Managing IT Security Projects

Russ Weeks, Northrop Grumman, Missile Defense Agency Project Manager, Security+ CE, CISSP, ITILv3 Practitioner - IT Service Management

Change is good. You go first!
DILBERT (BY SCOTT ADAMS)
MORDAC, THE PREVENTER OF INFORMATION SERVICES.

SECURITY IS MORE IMPORTANT THAN USABILITY.

IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.

To complete the log-in procedure, stare directly at the sun.
Introduction

- All IT projects require IT security baked in to the project plan from the start

- Planning for security in the project starts at the initial requirements phase

- IT security is designed, tested, retested and documented throughout the project

- IT security is part of the transition to Operations and Maintenance for continued support through the systems lifecycle until system retirement
Once organization’s vision and objectives are understood, process for creating project plan can be defined.

Major steps in executing project plan are:

- Planning the project
- Supervising tasks and action steps
- Wrapping up

Each organization must determine its own project management methodology for IT and information security projects.
Developing the Project Plan

- Creation of project plan can be done using work breakdown structure (WBS)

- Major project tasks in WBS are work to be accomplished; individuals assigned; start and end dates; amount of effort required; estimated capital and noncapital expenses; and identification of dependencies between/among tasks

- IT security should have its own WBS Task AND lines in each implementation activity
Work Breakdown Structure

Construction of a House

1. Internal
   - 1.1 Electrical
     - 1.1.1 Rough-in electrical

2. Foundation
   - 2.1 Excavate
     - 2.1.1 Pour Concrete

3. External
   - 3.1 Masonry Work
     - 3.1.1 Lay masonry

Level 1 Deliverables = 100%
Level 2 = 100%
Level 3 Work Package = 100%
Project Planning Considerations

- As the project plan is developed, adding IT security details is not always straightforward

- Special IT security considerations include financial; priority; time and schedule; staff; procurement; organizational feasibility; and training
Financial Considerations

- No matter what information security needs exist, amount of effort that can be expended depends on funds available.

- Cost-benefit analysis must be verified prior to development of project plan.

- Both public and private organizations have budgetary constraints, though of a different nature.

- To justify an amount budgeted for a security project at either public or for-profit organizations, may be useful to benchmark expenses of similar organizations.
Priority Considerations

- In general, most important information security controls should be scheduled first.

- Implementation of controls is guided by prioritization of threats and value of threatened information assets.
Time and Scheduling Considerations

- Time impacts dozens of points in the development of a project plan, including:
  - Time to order, receive install and configure security control
  - Time to choose IT security compliant devices and software
  - Time to test IT security systems and procedures
  - Time to train the users
  - Time to realize return on investment of control
Staffing Considerations

- Lack of enough qualified, trained, and available personnel constrains project plan

- Experienced staff often needed to implement available technologies and develop and implement policies and training programs
Procurement Considerations

- IT and information security planners must consider acquisition of goods and services.

- Many constraints on selection process for equipment and services in most organizations, specifically in selection of service vendors or products from manufacturers/suppliers.

- These constraints may eliminate a technology from realm of possibilities.
Organizational Feasibility Considerations

- Policies require time to develop; new technologies require time to be installed, configured, and tested

- Employees need training on new policies and technology, and how new information security program affects their working lives

- Changes should be transparent to system users, unless the new technology intended to change procedures (e.g., requiring additional authentication or verification)
Training and Indoctrination Considerations

- Size of organization and normal conduct of business may preclude a single large training program on new security procedures/technologies

- Thus, organization should conduct phased-in or pilot approach to implementation
Scope Considerations

- Project scope: concerns boundaries of time and effort-hours needed to deliver planned features and quality level of project deliverables

- In the case of information security, project plans should not attempt to implement entire security system at one time
The Need for Project Management

- Project management requires unique set of skills and thorough understanding of a broad body of specialized knowledge.

- Most information security projects require trained project manager or skilled IT manager versed in project management techniques.
The Need for Project Management
Supervising Implementation

- Some organizations may designate a champion from the general management community of interest to supervise the implementation of an information security project plan.

- An alternative is to designate a senior IT manager or CIO to lead the implementation.

- The optimal solution is to designate a suitable person from the information security community of interest.

- It is up to each organization to find the most suitable leadership for a successful project implementation.
Executing the Plan

- Negative feedback ensures project progress is measured periodically
  - Measured results compared against expected results
  - When significant deviation occurs, corrective action taken
- Often, project manager can adjust one of three parameters for task being corrected: effort and money allocated; scheduling impact; quality or quantity of deliverable
Negative feedback Loop

Plan is developed → Work occurs → Progress is measured

Complete?

Yes → Project is complete

No → On target?

Yes → Corrective action

No → Plan is developed
Project Wrap-up

- Project wrap-up is just as important as project planning.

- Good IT security installed during the project is wasted if not imparted to operations and maintenance activities.

- Collect documentation, finalize status reports, and deliver final report and presentation at wrap-up meeting.

- Goal of wrap-up to resolve any pending issues, critique overall project effort, and draw conclusions about how to improve process.
Summary

- IT Security is “baked in”, not “bolted on”
- IT Security is included in the first document and the first meeting of a project
- IT Security is included throughout the project
Bolt-On Solution