# Global Information Assurance Certification Paper

# Security Best Practices for IT Project Managers

*GIAC GSEC Gold Certification*

Author: Michelle Pruitt, michelle.pruitt@gmail.com

Advisor: Rich Graves

Accepted: June 18, 2013

## Abstract

IT Project Managers are responsible for guiding the implementation of new initiatives as well as upgrades to existing systems.

Considerable attention has been paid to incorporating security best practices into the software development life-cycle, i.e., security "baked-in" to code by various means. However, a large number of IT projects are not software development projects. Deliverables of outright security initiatives such as upgrades to network components will almost certainly receive the scrutiny of security experts but the project delivery methodology may not.

By including security considerations in every phase of a project, PMs have the opportunity to deliver more secure systems in a more secure manner.

Audience: Project managers that may not have detailed knowledge of security principles but are very familiar with project management principles.

# 1 Introduction

For a project manager, a bad week might go something like this:

- You open your email and see that one of your technical resources has inadvertently forwarded a network diagram to a competitor of your client.
- You're rolling out server builds during a weekend Go-Live and you realize your inventory spreadsheet is corrupted.
- You're about to walk into a meeting with your project sponsor and discover the laptop where you've stored the presentation you've been working on for three days has blue-screened.

Each scenario represents a security failure, a failure to maintain the CIA triad of information security:

- Confidentiality
- Integrity
- Availability

Project managers have special interests in all three components of the CIA triad.

*Information Security*

Information should be shared only with authorized persons, it should be verifiably authentic, complete, sufficiently accurate, trustworthy and reliable, and it should be accessible when needed.

IT projects warrant special consideration for maintaining confidentiality. The business case for any IT project will include strategic business goals whether the project delivers an exciting new technology or a mundane but essential upgrade to maintain enterprise productivity. IT project documentation also frequently includes intimate details of network and systems architecture that presents an attractive target for industrial espionage and hackers.

Failed changes to IT systems can also impact availability and integrity. Special attention to backups, back-out plans and security risks early in the project will pay big dividends when project rollout leaves little time to consider how to undo the changes made during a Go-Live or react to an unexpected risk occurrence that may cause systems to go down, or cause data loss, corruption or breach.

Michelle Pruitt, michelle.pruitt@gmail.com

Project managers should develop plans to mitigate risks to the project documentation and methodology itself. Do you really want to go into that big meeting with the project sponsor and not be able to access crucial files or find that the most recent version of the project issues log was overwritten with the previous week's version?

SANS has led the way in encouraging healthy security project management practice by encouraging the training of software developers to attend to security, providing education and certifications, etc. SANS recommends 20 critical security controls for the enterprise and provides advice for developing and implementing an enterprise security policy that will cover everything from end-user computing guidelines to O/S and networking configuration. It is incumbent upon the PM to be familiar with and to comply with the policy of all project sponsoring organizations. Although the primary audience for the SANS Critical Controls are CIOs and CISOs, the ultimate responsibility for implementation of the controls lies with technical teams. As PMs direct technical teams to accomplish project goals, they can leverage their awareness of the 20 Critical Controls to ensure their organization's system has the most secure baseline configuration possible (Center for Strategic & International Studies, 2013).


**Figure 1-1** Example project security plan milestones or checkpoints.

This paper will map information security checkpoints onto key PM processes, beginning with the important initiating and planning phases. We will then take a deeper dive into secure communications because of their critical role in project management and their inherent risk, and finally, we will review secure deliverables and operational handoff.

Michelle Pruitt, michelle.pruitt@gmail.com

# 2 Security integrated into PM methodology

The Project Management Institute defines a project as an iteratively elaborated endeavor (Project Management Institute, 2008) and security should be considered within each PM process or stage. Security checkpoints built in to the project during several key processes will ensure progress toward the desired security end state at project closure.

## 2.1 Baked-in Project Security

The best opportunity to ensure secure project delivery exists in the early stages of the project during initiating and planning. Beginning with the end in mind, i.e. the delivery of a secure system, will avoid costly scope, budget and schedule impacts.

### 2.1.1 Develop Project Charter

As Jeff Christianson noted in a 2003 SANS whitepaper: "True business value of a security solution is the amount of risk mitigation provided compared to the cost of solution implementation and maintenance" (Christianson, 2003).

A project that proposes to give a sales force access to data on their smart phones may be implemented very differently if security is considered as a basic requirement of the final deliverables rather than an afterthought to be addressed when security breaches occur after implementation. For example, if a particular smart phone that supports better security protocols becomes a requirement, cost and schedule may be impacted, but costly disclosures of intellectual property may be avoided.

The Ponemon Institute's seventh annual *U.S. Cost of a Data Breach Study* (Ponemon Institute, 2012) reported the average organizational costs of responding to a data breach were $4.5 million and lost business costs due to reputational damage, etc. were about $3 million. PMs can make a convincing case that security dollars will accomplish more if security is baked into the project from the outset, rather than applied as a Band-Aid to pass an audit during operational handoff, or worse, spent to recover from damage after a security incident.

A security impact analysis as part of a larger cost-benefit analysis should be executed during the initiation phase of every IT project to make a sound financial decision (Xie & Mead, 2004). Security can be considered part of the larger Cost of Quality of the project. Cost of Quality

includes both preventative measures and the costs of failure to create a quality product. In the context of security, preventative measures include just about everything that will be recommended in this paper, including planning, requirements collection, change management, risk management, and training. Additional internal costs will include appraisal costs to find quality problems such as inspections, tests and audits. The costs of failure include the costs to recover from a cyber-security incident like a data loss or theft. Those recovery costs would include external failure costs like loss of goodwill, lost sales, fines, liability costs, investigation of incidents and remediation as well as internal failure costs like wasted work, rework, and failed handoff to operations.

Calculating Annualized Loss Expectancy (ALE) attempts to quantify losses due to threats:

ALE = annual rate of occurrence (ARO) x single loss expectancy (SLE)

where SLE = asset value (AV) x exposure factor (EF)

ALE has been criticized as too inaccurate to be useful for information security risk calculations unless used with caution (Schneier, 2008). In fact, calculation of losses from cybercrime in general has been criticized as being grossly inaccurate (Maass & Rajagopalan, 2012.) Since security vulnerabilities are continuously evolving, it is difficult to quantify rates of occurrence. It is also difficult to estimate the damage to asset value that would be done in a single loss occurrence. However, in the absence of a better alternative, ALE can be used to estimate the value of security measures in terms of loss prevention and to prioritize mitigations when security risks are ranked.

Large organizations may have a project methodology that requires a security stage gate to be passed; small organizations may need to simply assign a capable reviewer to examine the project proposal at critical points in the project, especially prior to committing funds to the project.

### 2.1.2 Identify Stakeholders

A standard Interest vs. Influence stakeholder analysis matrix focused specifically on security considerations may be revealing. Identify the organizational security office, and find out if they have security sign-off on deliverables for your project. Analyze your sponsor's security attitude, especially if you anticipate the budget is inadequate for security. You may need to move key players higher on the security interest scale, including your project sponsor, technical teams and operations staff. Depending on the formality of the sponsoring organization, the PM may assign a standard list of security roles to project team members. Involving operations staff early in the project and soliciting their input on security requirements during planning will minimize the risk of last minute security fixes as the system rolls into production.

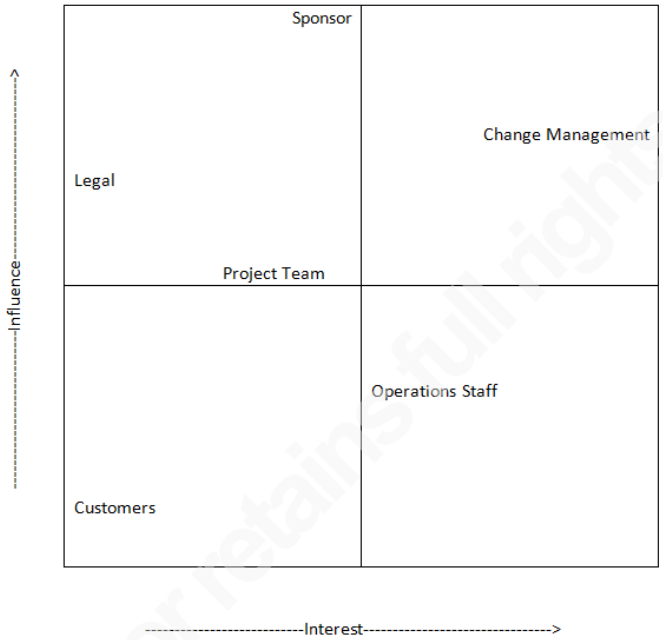


**Figure 2-1** Interest vs. Influence Stakeholder Matrix

### 2.1.3 Plan Communications

A recent report found over 126 billion files posted online by customers of Amazon's cloud computing service (Robertson, 2013), including confidential business information like sales records at an automobile dealership, computer source code, and spreadsheets with employee information. Amazon's service included a key security mechanism for protecting the information, but some users had deliberately or unintentionally disabled the default "private" setting on the files.

The bulk of a PM's work during the executing stage of a project has to do with communications. In fact, the PMBOK® (Project Management Institute, 2008) states that "Communication has been identified as one of the single biggest reasons for project success or failure." We will return for a deep dive into securing project communications in the next section of this paper, but the

communications plan is the first step toward ensuring information security during project execution.

A communications plan should include not only the method, frequency and audience for communications but may also consider guidelines and technical standards for a wide variety communication channels:

*Communications Plan – Sample Security Section*

All project communications will comply with the security policies of both [client organization] and [project management delivery organization]. In cases where policies overlap, the more restrictive policy will apply.

- Secure project document sharing that uses adequate encryption and access control for data transfers and storage.
- Telephone conference calls, including the requirement to password protect the meetings and/or use the roll call feature of the conferencing provider to ensure only those invited are on the line and periodically changing your meeting passcode, especially when a project closes.
- Distribution of meeting minutes and other project documents via email, including the availability of an encryption mechanism like PGP for sensitive emails.
- Instant messaging via a provider that meets your organization's security standards.
- Guidelines regarding forwarding work-related email to personal cell phones and what information is acceptable to be left in voice mailboxes and in auto-responders.
- Desktop or application sharing/video conferencing via an approved provider.
- Regular backups to guard against data loss due to computer crashes or user error.
- Guidelines for use of social media.

### 2.1.4 Develop Project Team

In 2002, the New York Times reported that the law firm handling the bankruptcy of Global Crossing inadvertently identified more than 50 potential and confidential bidders to each other simply by sending an email to all of them without using the blind carbon copy option ("Global Crossing confidential bidding compromised," 2002). Perhaps the most likely risk during project execution is inadvertent data leakage via one of the myriad of communication channels PMs utilize everyday: email, phone, VOIP, IM, numerous options for document sharing including

cloud collaboration, and the newest threat to information security, social media (Shullich, 2011) (Gordon, 2007).

The ideal defense against inadvertent data leakage is a project team that is aware of the risk and uses secure information systems intelligently. Failing that, security training may help (Brodie, 2009) (Rashid, 2013). A review of the communications plan at a team kickoff meeting can set expectations. Periodic reviews of the plan will remind team members of their critical role in project security. Free basic employee training materials are available from the National Cyber Security Alliance on their "Stay Safe Online" web site at http://www.staysafeonline.org/business-safe-online/train-your-employees. SANS offers a free trial subscription to their "Securing the Human" end user awareness training materials at http://www.securingthehuman.org/.

### 2.1.5 Plan Risk Management

Of the 42 PMI® project management processes, "Plan Risk Management" often gets less attention than, say, "Create Work Breakdown Structure" or "Estimate Costs," but information security, and ultimately project management, are fundamentally about risk management. A malware attack may or may not occur during your project; a resource may or may not be available when scheduled; how much time and money should be dedicated to reducing the negative impact of an uncertain event? Risk management attempts to qualify and quantify potential impacts and choose effective mitigation strategies.

> True business value of a security solution is the amount of risk mitigation provided compared to the cost of solution implementation and maintenance.
>
> (Christianson, 2003.)

Qualitatively, organizations may have particular risks they tend to avoid; for example, organizations subject to HIPAA regulations will avoid loss of protected data. Quantifying security risk is even more challenging and numerous models and techniques are available (Wright, 2011) (Poole, 2009). Sources of statistics for quantifying risk include annual reports from Symantec (Symantec, 2012), Mandiant and the Ponemon Institute. Technical experts designing an IT system will likely use more sophisticated techniques for risk analysis than the

PM will use to manage risks to the project, but both aspects of risk management are essential to successful project delivery.

Each IT security risk to a project may require custom estimates. As an example, consider the potential impact of a data breach during project execution. According to the Association of Privacy Professionals, four factors are most important in determining the likelihood that a breach of private consumer data will result in litigation: data type, breach cause, evidence of misuse and size of incident (Phan, 2012).

These four general factors may also be useful for evaluating the impact of a breach for other types of IT data. More valuable data such as account names and passwords or network details will have higher impact than publicly available email addresses. Information stolen by bad actors will likely have higher impact than information inadvertently misdirected. Information that is actively misused will have higher impact than information stolen with no evidence of intent to misuse. And loss of larger amounts of data will be higher impact than smaller amounts of data.

The U.S. National Institute of Standards and Technology (NIST) has developed a technique for quantifying and comparing IT security risk levels called Probabilistic Attack Graphs which analyzes attack paths through a network and applies probabilities that vulnerabilities can be exploited (Jackson, 2011) (Singhal & Ou, 2011).

The "Practical Risk Analysis and Threat Modeling Spreadsheet" available on the SANS Windows Security Blog (Fossen, 2009) is a relatively straightforward starting point for a PM to list threats and mitigations, and to estimate overall risk to the project using a some or all of seven factors including damage to reputation and productivity, exploitability, and legal liability.

## 2.2 Secure Communications

Communication is at the heart of project management and every communication channel carries the risk of exposing confidential data. An email sent to the wrong person or worse, distribution list, a team member that stores project documents with an insecure cloud provider, a smart phone lost on the bus, a laptop left in a hotel room, the list runs the gamut from the mundane to episodes worthy of inclusion in the next installment of the Bourne franchise (Crawley, 2013).

Something as simple as neglecting to sanitize internal document meta-data before forwarding to external customers runs the risk of exposing confidential information (Pesce, 2008).

Mandiant, a cybersecurity firm that focuses on targeted attacks, detects and studies the tactics of dozens of "Advanced Persistent Threat" (APT ) actors worldwide, many located in China. APT groups are large, well-organized, and well-funded, sometimes by national military organizations. Their mission is to methodically gather broad categories of intellectual property like business plans, email addresses and contact lists of organizational leadership, technology blueprints, and proprietary manufacturing processes. According to Mandiant's 2013 annual report, attackers frequently steal data to make reconnaissance faster, like network infrastructure data and sysadmin guides. In particular, VPN configuration files, systems documentation, and network documentation like firewall configuration files are specifically targeted during reconnaissance (Mandiant, 2013).

IT project managers often handle intellectual capital that is the equivalent of the keys to the kingdom. IT project records are a rich source of valuable documents and due to the temporary and fast-moving nature of project work, access controls and records systems may not be maintained after the project closes and the team moves on. Industrial espionage targets blue chip companies and small and mid-sized businesses have also been targeted, especially as easy targets for banking fraud, so no organization is immune to the threat (Gonsalves, 2012) (Richmond, 2010) (Mandiant, 2013).

**How Secure is email?**

Is email really intercepted and used for nefarious purposes? Here are two much more likely and equally damaging scenarios:

1. An authorized recipient inadvertently forwards a confidential email to someone that is not authorized to see it. See "Global Crossing confidential bidding compromised," 2002.

2. A personal smart phone configured to access internal company emails is lost or stolen. 81% of recent survey respondents said that they allow personal devices to access company data (BYOD or Bring Your Own Device policy) Less than 50% of smartphone users have password protection on their devices ("Survey shows," 2011).

So while you may want to have an email encryption tool like PGP available for extremely sensitive emails, you need two more fundamental tools to close the email security gap: a policy that ensures only secure devices are allowed to access internal data, including email, and educated end users that avoid emailing sensitive information altogether, even internally, if it is avoidable.

Michelle Pruitt, michelle.pruitt@gmail.com

### 2.2.1 Authentication and Password Management

Mandiant reports that 100% of breaches by advanced persistent threat "bad actors" involve stolen credentials. Read that again: 100% of breaches involve stolen credentials (Mandiant, 2013). Popular security blogger Brian Krebs frequently writes on the topic of the value of stolen data. On Krebs on Security, he says "nearly every aspect of a hacked computer and a user's online life can be and has been commoditized" (Krebs, 2012). The argument that "no one would be interested in my data" has been thoroughly debunked. Hackers market lists of stolen credentials for online retailers by the gigabyte. Credentials for critical systems are a prized commodity.

In February 2013, popular cloud service Evernote was hacked and usernames, emails and encrypted passwords were stolen in a "coordinated attempt" to steal user data (Davies, 2013). LinkedIn, Yahoo, and Twitter are just a few of the many sites which have been high profile victims of password stealing attacks. Passwords that are reused on a variety of sites and are never changed are a big security risk.

- Use long, complex passwords.
- Don't reuse passwords on multiple web sites or for multiple accounts.
- Change passwords periodically.
- Use a password manager so you can choose difficult to guess and unique passwords for each account.
- Use two-factor authentication where appropriate.

### 2.2.2 Access Management

Members of the project team should have the access they need and only the access they need to systems. In the name of speed, credentials are sometimes handed out fast and loose. Defining and documenting a clear system for onboarding and off-boarding personnel will not only improve efficiency of these processes but also ensure credentials are current. Team member access rights need to be reviewed and updated periodically. If people leave the project or company, access should be revoked.

- Document and use secure onboarding and off-boarding procedures.
- Schedule periodic reviews of access permissions.

Michelle Pruitt, michelle.pruitt@gmail.com

### 2.2.3 Encryption

Encryption protects sensitive and valuable data at rest and in motion by transforming plaintext into coded form referred to as ciphertext. Encryption is an almost invisible part of many communications protocols, including web browsing, email, instant messaging, VoIP. Encryption can be especially valuable for storage of data as another layer of protection against data theft or breaches on cloud infrastructure or mobile devices.

The ease and convenience of cloud storage brings new challenges, including inadvertent data leakage during storage or transfer or even through deliberate data harvesting by the cloud provider, and challenges for the availability of project records.

According to the report "Securing Outsourced Consumer Data" by the Ponemon Institute and sponsored by the credit reporting agency Experian (Krenek, 2013), it's a mistake to choose a cloud vendor based solely on quality of service and price if their privacy and security standards are not adequate. Of the survey respondents, 65% reported that their organization had experienced a breach of outsourced consumer data. The vendor should provide verifiable evidence that data is secure on their infrastructure like security certifications that require audits of their practices with respect to NIST and FISMA standards by accredited organizations like Logyx and Veris group, or via STAR or FedRAMP certs (Trappler, 2013) (U.S. General Services Administration, 2013).

Make sure you are familiar with and understand the disaster recovery provisions, privacy terms and conditions, and long-term financial viability of the cloud provider before storing project records in the cloud (Rao, 2012).

Cloud storage providers like Microsoft and Amazon have responded to being hacked by improving their default security configuration (Tajadod, Batten & Govinda, 2012). However, even strong encryption is only as secure as the password(s) used to unlock the encryption. In 2011, a code update at Dropbox allowed anyone to login to any account using any password for a period of four hours (Ferdowsi, 2011).

Data on mobile devices like laptops and smart phones should be secured with encryption plus strong authentication since they are frequently lost or stolen. The National Institute of Standards

and Technology publishes a Cryptographic Toolkit (U.S. NIST, 2013) on their website with cryptographic algorithms that meet NIST's crypto standards.

- Protect data in the cloud or on mobile devices with encryption.
- Enforce strong authentication policies for accessing encrypted data.
- Transmit data only with secure protocols.

### 2.2.4 Wireless Attacks

Road warriors will undoubtedly have been faced with the question of whether connecting to a hotel, airport or coffee shop wireless connection is "safe." Connecting to an open wireless network provides a fat attack surface, including the possibility of bad actors potentially intercepting transmitted information, compromising the computer or smart device, or harvesting passwords or information about secure corporate VPN or wireless systems due to unsecured behavior of the wireless card.

Handhelds like smart phones hold and transmit rapidly increasing amounts of data and deserve special scrutiny since they are easily and frequently lost or stolen and have in many cases minimal built-in provisions for security. If they do not conform to company security policies for passwords, encryption and virus protection they should not have access to company data, including email and voice messaging (Horwath, 2013). The most common cause of data breaches due to smartphones is a lost device.

The U.S. Federal Communications Commission released a "Smartphone Security Checker" in December 2012 which is available at: http://www.fcc.gov/smartphone-security.

- Require a secure configuration and security measures for all devices accessing internal data, especially smartphones and laptops, including: data encryption, password protection, anti-virus software and remote wipe ability.
- Restrict end user administrative permissions.
- Avoid using unsecured wireless networks in coffee shops, hotels and airports. If using unsecured networks is unavoidable, use VPN or another secure tunnel to access all data.
- Keep smartphone software up-to-date by enabling automatic updates.

- Backup smartphone data periodically to avoid losing data, especially contacts, if the device is lost, stolen or damaged.

### 2.2.5 Physical security

If your employer or client has locations in several countries, it is likely they are an attractive target for intellectual property theft or industrial espionage. During foreign travel, especially to certain countries, any work-related information on your laptop or smart phone will require special consideration for maintaining the confidentiality of that information. The U.S. Department of State warns travelers to China that computers left in hotel rooms may be searched for trade secrets, negotiating positions, and other business-sensitive information (U.S. Department of State, 2013). Law firms in particular have been targeted by hackers to harvest business intelligence on their clients, both at home and abroad (Cohen, 2013). Checked baggage should never contain papers or devices carrying confidential information.

At home, physical security for project records should include not only physical access to the electronic systems that store data such as laptops but also physical access to printouts and paper filing systems. Recycling bin, printer and fax output trays and filing cabinets all need to be covered by security policy. Sensitive documents should never be left unattended in insecure locations and should be shredded with cross-cut shredders when disposed of. In a famous example of destroyed documents being physically reconstructed, Iranian women stitched shredded documents back together after student protesters took over the U.S. Embassy in Tehran in 1979. Commercial software can now digitally reassemble most documents shredded on popular and inexpensive strip shredders ("Unshredder," 2013).

- Secure hard copies of data in file cabinets, on fax machines, in printer trays and in waste baskets/shredders.
- Use security cables.
- Educate travelers about risks of theft and data leakage.

## 2.3 Secure Deliverables

### 2.3.1 Collect Requirements

Requirements gathering is a critical stage for project security. Security requirements should consider the sponsoring organization's security policy and regulatory environment. The PMBOK® (Project Management Institute, 2008) notes that security requirements may impact project costs via the scope baseline and procurements.

Requirements elicitation is often not straight-forward; security requirements elicitation may be even less well-defined. A systematic approach may help to achieve a consistent, complete set of security requirements. The "Build Security In" web site sponsored by the U. S. Department of Homeland Security Office of Cybersecurity and Communications provides a number of papers on the topic of requirements engineering for software (Mead, 2006). Recommended requirements elicitation, analysis, prioritization and evaluation methods may be useful for more general IT projects as well, such as focused interview questions, using checklists, and weighting schemes.

SANS SCORE (Security Consensus Operational Readiness Evaluation) provides CIS security configuration benchmarks for hardening O/S, middleware, software and network devices on the cisecurity.org website: http://www.sans.org/score/benchmark.php The Common Criteria Recognition Arrangement (CCRA) publishes Protection Profiles which may provide an initial set of questions for review to elicit requirements accepted by a large number of government signatories (Common Criteria Recognition Arrangement, 2013). The U.S. National Institutes of Standards and Technology (NIST) provides publicly available security checklists on setting the security configuration of operating systems and applications at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository. Some benchmarks are available for automated scanning during operational handoff with SCAP (Security Content Automation Protocol) tools listed at http://nvd.nist.gov/scapproducts.cfm.

### 2.3.2 Monitor and Control Risks - Change Control

Information security is often identified only with hackers and malware, but basic system availability is impacted by a much broader category of events, including planned and even routine system changes. PMs tend to leave technical change management to their technical

teams. However, technical change management presents risks to information security availability and integrity and PMs should be familiar with its risks and mitigation of those risks.

If a system goes down during a Go-Live event and adequate time has not been reserved to back out changes, the availability of the system to support business functions is compromised. A good change control plan will include enough time to make all changes and complete testing, plus enough time to roll back all changes if the system doesn't pass operational or functional tests at scheduled checkpoint(s).

Similarly, information integrity is at risk if adequate measures aren't in place to backup and then restore data from backup during the change window if necessary.

Changes should be evaluated on a risk matrix, i.e., probability vs. impact, based on impact urgency, risk, benefits and costs, and managed to minimize impacts to business needs (Cisco, 2012). Change windows should have longer lead times and be larger for higher risk changes.

### 2.3.3 Verify Deliverables - Operational hand-off

Operations may expect the project delivery team to deliver an inherently secure system, while the project delivery team may expect security to be the responsibility of operations management after the system is handed off. Consideration should be given to when and how security concerns are most efficiently and effectively addressed in the total system lifecycle, not just during project delivery (Scheessele, 2007) (Rodgers, 2002). Ownership of security should rest with the project manager to the extent that the initial system setup is securable.

"An organization can either incorporate security guidance into its general project management processes or react to security failures." says Robert Ellison of Carnegie Mellon University (Ellison, 2006). If security has been included in requirements gathering with input from the operations team, operational hand-off will be organized around verifying security deliverables as specified and transferring ownership rather than reacting to security problems identified by operations staff as the system is being put into production.

Operational Acceptance Testing checklists (Moraetes, 2009) for non-functional components of a system (i.e., quality attributes such as performance, availability, and reliability) like

backup/recovery, maintenance and security can guide the hand-off and ensure that operations staff have the documentation and verified configurations they need to support the system.

### 2.3.4 Document Lessons Learned

In the excitement of a completed project and the usual pressure to move on to a new one, it may be often overlooked, but capturing lessons learned is an important part of building Organizational Process Assets and your security expertise as a PM. War stories can be one of the most effective ways to motivate secure behaviors and to establish a culture of security in your organization over the long-term. Any security experiences, risks or threats that materialized or not should be noted in the risk register and documented for future project evaluation and planning.

## 2.4 Conclusion

A good week for a project manager might look something like this:

- You open your email and see that one of your technical resources has flagged an email containing a network diagram as confidential, preventing it from being forwarded to a competitor of your client.
- You're rolling out server builds during a weekend Go-Live and you realize your inventory spreadsheet is corrupted. Your change window gives you time to retrieve a pristine copy of the inventory from backup, verified with your document versioning system, and your team completes the builds successfully.
- You're about to walk into a meeting with your project sponsor and discover the laptop where you've stored the presentation you've been working on for three days has blue-screened. An authorized member of Operations Staff you've been working with closely since requirements gathering pulls up the file in the encrypted cloud storage backup for you and the presentation continues as planned.

PMs are not expected to be security experts, but by including security considerations in every phase and process of a project, especially in initiating and planning, communications and deliverables, PMs have the opportunity to deliver more secure systems in a more secure manner.

Basic familiarity with SANS' 20 critical security controls (Center for Strategic and International Studies, 2013) for the enterprise is a good place to start to build expertise. Almost every IT

project will impact or be impacted by the critical controls. As PMs direct technical teams to accomplish project goals, they can leverage their awareness of the 20 Critical Controls to ensure their organization's IT systems have the most secure baseline configuration possible.

### 2.4.1 Resources

SANS recommends 20 critical security controls (Center for Strategic and International Studies, 2013) for the enterprise and provides advice for developing and implementing an enterprise security policy that will cover everything from end-user computing guidelines to O/S and networking configuration. SANS also provides standards for information security practices on the SANS web site here: http://www.sans.org/reading_room/whitepapers/standards/

| # | **SANS 20 Critical Controls** | **Possible PM Applicability**<br><br>(including processes, enterprise environmental factors, organizational process assets) |
|---|---|---|
| 1 | Inventory of Authorized and Unauthorized Devices | Plan Communications |
| 2 | Inventory of Authorized and Unauthorized Software | Plan Communications |
| 3 | Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers | Gather Requirements |
| 4 | Continuous Vulnerability Assessment and Remediation | Operational handoff documents |
| 5 | Malware Defenses | Develop Project Team |
| 6 | Application Software Security | Gather Requirements |
| 7 | Wireless Device Control | Plan Communications |
| 8 | Data Recovery Capability | PMIS, Gather Requirements, Back-out planning |
| 9 | Security Skills Assessment and Appropriate Training to Fill Gaps | Team building, ground rules, staffing expertise, training |

| | | |
|---|---|---|
| 10 | Secure Configurations for Network Devices such as Firewalls, Routers, and Switches | Gather Requirements |
| 11 | Limitation and Control of Network Ports, Protocols, and Services | Gather Requirements |
| 12 | Controlled Use of Administrative Privileges | Technical team entitlements |
| 13 | Boundary Defense | Organizational process assets |
| 14 | Maintenance, Monitoring, and Analysis of Audit Logs | Organizational process assets |
| 15 | Controlled Access Based on the Need to Know | Technical team entitlements |
| 16 | Account Monitoring and Control | Organizational process assets |
| 17 | Data Loss Prevention | PMIS, Communications |
| 18 | Incident Response and Management | Organizational process assets |
| 19 | Secure Network Engineering | Gather Requirements |
| 20 | Penetration Tests and Red Team Exercises | Organizational process assets |

### 2.4.2 IT Project Security Checklist

**Initiating:**

- ✓ Does the project impact the security stance of the organization for better or worse?
- ✓ Does security impact the cost/benefit of the project?
- ✓ Which stakeholders have sign-off on security deliverables?

**Planning:**

- ✓ Consider security aspects of schedule, cost, scope. Do your deliverables have special security considerations that may impact schedule and costs?
- ✓ Consider security risks: which threats are most likely to occur and have the largest impacts? Has a formal risk management plan been created?
- ✓ Does your project management information system (PMIS) include provisions for availability and appropriate access to all members of the team?

- ✓ Does your communication plan specify the use of secure systems for project communications?
- ✓ Is there a high-availability communications plan to deal with technology failures and personal emergencies during critical Go-Live activities?

**Executing:**

- ✓ Are documents stored securely using encryption and strong, unique password(s)? Are documents backed up regularly? Are backups tested?
- ✓ Are communications secured via meeting passcodes? Do all devices used to access email have secure configurations including encryption and passwords, especially mobile devices?
- ✓ Do resources have the access they need and only the access they need to sensitive systems? Is access revoked when no longer needed?
- ✓ Is the team aware of and accountable for project security? What training or ground rules apply?
- ✓ Do deployments, implementations/cutovers have carefully documented backout plans to avoid availability and integrity failures?

**Monitoring and Controlling:**

- ✓ Are risks and mitigations periodically reviewed with the technical team and other stakeholders?
- ✓ Are deliverables validated for security requirements?
- ✓ Is system security stance verified at operational hand-off?

**Closing:**

- ✓ Are security lessons learned captured and shared with your organization?

Michelle Pruitt, michelle.pruitt@gmail.com

# 3 References

Brodie, C. (2009). The Importance of Security Awareness Training. *SANS Institute Reading Room.* Retrieved May 28, 2013 from http://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013

Center for Strategic and International Studies. (2013). *Twenty Critical Security Controls for Effective Cyber Defense: Version 4.1.* Retrieved May 22, 2013 from http://www.sans.org/critical-security-controls/guidelines.php

Cisco. (2013). Change Management: Best Practices. *Cisco Corporation.* Retrieved May 13, 2013 from http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.html

Christianson, J. (2003). Cryptography – Business Value Behind the Myth. *SANS Institute Reading Room.* Retrieved May 15, 2013 from http://www.sans.org/reading_room/whitepapers/vpns/cryptography-business-myth_1236

Cohen, A. (2013). Data security for lawyers traveling to China. *The American Lawyer*. Retrieved February 12, 2013 from The Corporate Counsel website: http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1359312802334&thepage=1

Common Criteria Recognition Arrangement. (2013). *Official CC/CEM Versions: Protection Profiles.* Retrieved May 28, 2013 from http://www.commoncriteriaportal.org/pps/

Crawley, J. Matt Damon Would "Consider Revisiting Bourne Franchise." (January 3, 2013). *Entertainment Wise.* Retrieved May 28, 2013 from http://www.entertainmentwise.com/news/99915/Matt-Damon-Would-Consider-Revisiting-Bourne-Franchise

Davies, C. (2013). Evernote hacked: emails, encrypted passwords stolen. *Slash Gear.* Retrieved April 29, 2013 from http://www.slashgear.com/evernote-hacked-emails-encrypted-passwords-stolen-02272197/

Ellison, R. (2006). Security and project management. *Build Security In (BSI) portal , U.S. Department of Homeland Security (DHS), National Cyber Security Division*. Retrieved January 23, 2013 from https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/project/38-BSI.html

Michelle Pruitt, michelle.pruitt@gmail.com

Federal Communications Commission. (2012). *FCC Releases New "Smartphone Security Checker" To Help Consumers*. Retrieved May 10, 2013 from http://www.fcc.gov/document/fcc-releases-new-smartphone-security-checker-help-consumers

Ferdowsi, A. (2011). Yesterday's Authentication Bug. *The Dropbox Blog.* Retrieved May 8, 2013 from https://blog.dropbox.com/2011/06/yesterdays-authentication-bug/

Fossen, J. (2009). Practical Risk Analysis and Threat Modeling Spreadsheet. *SANS Windows Security Blog.* Retrieved May 10, 2013 from http://www.sans.org/windows-security/2009/07/11/practical-risk-analysis-spreadsheet

Global Crossing confidential bidding compromised by an errant "reply to all." (April 10, 2002) *The Street*. Retrieved April 14, 2013 from http://www.thestreet.com/story/10016536/1/law-firm-reportedly-reveals-global-crossing-suitors.html

Gonsalves, A. (2012). Hackers increasingly zero in on small businesses, Symantec says. *CSO Online.* Retrieved May 28, 2013 from http://www.csoonline.com/article/712942/hackers-increasingly-zero-in-on-small-businesses-symantec-says

Gordon, P. (2007). Data Leakage – Threats and Mitigation. *SANS Institute Reading Room.* Retrieved February 15, 2013 from http://www.sans.org/reading_room/whitepapers/awareness/data-leakage-threats-mitigation_1931

Horwath, J. (2013). Managing the Implementation of a BYOD Policy. *SANS Institute Reading Room.* Retrieved May 10, 2013 from http://www.sans.org/reading_room/whitepapers/leadership/managing-implementation-byod-policy_34217

Jackson, W. (2011). New technique maps attack paths to quantify cyber risk. *GCN (Government Computing News).* Retrieved May 22, 2013 from http://gcn.com/Articles/2011/10/04/NIST-attack-graphs-measure-cyber-risks.aspx?Page=1

Krebs, B. (2012). Exploring the Market for Stolen Passwords. *Krebs on Security.* Retrieved on April 29, 2013 from http://krebsonsecurity.com/2012/12/exploring-the-market-for-stolen-passwords/

Michelle Pruitt, michelle.pruitt@gmail.com

Krenek, B. (2013). Secure your outsourcing practices to prevent data breaches. *Experian Data Breach Resolution Blog.* Retrieved April 29, 2013 from http://www.experian.com/blogs/data-breach/2013/04/15/secure-your-outsourcing-practices-to-prevent-data-breaches/

Maass, P. & Rajagopalan, M. (2012.) Does Cybercrime Really Cost $1 Trillion? *ProPublica.* Retrieved June 16, 2013 from http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

Mandiant. (2013). M-Trends® 2013: Attack the Security Gap™ . *Mandiant*. Retrieved April 14, 2013 from https://www.mandiant.com/resources/m-trends.

McAfee. (2012). McAfee Threats Report: Fourth Quarter 2012. *McAfee.* Retrieved May 10, 2013 from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012.pdf

Mead, N. (2006). Requirements Elicitation Case Studies Using IBIS, JAD, and ARM. *Build Security In (BSI) portal , U.S. Department of Homeland Security (DHS), National Cyber Security Division.* Retrieved May 13, 2013 from https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/requirements/532-BSI.html

Mead, N. (2006). Requirements Elicitation Introduction. *Build Security In (BSI) portal , U.S. Department of Homeland Security (DHS), National Cyber Security Division.* Retrieved May 13, 2013 from https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/requirements/533-BSI.html

Moraetes, G. (2009). A Risk Assessment Checklist for Small Business. *CompTIA.* Retrieved May 28, 2013 from http://www.comptia.org/Libraries/ME-Misc/The_Purpose_of_Developing_Security_Checklists.sflb.ashx

National Institute of Standards and Technology. (2013). Cryptographic Toolkit. *U.S. NIST Information Technology Laboratory.* Retrieved April 29, 2013 from http://csrc.nist.gov/groups/ST/toolkit/index.html

Phan, K. (2012). Assessing risk: Data breach litigation in U.S. courts. *The Privacy Advisor: The Official Newsletter of the International Association of Privacy Professionals.* Retrieved May 6, 2013 from https://www.privacyassociation.org/publications/2012_11_01_assessing_risk_data_breach_litigation_in_u.s._courts

Michelle Pruitt, michelle.pruitt@gmail.com

Poole, E. (2009). Quantifying Business Value of Information Security Projects. *SANS Institute Reading Room*. Retrieved June 16, 2013 from http://www.sans.org/reading_room/whitepapers/leadership/quantifying-business-information-security_33149.

Ponemon Institute. (2012). *U.S. Cost of a Data Breach Study.* Retrieved May 6, 2013 from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Ponemon Institute (2012). *Third Annual Benchmark Study on Patient Privacy & Data Security.* Retrieved May 10, 2013 from http://www2.idexpertscorp.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf

Project Management Institute. (2008). A guide to the project management body of knowledge (PMBOK® Guide) (Fourth Edition). Newtown Square: Project Management Institute.

Rao, V. (2012). Nine Challenges in Project Management Clouds. *Project Management Institute Voices on Project Management blog.* Retrieved February 18, 2013 from http://blogs.pmi.org/blog/voices_on_project_management/2012/06/9-challenges-in-project-manage.html

Rashid, F. (2013). Security Awareness Training Debate: Does it Make a Difference? *Security Week.* Retrieved May 28, 2013 from http://www.securityweek.com/security-awareness-training-debate-does-it-make-difference

Richmond, R. (2010). Wanted: Defense Against Online Bank Fraud. *Wall Street Journal.* Retrieved May 28, 2013 from http://online.wsj.com/article/SB10001424052748703483604574630690362605018.html

Robertson, J. (2013). How Private Data Became Public on Amazon's Cloud. *Bloomberg.* Retrieved April 14, 2013 from: http://www.bloomberg.com/news/2013-03-26/how-private-data-became-public-on-amazon-s-cloud.html

Rodgers, D. (2002). Implementing a Project Security Review Process within the Project Management Methodology. *SANS Institute Reading Room.* Retrieved January 8, 2013 from http://www.sans.org/reading_room/whitepapers/modeling/implementing-project-security-review-process-project-management-methodology_987

Scheessele, E. (2007). Building a Security Practice within a Mixed Product-R&D and Managed-Service Business. *SANS Institute Reading Room*. Retrieved February 5, 2013 from

http://www.sans.org/reading_room/whitepapers/bestprac/building-security-practice-mixed-product-r-d-managed-service-business_1831

Schneier, B. (2008). Security ROI. *Schneier on Security Blog.* Retrieved June 16, 2013 from http://www.schneier.com/blog/archives/2008/09/security_roi_1.html

Shullich, R. (2011). Risk Assessment of Social Media. *SANS Institute Reading Room.* Retrieved February 18, 2013 from http://www.sans.org/reading_room/whitepapers/privacy/risk-assessment-social-media_33940

Singhal, A. & Ou, X. (2011). Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs (NIST Interagency Report 7788). *U.S. Department of Commerce, National Institute of Standards and Technology.* Retrieved May 22, 2013 from http://csrc.nist.gov/publications/nistir/ir7788/NISTIR-7788.pdf

Survey shows smartphone users choose convenience over security. (2011). *Confident Technologies.* Retrieved May 10, 2013 from http://confidenttechnologies.com/news_events/survey-shows-smartphone-users-choose-convenience-over-security

Tajadod, G., Batten, L., & Govinda, K. (2012). Microsoft and Amazon: A comparison of approaches to cloud security. *2012 IEEE 4th International Conference on Cloud Computing Technology and Science.*

Trappler, T. (2013). Certification programs are making it easier to know all about a cloud vendor. *Computerworld.* Retrieved April 29, 2013 from http://www.computerworld.com/s/article/9235506/Certification_programs_are_making_it_easier_to_know_all_about_a_cloud_vendor

Unshredder: The first commercial document reconstruction tool in the world. Retrieved April 29, 2013 from http://www.unshredder.com/www/407/1001127/default.asp

U. S. Department of State. (2013). *China: Country Specific Information.* Retrieved May 24, 2013 from http://travel.state.gov/travel/cis_pa_tw/cis/cis_1089.html#special_circumstance

U. S. General Services Administration. (2013). *FedRAMP Accredited 3PAOs.* Retrieved April 29, 2013 from http://www.gsa.gov/portal/content/131991

Wright, C. (2011). A preamble into aligning Systems engineering and Information security risk. *SANS Institute Reading Room.* Retrieved February 18, 2013 from

http://www.sans.org/reading_room/whitepapers/riskmanagement/preamble-aligning-systems-engineering-information-security-risk_33891

Xie, N., & Mead, N. (2004). *SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies* (CMU/SEI-2004-TN-045). Retrieved May 28, 2013, from the Software Engineering Institute, Carnegie Mellon University website: http://www.sei.cmu.edu/library/abstracts/reports/04tn045.cfm