Information Security: Challenges to Compliance

Matthew Junod, JD
CISM, CISSP, CIPP/US
Information Security Officer
The University of Toledo

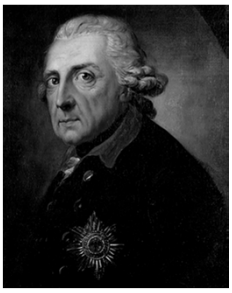
Information Security: Agenda

- The State of Security, 2016: A View from the Trenches
- Security & Compliance Challenges: Social Media, the "Cloud", the Internet of Things
- Security, Privacy, Compliance: Strategies to Manage Technology Concerns

Information Security: Words of Wisdom

"He who defends everything, defends nothing."

- Frederick the Great



The State of Security, 2016:

A View from the Trenches on
Security Core Functions and the Current Landscape

The State of Security: My Organization

UT IT security at a glance:

- State University with teaching hospital
  - >20,000 Students
  - >9,000 Employees, Affiliates
- Self-hosted infrastructure
  - 2 primary datacenters
  - Utility, PV, wind, gas co-gen power
  - 2 "class b" networks; OARNet fiber
  - 3500 servers, 14,000 UT owned "things"
- Merged institutions, centralized IT
  - 1 Security Officer, 4 FT staff, 3 graduate workers
  - Pure security & investigations function
  - HIPAA handled in-house with external support
- Cybersecurity reports through CIO/CTO
  - Dotted lines to Audit/Compliance and Legal
- Privacy and Compliance under CCO/Dir. Internal Audit

The State of Security: The Core Functions of a Security Office

Identify, Prevent, Detect, and Respond to and Recover from security threats, by:

- Identifying security requirements
- Using a framework for alignment
- Discovering the environment
- Conducting a security risk analysis
- Developing a security plan, strategy
- Prioritizing improvement activities
- Monitoring & measuring progress

The State of Security: Security Landscape

Trends putting stress on the standard security operating model:

- Ubiquitous, continuous attacks of all types and from all actors
  - Nation-states, criminal gangs, hacktivists, ???
- Malware is more dangerous, and there's more of it
  - 0-Days, exploit kits, cryptomalware/ransomware, forensic-resistant malware
- Commoditization of security and hacking tools
  - Barriers to entry are low
- Traditional security tools losing effectiveness on their own:
  - Antivirus, firewalls, complex passwords

The State of Security: Security Landscape (cont'd)

Trends putting stress on the standard security operating model:

- Large increase in quantity and variety of devices and systems
- Users expect mobile & "consumer-like" experiences
- Bring-Your-Own Device ("BYOD")
  - Learn to defend a network with no perimeter
- Increasing executive, regulator, and consumer attention
  - Civil Suits, Fines, Loss of Business, Pink Slips
- Increasing resource demands, increasing compliance burden
  - Tight market for security talent, not enough capacity for workload

Security & Compliance Challenges:

Social Media, "Cloud", the Internet of Things
Stretching the Security

Security & Compliance Challenges: Social Media, "Cloud", & the Internet of Things

- Social Media
- Cloud Services
  - IAAS
  - PAAS
  - SAAS
- Internet of Things

Security & Compliance Challenges: Social Media

Courtesy Overdrive Interactive

Security and Compliance Challenges: Social Media

"Social Media" defies definition

Attributes:
- Web-based technologies
- User generated content
- Individual user profiles
- Service facilitates connections between users

Example categories:
- Social Networks
- Blogging
- Media sharing
- Location services
- Streaming
- Gaming
- Employment sites
- Wikis

Security and Compliance Challenges: Social Media

Know what's in your public profile.

Security issues include:

- Oversharing, Overpublication
- Hacker reconnaissance
- New vectors for cyberattack
  - URL shorteners
  - XSS and web attacks
  - Insecure apps
- Credential re-use
- Account compromises
  - "Twitter Hacks"

Security and Compliance Challenges: Social Media (cont'd)

Security issues include:

- Public relations mishaps
- Identity Theft
- Doxing / Identity dumps
- Cyberstalking
- "Real World" crimes: Burglary, Assault, Stalking/Harassment

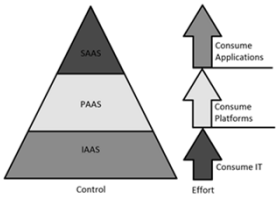
Do you know where this sends you?

Security & Compliance Challenges: Cloud Computing

Security & Compliance Challenges: What is the "Cloud" Anyway?

Three traditional flavors:

- SAAS: Software as a service
  - "Cloud" for end users
- PAAS: Platform as a service
  - "Cloud" for application developers
- IAAS: Infrastructure as a service
  - "Cloud" for IT folks



Security & Compliance Challenges: Cloud Computing

Cloud computing issues to look out for:

- Shadow IT
  - Is there unmanaged or unauthorized use of cloud apps?
- Licensing
  - Is the cloud service licensed for business or personal use?
- Governance (which cloud services get bought/used and how)
  - Do end users choose the applications? IT? A committee?
- Monitoring capabilities – users, software, platforms, infrastructure
  - What's going on in an environment you don't totally control?

Security & Compliance Challenges: Cloud Computing (cont'd)

- Business Associate Agreements
  - Necessary for cloud services dealing with ePHI
- Contractual security controls
  - Do they meet your organization's security standards?
  - If so, will they agree to be bound by them contractually?
- Contractual right to audit
  - Do they do what they say they do?
- Contractual allocation of risk (indemnification, limits on damages)
  - Healthcare is #1 industry for breach costs on a per-capita basis

Security & Compliance Challenges: The Internet of Things

The Internet of Things: What is the Internet of Things?

"Stuff" connected to a network (the Internet) for some purpose.

Examples:

- Webcams
- Industrial control systems
- Traffic control devices
- Household Appliances
- Medical Equipment, such as:
  - Pumps
  - Monitors
  - Imaging modalities

Security and Compliance Challenges The Internet of Things:

Security and Compliance Challenges: The Internet of Things

- If it's directly exposed to the Internet, it will be found:

- If it's connected to a network, it's a target for compromise

Security and Compliance Challenges: The Internet of Things

Factors impacting medical device cyber (in)security:

- Weak to nonexistent security controls
- Long device service lives, infrequent security fixes
- Legacy, outdated commodity operating system software
- Device vendor sales and support model
- Confusion over FDA regulations
- Lack of device vendor enforcement and security oversight

Security, Privacy, Compliance:

Strategies to Manage Technology Concerns

Strategies to Manage Technology Concerns: Navigating the Security Landscape

You've already been and will continue to be compromised, now deal with it:

- Have a strategy, develop a plan
  - Compliance ≠ Security…but compliance is not a bad place to start
  - The HIPAA security rule: You're in healthcare, so look here first
  - Be agile, but have guiding principles and know your boundaries
- Vision, swiftness and competence of execution are vital
  - Something is better than nothing, so focus on high-risk/low-maturity areas first
  - Don't let perfect become the enemy of the good – there is no perfect security
- Establish cross-functional ownership of the plan and oversight of execution
  - Get buy-in and participation
  - Typical players include:

    Cybersecurity, IT, Business Units, Privacy Office, Legal, Risk Management, Compliance, Internal Audit, Human Resources, Safety/Corporate Security, Marketing/Communications

Strategies to Manage Technology Concerns: Navigating the Security Landscape

Factor relative cost/benefit into your security plans:

- Take advantage of low investment, high return activities
  - Risk Analysis
  - Asset Inventories
  - Training and Awareness
  - Operating Policies and Procedures
  - Security Standards and Baselines
- Consolidate spending to targeted investments in big ticket items
  - Advanced security technologies (APT defenses, NGFW's, SIEMs and UBA)
  - Additional staffing, consultants and managed services

Strategies to Manage Technology Concerns: Social Media

To manage risks associated with Social Media:

- Understand your compliance environment
- Survey social media use among user population
  - Network analysis (DNS, IPS/IDS, Firewalls)
  - Web usage reporting tools
  - Third party cloud security tools (CASB)
- Identify problematic cloud services
- Investigate the "Enterprise Edition"
- Develop organizational policies for social media use at work and away
- See what the hackers see: Use social media for threat intelligence

Strategies to Manage Technology Concerns: Additional Tips for Consumers of Social Media

For individual users of social media services, think about:

- Burner accounts
- Credit monitoring
- Privacy settings
- App permission creep
- Pruning your networks periodically ("Defriending")

Strategies to Manage Technology Concerns: Cloud Services

To manage risks associated with cloud services:

- Establish governance over technology acquisitions and procurement
- Survey cloud service usage among employees
- Consider embracing popular services (e.g., Gmail for Business)
- Develop policies and standards for use of cloud services
- Have security strategies that cover all cloud models:
  - SaaS: Define security controls for application access
  - PaaS: Protect data and application customizations
  - IaaS: Secure the computing environment, protect data and applications

Strategies to Manage Technology Concerns: Internet of Things

To manage risks associated with smart devices:

- Don't let the problem get (further) out of control
  - Establish governance over technology selection and acquisition
  - Build checkpoints into your procurement processes
  - Conduct security analysis on proposed device purchases
- Develop technical security standards for networked devices
  - Windows XP should not be on the table in 2016
- Trust, but verify device vendor claims
  - Ask vendors for security testing reports of their devices
  - Get written responses to your identified security concerns
    - Flag outliers in your HIPAA covered entity risk analysis

Strategies to Manage Technology Concerns: Internet of Things (cont'd)

To manage risks associated with smart devices:

- Know what you own, what you acquire, and what you dispose of
  - Establish inventory processes that include all network enabled assets
- Know your exposures
  - Perform external and internal scans to learn your security vulnerabilities
- Limit the potential damage to at-risk systems
  - Implement firewalls and compartmentalize your networks ("segmentation")
- Understand the attendant risks with different types of "things"
  - Evaluate special controls for mobile devices (MDM, MAM, MCM)

Information Security: Parting Words of Wisdom

- "Everything is Awesome"

  - Emmet the Lego guy

Questions & Comments Contact Information

Matthew C. Junod
University of Toledo:
matthew.junod@utoledo.edu
419-530-3995

Personal:
matt@junod.com
567-343-2041