How to Build Security into Your Project Lifecycle

Frederick Scholl, Ph.D., CISSP
Kathleen Wark, PMP
Presentation Mission & Objectives

• Mission: “Build Security In”
• Security is bigger than IT
• Educational…point out opportunities for PM’s
• Objectives:
  • What questions to ask?
  • Potential stumbling blocks
  • Key opportunities for PMs
    • Reduce risk of project delays
    • Reduce risk of security failures
Presentation Approach

• Why is security important?
• Definition of security
• Approaches and challenges for Project Managers
• Key opportunities
• Q&A
Language Gaps: Is a Cloud Secure?

Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data

By MIKE ISAAC, KATIE BENNER and SHEERA FRENKEL  NOV. 21, 2017

The Switch

Equifax’s massive 2017 data breach keeps getting worse

';--have i been pwned?

Check if you have an account that has been compromised in a data breach
What is Security? More than Technology

- Confidentiality
- Integrity
- Availability
- Abuse
- Misuse
- Breach management
“Thank goodness I had the ultimate tires, engineered to meet the unexpected.”
Where are Today’s Vulnerabilities?
High-Likelihood, High-Impact Risks
Security is an Emergent Property
What Happened?

- Seaman went to sleep
- Another seaman noticed open door…did nothing
- Captain didn’t check because it never happened before
- Company operated with reduced crew
- No one knew what was going on
Project Managers Approach/Challenges

• PMBOK – security is mentioned 22 times
  • Follow your industry & organizational security policies, processes, & procedures.
  • Ensure security of work positions
  • Include security in the non-functional section of the requirements document.
  • Additional security measures may be needed for sensitive information

• What’s the reality?
  • Lack of knowledge concerning WHAT resources are needed
  • Understanding of WHEN those resources are needed
  • Security ‘black hole’
  • Understanding that security is MORE than just the resources & technology
Stumbling Blocks: How to Engage with Security?

- Language barrier
- Knowledge
- Availability
- Communication
- Time

Clear definition of terms
Clearly defined responsibility areas
Clear understanding of timelines:
  - advanced notice
Clear understanding of test processes
Personality Traits of Cybersecurity Professionals*

- Less trusting
- Higher intellect
- More adventurous
- Low-vulnerability score
- Low self-consciousness

* Sarah Ellen Freed, UT Chattanooga, 2014
Key Opportunities to Address Security

- Initiation
- Budgeting
- Requirements
- Architecture & Design
- DevOps/development
- Testing
- Deployment
- Transition to Support / Support

Proactively address security into each phase and/or deliverable
Building the Team

Traditional Security Resources:
- Security architect
- Application security engineer
- Network security
- Data center operations
- Cloud security

Other Resources to Consider:
- Internal audit
- Legal (vendor, contracts)
- Privacy engineer/Chief Privacy Officer (CPO)
- Chief Risk Officer (CRO)
- Compliance Officer
- Business continuity
- Incident response
“With the money we’ll save by shutting down quality control, we can issue some truly spectacular apologies.”
Budgeting

• Security resources
• Project Team
  • Project team members – background/drug testing
  • Project team access
  • Document repositories
  • VPN/communication
• Security of the project development environment
  • Development environments
  • VPN/communication
• Ongoing maintenance
• Patching of open-source software
• Business continuity
• Disaster recovery
NIST CSF

- Cyber Security Framework

| Identify (Threat Model) | Protect (Defensive) | Detect | Respond (Incident Response) | Recover (BC/DR) |
Requirements - NFR

- Roles & Responsibilities
  - Segregation of duties
  - Least privilege
- Authentication & Authorization
- Compliance
- Privacy Engineering
  - GDPR
Risk Level of Information – Things to Consider

- Data sensitivity (PI)
- Availability of the data
- Accuracy of the information
- Compliance requirements (HIPPA)
- Third-party requirements
- Business secrets
- Contracts
  - Vendors
  - Applications
Vendors: Third-Party Risk Management

- Falls outside traditional IT security
- SaaS
- Facebook

Data Breach at Sears and Delta May Have Hit 'Several Hundred Thousand' Customers
Architecture & Design

- Threat modeling – who will attack and who will break in?
- Third-party risks
- Design the testability in
- Integration
- Monitoring
- Intrusion
- Existing environments (existing risks)
- Disaster Recovery

Don't forget NIST CSF
Development Lifecycle

• Development lifecycle speeding up
  • Waterfall
  • Agile
  • DevOps
• Condensed timelines
• Segregation of dev and testing and production
Security Testing in Dev Lifecycle

- Automation
- Static testing
  - Definition
  - When to do?
- Dynamic testing
- Penetration testing
- Bug bounties
Development & Post Implementation Support

- Security awareness training for users
- User roles & responsibilities
- Potential for new log-on issues
- Limit access to old/sunset systems
- Bug bounty
- Incident response
Takeaways

• PMs are in the best position to assure “built-in” systems security.
• PMs to become more active as stakeholders in the project.
• Security isn’t “IT security” anymore.
• Security can’t be assured by IT security.
• Good security is a team sport.

**Proactively build security in**
Resources

- The Phoenix Project, applying security in a modern DevOps world
- DevOps for the Modern Enterprise, Mirco Hering
- Online glossary of security terms for PM’s

- Frederick Scholl: freds@monarch-info.com
- Kathleen Wark: Kathleen.wark@infoworks-tn.com
THANK YOU