SAIS 2016 Proceedings | Southern (SAIS)

2016

A Process Framework for Managing Cybersecurity Risks in Projects

Steven S. Presley
University of South Alabama, ssp1521@jagmail.southalabama.edu

Jeffrey P. Landry
University of South Alabama, jlandry@southalabama.edu

CONSIDERATIONS FOR MANAGING CYBERSECURITY RISKS IN PROJECTS

Steven S. Presley
University of South Alabama
ssp1521@jagmail.southalabama.edu

Jeffrey P. Landry
University of South Alabama
jlandry@southalabama.edu

ABSTRACT

This paper builds on the need for earlier and earlier consideration of cybersecurity risks in the information systems life cycle by focusing on how cybersecurity threats apply to project execution, and whether the project manager should become more cyber-aware. Recent high-profile cases and decisions by the United States Department of Defense (US DoD) support early identification and analysis of cyber security risks. While the authors found no current academic research linking cybersecurity risks and project management, they did find a link between cybersecurity and information technology supply chain management. The paper makes the case for early cybersecurity risk management, and suggests that project managers broaden their awareness of cybersecurity risks. Future directions in the examination of early cybersecurity risks in projects are explored.

Keywords

Project management, project risk, cybersecurity, cyberattacks, Project Management Institute (PMI), United States Department of Defense (DoD)

INTRODUCTION

Cybersecurity threats are increasingly recognized as a significant concern for projects undertaken by private businesses and government organizations. Reports of security breaches and criminal misconduct can be seen daily in major news sources. Recent high-profile events have highlighted the risks that cybersecurity threats can pose to any project and their stakeholder organizations (Rushe, 2015; Rieder, 2014; Perez and Wallace, 2014; Basu, 2105). Evidence indicates that cybersecurity threats are not slowing but increasing. The number of cyberattacks worldwide increased by 25% in 2013, and in that same year, four of the 10 largest data breaches in Internet history occurred (Hendershot, 2014).

Recent evidence suggests that cybersecurity threats are becoming a concern earlier in the information systems life cycle. This paper examines three lines of evidence, exploring the issue of whether cybersecurity risk management should take place early, and how early. Specifically, we address the question,

Are cybersecurity threats a significant concern for IS projects and project managers?

The question is an important one because it identifies a major, common information systems activity—project management—targeting it as a potential soft spot for cyberattacks. It is not only a “when” question (during projects) but also a “what” question (what assets are vulnerable and what attacks should we be concerned about) and a “who” question (who are the attackers and who is responsible for early cybersecurity). If vulnerable, projects should be subject to enhanced cybersecurity risk management, and further research into cybersecurity issues in project management would be warranted. These issues would include the when, what, and who questions for future discovery.

DIRECT CYBERSECURITY THREATS AS RISKS TO EXECUTION AND DELIVERABLES

There is evidence that cybersecurity threats pose risks to projects in terms of both project execution as well the project deliverables (Hendershot, 2014; US DoD, Sept. 2015). Any cybersecurity risk that would affect an organization can also affect projects within that organization. For example, most projects depend on the same enabling technology resources to carry out project tasks (e.g. - mobile devices, infrastructure, networks, and workstations) that are also used for other business activities. If these devices are disabled or compromised, impacts to the project will be unavoidable and may be disastrous. Security controls at the organization level, such as two-factor authentication, may be needed to mitigate specific project risks (Hendershot, 2014).

The deliverables of a project may also be vulnerable to cybersecurity risks, and this becomes a concern for the project manager as well. For example, a decision to source components for a new product from a supplier with competing interests can result in serious cybersecurity risks. For example, in 2012 researchers discovered that microchips designated for military use had security backdoors allowing for theft of intellectual property and possible introduction of malicious code (Skorobogatov and Woods, 2012).

PROJECT RISK FROM CYBERATTACKS ON SUPPLY CHAIN

Any project involving the creation of a new product or service will require the acquisition of resources, including human resources. Recent attacks at Target (Vijayan, 2014) have demonstrated that outside suppliers may be a source of risk related to cybersecurity that should be considered by the project manager. Projects consist of insiders such as members of the user group or the project team with access to potentially sensitive information and systems that they otherwise might not have access to once the system is fully deployed.

ACADEMIC RESEARCH ON SUPPLY CHAIN SECURITY

Academic research also supports the idea. The supply chain has emerged as a potential area of vulnerability to cybersecurity risks in recent studies (Windelburg, 2016; Boyson 2014). Upton and Creese (2014), researchers in the area of insider threats, state that several sources estimate at least 80 million such incidents per year, with costs in the tens of billions.

Many projects also involve the integration of components from various suppliers. This also has been shown to a source of risk for the project and the project deliverables. A widely-publicized 2012 study by Skorobogatov and Woods (2012) demonstrated that adversaries could inject “back doors” into the design of integrated circuits, such that the introduction of malicious code such as Trojans, or even the disabling of the chip, would be possible. The vulnerable chips were the “ProASIC3 chip (which) is used in medical, automotive, communications and consumer products, as well as military use”. This is a risk for many potentially critical project outputs such as aircraft designs like the Boeing 787 (Arthur, 2012). Selection of suppliers is a part of project management concern, as it related to both procurement and the quality of the project output (PMI, 2013).

TOWARDS CYBERSECURITY RISK MANAGEMENT IN PROJECTS

Tentatively, it would seem that evidence from recent published breaches, the academic literature on IT supply chain cybersecurity, and the U.S. DoD’s recent directives on acquisitions cybersecurity all indicate that cybersecurity threats early in the life cycle are real. Further research may be needed, however, to verify and quantify the extent to which early life cycle threats are actually occurring.

Given the preliminary evidence of early life cycle cybersecurity risk, we move on to explore the link between cybersecurity and projects. Cybersecurity threats present unique challenges to project management due to the unique nature of the risks, the specialized knowledge required to assess them, and the security controls needed to avoid or mitigate them. Cybersecurity threats are extremely broad in nature – both in terms of the wide variety of potential attack vectors, the types and mechanisms of threats, and the fact that all phases of the project are potentially affected (US DoD, Jan. 2015 and Sept. 2015). The risks posed by cybersecurity threats change rapidly – new threats and vulnerabilities are discovered constantly. This underscores the need for a multidisciplinary approach and constant vigilance (Hendershot, 2014). Controlling risks associated with cybersecurity threats often require highly specialized and technical security controls, such as firewalls, intrusion detection software, and network segregation – these require specialists to implement and monitor.

US GOVERNMENT TREATMENT OF CYBERSECURITY THREATS AS PROJECT RISKS

In response to the growing cybersecurity threats, the United States Department of Defense is transitioning its defensive posture from “a historically compliance-based process to a risk-based, full-lifecycle approach” (US DoD, Sept. 2015). The change is based on a belief that cyberattacks will be coming earlier and often, and will bring increased risk to highly interconnected DoD systems (US DoD, Jan. 2015). So, instead of focusing on post-project security testing of recently completed systems, the new DoD cybersecurity approach is focusing instead on cybersecurity risk management throughout the project life cycle. The new approach is more iterative. It is more about testing throughout rather than testing at the end, consistent with software engineering best practices. It requires early involvement on the part of cybersecurity specialists, and more cyber awareness on the part of project managers. Specifically, the DoD is implementing the new approach by requiring every acquisitions program with an IT component to include cybersecurity risk management (US DoD, Jan. 2015). The directive is a broad requirement capturing not only weapon systems but also all other IT acquisitions.

CURRENT RISK MANAGEMENT PROCESSES FOR PROJECTS RELATED TO CYBERSECURITY

Two risk management models were reviewed which appear useful for the management of cybersecurity-related project risks:

1. The PMI Project Management Body of Knowledge, 5th Ed. risk management process (PMI, 2013), selected to represent widely-accepted risk management practices in projects.

2. "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle" (DoD, Sept 2015), selected to represent a cybersecurity-specific risk management framework based on recognized best practices by the US Department of Defense

These two models each have their own strengths for the project manager in the cybersecurity domain. The PMI Model reflects known good practices and overarching project management processes. It is an ANSI standard for project management that has been widely reviewed and adopted (PMI, 2013). The DoD Program Managers Guidebook represents the culmination of an extensive multi-agency review to identify and define the best practices for managing cybersecurity risks based on the DoD's long experience in being a constant target of cyberattacks (US DoD, Sept 2015). It includes NIST standard 800-53r4 (NIST, 2013), which is often cited, and is an implementation of the DoD Risk Management Framework. It is required to be used for highly sensitive programs whose purpose is to acquire systems deemed vital to national security (US DoD, Sept 2015).

Based on a review of the language and intent of the process steps in each model, it was noted that it may be possible in a future research effort to adapt the DoD Cybersecurity Risk Management model (US DoD, Sept 2015) to include concepts and language from the PMI Project Management Body of Knowledge (PMI, 2013). The resulting cybersecurity process might then send information into the risk register, and thereby interface with the standard PMI risk management processes for the project. The two frameworks, along with this potential linkage, is shown in Figure 1 below.

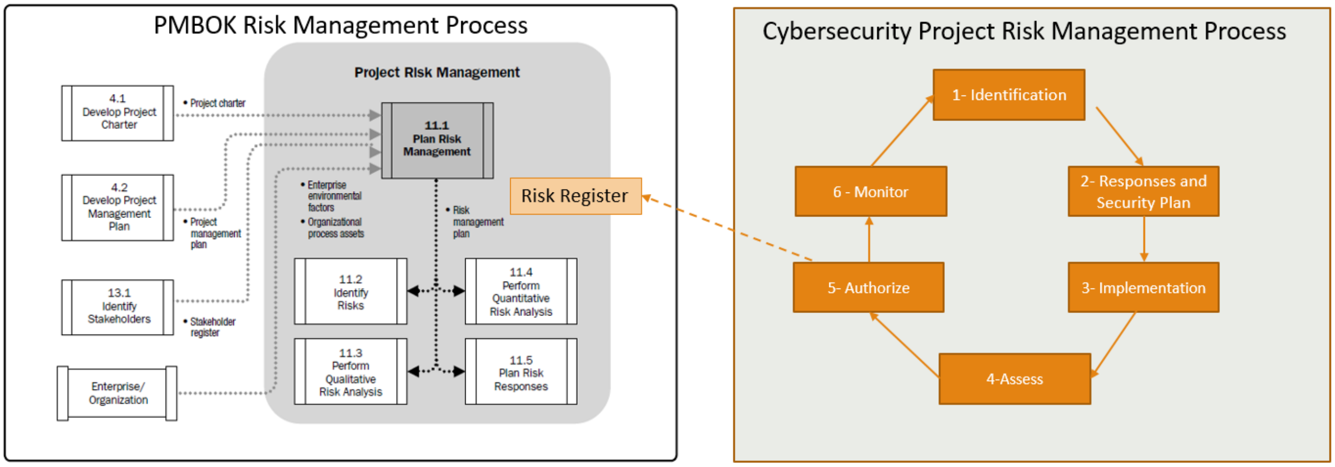
PMBOK Risk Management Process
Project Risk Management
4.1 Develop Project Charter
• Project charter
4.2 Develop Project Management Plan
• Project management plan
13.1 Identify Stakeholders
• Stakeholder register
Enterprise/ Organization
11.1 Plan Risk Management
• Enterprise environmental factors
• Organizational process assets
• Risk management plan
11.2 Identify Risks
11.3 Perform Qualitative Risk Analysis
11.4 Perform Quantitative Risk Analysis
11.5 Plan Risk Responses
Risk Register
Cybersecurity Project Risk Management Process
1- Identification
2- Responses and Security Plan
3- Implementation
4-Assess
5- Authorize
6 - Monitor

Figure 1. Cybersecurity Risk Management Processes

CONCLUSIONS AND FUTURE RESEARCH

Cybersecurity is a key area of risk management for businesses and organizations, and has been demonstrated to affect information systems early in the life cycle and involving players in the IT supply chain. The U.S. DoD has targeted acquisitions as an area of improvement, believing a significant cyber risk is present. It is expected that further examples of actualized risks in projects will continue to appear in the news and in trade journals.

There are unique challenges and expertise needed which present a real challenge to the traditional risk management efforts as outline in the PMBOK (PMI, 2013). The DOD model offers insight into what may be an effective approach, involving the active management of security controls on a continuous process cycle, and performed by experts in the field of cybersecurity. This would seem to indicate it may be optimally provided as a service to project managers, rather than be replicated in every project.

A potentially fruitful area of future research is in the area of cybersecurity threat identification. Cybersecurity threats change very rapidly. It is almost a foregone conclusion that any definitive list will be out of date almost as soon as it is written, so ongoing monitoring will be needed (Hendershot 2014). A general framework of the types of attacks would be useful to a project manager as a starting point. This would require a high-level checklist that could point to the need for further analysis and expertise.

Another area of future research is in risk assessment. Once a potential cybersecurity threat has been identified, the project team will need a way to assess the probability of the attack and the potential impact in order that these threats may be prioritized. A high level description of this process is described in section 11 of the PMI Project Management Body of Knowledge (PMI, 2013) but specific methods to examine cybersecurity threats needs to be researched. Specifically, consideration should be given to:

- What are the characteristics of a project that would invite attention from potential attackers?
- What motivations would inspire cyber attacks
- Would certain motivations potentially affect the methods chosen by potential attackers
- Who are the potential attackers, and what are their motivations and capabilities?
- Which ideological characteristics could influence attacker behavior, if any?
- What are the risks of attribution and consequences to the attacker if caught, and how will this affect the likelihood of an attack?

Many models for risk assessment exist, and future research could focus on identifying models that yield useful information relatively quickly based on information likely to be available to the project manager. An example of this type of research can be found in a study of e-voting risks. This effort used a combination of threat tree analysis and Monte Carlo simulations to perform quantitative analysis of specific risks (Pardue, Yasinsac, and Landry, 2010). A similar method may be generalized and used to assess cybersecurity risks in a wide range of projects.

REFERENCES

1. United States Department of Defense (US DoD) (Jan. 2015), Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, January 7, 2015. United States Department of Defense, Washington DC.
2. Project Management Institute (PMI) (2013) A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Fifth Edition, Project Management Institute, Newtown Square, PA, USA
3. Hendershot, S. (2014) Cyberattack Growth Means Sophisticated Cybersecurity | PM Network," PM Network, Project Management Institute, Newtown Square, PA
4. Rushe, D. (2015) OPM hack: China blamed for massive breach at US federal agency, The Guardian, June 4, 2014, New York, NY, USA. Available: http://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances.
5. Rieder, R. (2014) Rieder: Edward Snowden's powerful impact, USA Today, Jan 17, 2014, McLean, VA, USA. Available: http://www.usatoday.com/story/money/columnist/rieder/2014/01/17/obama-speech-shows-snowden-impact/4583417/.
6. Perez, E. and Wallace, G. (2015) After Target breach, Homeland Security warns retailers," CNNMoney, 16-Jan-2014, Cable News Network (CNN), Atlanta, GA, USA. Available: http://money.cnn.com/2014/01/16/news/companies/target-breach-report/index.html.
7. Basu, E. (2015) Cybersecurity Lessons Learned from the Ashley Madison Hack, Forbes Media, October 26, 2015, Jersey City, NJ Available: http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/.
8. United States Department of Defense (US DoD) (Sept. 2015), DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, Version 1.08, Office of the Secretary of Defense, September 2015. United States Department of Defense, Washington, DC, USA
9. Pardue, H., Yasinsac, A., and Landry, J. (2010) "Towards internet voting security: A threat tree for risk assessment," in Risks and Security of Internet and Systems (CRiSIS), 2010 Fifth International Conference on, 2010, pp. 1–7
10. National Institute of Standards and Technology (NIST) (2013), Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology, NIST SP 800-53r4, Apr. 2013, US Department of Commerce, Washington DC, USA
11. Skorobogatov, S. and Woods, C. (2012) Breakthrough silicon scanning discovers backdoor in military chip, in Cryptographic Hardware and Embedded Systems–CHES 2012, Springer, 2012, pp. 23–40
12. Arthur, C (2012) Cyber-attack concerns raised over Boeing 787 chip's 'back door', The Guardian, May 29,2012
13. Windelberg, M. (2016) Objectives for Managing Cyber Supply Chain Risk. International Journal of Critical Infrastructure Protection 12: pp. 4-11.
14. Boyson, S. (2014) Cyber Supply Chain Risk Management: Revolutionizing The Strategic Control of Critical IT Systems. Technovation 34.7: pp. 342-353.
15. Vijayan, J. (2014) Target breach happened because of a basic network segmentation error, Computerworld, Feb 6, 2014. Available: http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html
16. Upton, D. M., and Creese, S. (2014) "The Danger from Within." Harvard Business Review 92.9: pp. 94-101