIST, ISO 27K, PCI DSS, SOX
  • At this point, does not deliver on its promise
    • Mapping between the standards does not appear accurate
    • Assumes the scope from one standard is sufficient for other standards
    • Assumes that assessment testing is consistent from standard to standard
    • Assumes the level of testing detail required by one standard is sufficient for other standards
Program Depth

NIST
ISO
PCI
HIPAA
Testing Example #1

- User management
  - HITECH – users with access to PHI are tested
  - PCI DSS – users with access to bulk SAD/CHD are tested
  - SOX – users with access to material financial data are tested

- Are system users in these groups the same?
  - Probably not other than possibly system and network administrators
  - As a result, any testing in one group will not cover the other two groups

Tweet along: #Sec360  www.Secure360.org
Testing Example #2

• Internet-based solutions
  • HITECH – electronic medical records (EMR) online solution is in-house providing a secure gateway to internal EMR
  • PCI DSS – bill payment is outsourced to payment processor
  • SOX – financial systems are isolated away from all other systems

• How do you get leverage from testing?
  • You do not
  • Solutions were isolated from one another for valid security, compliance and business reasons
Compliance vs Consistency

• Standards must be followed and executed 24x7x365 without significant lapses in coverage to ensure security
  • Organizations confuse “compliance” with “consistency”
  • If people are NOT executing security standards and procedures consistently each and every day, then they are NOT complying with those security standards and procedures
    • Therefore, the organization is NOT compliant
  • However, a security assessment is not necessarily a good gauge of an organization being secure because they are usually completed as of a single point in time, not over a period of time
The Dilemma—Compliance Is Never 100%

- Organizations constantly generate alerts or have gaps in security
  - Spam
  - Phishing
  - User sends an email or instant message that contains prohibited information
  - Account locked out due to password forgotten
  - User attempts to access a “bad” Website
  - User infects computer from email attachment or file from USB drive
  - User accesses an infected USB drive
  - DDoS attacks

Tweet along: #Sec360  www.Secure360.org
Compliance Is Never Done

• Compliance is an on-going effort NOT a one time thing
  • Compliance is a constant journey not a destination

• Compliance with a standard says that, at a given point in time, the organization complied with the standard
  • Although, this appears to be changing for some standards
  • Which means the cost of ensuring compliance will go up because additional testing will be required
Which Is Why …

• We have defense in depth
  • People make mistakes or have accidents
  • Because of mistakes/accidents, we need other controls to prevent those mistakes/accidents from creating holes in our security

Tweet along: #Sec360
www.Secure360.org
Bank Defense In Depth

• Alarm system
• Multiple vaults
• Time locks
• Video surveillance
• Dye packs
• Limited amount of cash in drawers
• Guard(s)
• Bullet proof glass
• Regular cashier training and robbery drills
Technology Defense In Depth

• Physical security on data centers
• Firewalls with access control lists (ACL)
• Intrusion Detection/Prevention (IDS, IPS)
• Anti-virus and anti-malware
• Application white and/or black listing
• System incident and event management (SIEM)
• Integrated authentication management (IAM)
• Critical file monitoring (FIM)
• Encryption

Tweet along: #Sec360
www.Secure360.org
What Was Missing Between The Two?

• Security awareness training
  • The big gap that remains in information security
    • We are great technologists
    • We are lousy with people which is why we are technologists
  • Why social engineering techniques are being relied upon to breach organizations
    • Everyone has firewalls with ACLs, IDS/IPS and other security technologies
    • Humans (i.e., hOS) are not regularly “patched”
    • Easier to hack a human than a firewall or network
Security Awareness Is …

• NOT easy
• NOT effective if not done regularly
  • You really think that annual training is often enough? Think again
• NOT effective if not made relevant
  • Explain the scams not the technologies behind them
• NOT effective for all people
  • Some people are just gullible and cannot be “patched”
  • Have to mitigate this risk with either additional controls or move these people into positions where they present little risk
Take Aways

• 24x7x365 compliance with an organization’s security policies, standards and procedures is NOT easy
• Complying with a standard as of a given point in time IS easy
• We have all of the technology we need but we need to use it better
• Security awareness training is the last area we need to address
• Partner with Human Resources, security training companies and industrial psychologists for security awareness training assistance

Tweet along: #Sec360
Bottom Line

• Done right, compliance does equal security
Thank You!
Jeff Hall, Principal Security Consultant
CISSP, CISM, CGEIT, PCI QSA, PCIP
Optiv Security
jeff.hall@optiv.com