International Journal of Security and Its Applications
Vol. 3, No. 2, April, 2009

A Governance Framework for Building Secure IT Systems*

Abdelwahab Hamou-Lhadj[1] and AbdelKrim Hamou-Lhadj[2]
[1]*Department of Electrical and Computer Engineering*
Concordia University
1455 de Maisonneuve West
Montréal, Québec, Canada
abdelw@ece.concordia.ca

[2]*Cognos Inc.*
3755 Riverside Drive
Ottawa, Ontario, Canada
abdelkrim.hamou-lhadj@cognos.com

Abstract

In this paper, we present a framework that aims to align software development with sound business practices for building software systems with security in mind. The framework comprises four main components: Governance, People, Process, and Technology. Governance ensures that security is part of the strategic decisions of an organization. The people component focuses on selecting, training, and retaining, qualified personnel in the area of software security. The process component ensures that the company has the right processes in place to handle security requirements. The technology component consists of a set of tools and techniques that are needed to design and implement secure software.

1. Introduction

Security of information has become one of the major concerns in today's digitized world since critical decisions are made based on information stored and analyzed by software systems. As a consequence, the need for effective techniques to protect software systems from malicious attacks has increased the level of significance of the software security field to meet industry needs. Attacks can range from viruses and worms, Internet browser exploits, identity theft to more sever threats such as cyber-attacks and cyber-terrorism.

For major software companies, building secure software products has perhaps become one of their most urgent priorities. Failure to meet security requirements can have a significant impact on the company such as loss of business and damage to the reputation. In 2002, Chief Executive Officers ranked software security as 7.5 out of 10 in importance [1]. The average firm's budget spent on security was about US$1.1 million in 2002 representing a total of US$196 spent on security per employee per year [2]. According to Schneier [3], budget allotted to building secure software system increases at the rate of 20% every year.

Recently, there has been a significant increase in the number of techniques and tools to design, develop, and test software products that aim to detect malicious attacks and recover if these attacks occur [4, 5, 6, 7]. However, these techniques and tools address security only from the technological aspects, focusing less on the organizational context needed to leverage proper development of a secure system. The issue is that even the most advanced

* This paper is based on the paper: A. Hamou-Lhadj, A-K. Hamou-Lhadj, "An Organizational Framework for Building Secure Software", In Proceedings of the 2nd IEEE International Conference on Information Security and Assurance, IEEE CS, Busan, Korea, 2008.

technological solutions may deem to be ineffective if there is no consistent support of security from the business standpoint, including commitment from senior management to security, skilled employees, and efficient and effective business processes.

In this paper, we propose a framework that aims to align software security with sound business practices. The objective is to work towards a holistic approach to security that combines technology and management in an effective and efficient manner. Our framework extends the People-Process-Technology framework proposed in project management studies [10] by adding a Governance component.

The remaining parts of this paper are as follows. In the next section, we present the security governance framework and describe its components in more detail. In Section 3, we conclude this paper and present future work.

2. The proposed framework

Figure 1 illustrates the components of the proposed framework for building secure systems. We describe in more detail each component of the framework in the following subsections.

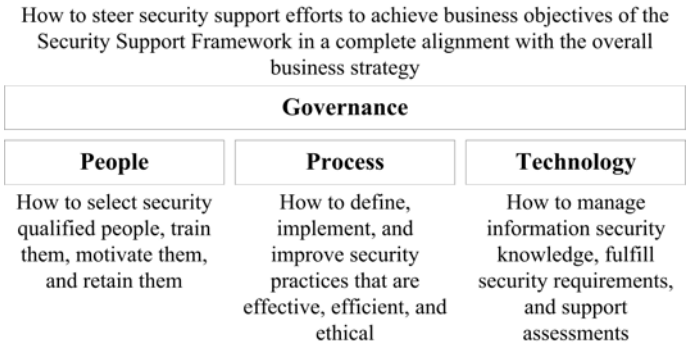

Figure 1. Components of a Framework for Security

2.1. Governance component

Governance, or more precisely enterprise governance, is defined as “the system by which entities [in an organization] are directed and controlled” [8]. The objective of the governance component of the security framework is to ensure that security activities are aligned with software development practices at the strategic level. This can be achieved by involving the board of directors in security-related decisions. The key outcome of the governance component is a set of mechanisms that support effective planning, execution and monitoring of software engineering projects with security in mind.

More specifically, organizations need to introduce policies and guidelines that help software developers determine the way security needs to be handled through the software lifecycle. Examples of such policies include proper quality assurance practices, designing for security, and inclusion of security testing.

Another important aspect of the governance component is to determine a set of key performance indicators to assess the performance of the security support framework against measurable goals that the organization would target in order to fully integrate security support

activities with software development practices. These performance indicators can be collected using management controls and audit procedures.

2.2. People component

The goal of the people component focuses on the hiring and retention of qualified personnel that can operate the security support framework and deliver on its objectives. For this purpose, organizations must invest in training and educational activities that provide practitioners with the knowledge and expertise needed to design and implement security requirements for large systems. There exist today many programs offered in most major universities that focus on various aspects of software security including secure wireless and wired data networks, computer system security, cryptography, secure database systems, secure software engineering, secure e-Commerce, enterprise security, secure operating systems and networks, etc.

In addition, knowledge of regulations, laws, and standards in the area of privacy and security is also important since most of these authoritative rules have a direct impact on the way software is built, tested, and maintained. For example, the ISO/IEC 27000[†] series of standards defines a set of recommendations that describe how information security management systems should be implemented, operated, monitored, reviewed, and maintained. Another example would be the Payment Card Industry Data Security Standards[‡], developed by major credit companies such as Visa, Master Card, American Express and that contain guidelines on how to store and process credit card information.

Furthermore, there is a need to work towards defining a body of knowledge in the area of software security that can be used by training institutions to design their security programs and professional certifications.

2.3. Process component

The process component focuses on the needed business processes for the framework to be operational. A business process can be defined as a set of activities that deliver directly or indirectly value to customers [9]. The key processes that need to be considered can be grouped into two categories: Development processes, and assessment/improvement processes.

From the development perspective, business processes need to be defined on how software development should be carried out to ensure that the resulting products satisfy security requirements. Examples of such processes need to address questions such as how to define security-related requirements, how to design for secure software, how to test for security, etc.

From the assessment and improvement viewpoint, processes need to be put in place to identify areas of improvements based on assessment measures, which in turn need to be determined. Examples of these processes include identifying the impact of potential security issues earlier in the project lifecycle, developing a more efficient model for regression testing, etc.

2.4. Technology component

The technology component of the security framework embodies a set of techniques and tools that can be used by software engineers to design secure software systems.

[†] http://www.iso27001security.com
[‡] http://www.pcisecuritystandards.org

Software security has progressed over the years to becoming a well established discipline. There exist various algorithms applied depending to what needs to be secured and the degree of security needed [4, 5, 6, 7]. There is also an increasing interest in techniques that address security throughout the entire software development life cycle [11, 12, 13]. The objective is to deal with security requirements early in the software life cycle and not only during implementation. Examples of such techniques include the concepts of abuse cases [11] and threat modeling [12]. Abuse cases are based on UML [14] use cases and consist of designing scenarios that simulate attacks to the system, and design techniques that prevent these attacks.

Threat modeling is another security-analysis methodology used to assess and document the security risks associated with a software system during the design phases [12]. This popular technique aims at helping system designers reason about security threats using models. Threats are ranked based on their severity and mitigation techniques are designed to respond to such threats.

3. Conclusion and future work

In this paper, we proposed a framework that aims to align software security with effective business practices. The framework consists of four main components: Governance, People, Process, and Technology. The government component ensures that the board of directors is involved in setting long term strategic decisions on how security should be handled. The people component is concerned with hiring, retaining, and motivating, qualified security architects and designers. The process component puts the emphasis on the needed business processes for the framework to be effective. Finally, the technology component consists of a set of techniques for designing and implementing secure software. Our immediate future step is to expand this framework and experiment with it in an organization setting to assess its effectiveness.

References

[1] M. Gerencser and D. Aguirre, “Security Concerns Prominent on CEO Agenda”, *Strategy + Business Press*, 2002. URL: http://www.strategy-business.com/press/enewsarticle/22197.
[2] A. Carey, “Worldwide Information Security Services Forecast, 2001–2006”, *IDC Report No. 26899*, 2002
[3] A. Schneier, *Secrets & Lies*, John Wiley & Sons, 2000.
[4] J. Viega, G. McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way*, Addison-Wesley, 2002.
[5] N. Davis, “Developing Secure Software”, *Software Tech News: Secure Software Engineering, 8(2)*, 2005.
[6] M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2002.
[7] G. McGraw, *Software Security: Building Security In*, Addison-Wesley, 2006.
[8] Wim Van Grembergen, "Strategies for Information Technology Governance", Idea Group Publishing, 2003.
[9] U. J. Gelinas, S. G. Sutton, J. Fedorowicz, "Business Processes and Information Technology", South-Western College Publisher, 2003.
[10] S. Berkun, *The art of project management*, O'Reilly Media, 2005.
[11] G. Sindre & A. L. Opdahl, “Eliciting Security Requirement by Misuse Cases”, *Journal of Requirements Engineering, Springer London, 10(1)*, 2005, pp. 34 – 44.
[12] F. Swiderski, W. Snyder, *Threat Modeling*, Microsoft Press, 2004.
[13] K. Sultan, A. Ennouary, A. Hamou-Lhadj, "Catalog of Metrics for Assessing Security Risks of Software throughout the Software Development Life Cycle", *In Proc. of the 2nd IEEE International Conference on Information Security and Assurance*, IEEE CS, Busan, Korea, 2008.
[14] Al. Cockburn, *Writing Effective Use Cases*, Addison-Wesley, 2000.

Authors

Abdelwahab Hamou-Lhadj is an Assistant Professor in the Department of Electrical and Computer Engineering (ECE) at Concordia University, Montreal, Canada. He holds a PhD degree in Computer Science from the University of Ottawa, Canada. His research interests include software engineering, software compliance, and information technology. He has published numerous articles in renowned conference and journal proceedings. He has also been involved in the organization and the program committees of several international conferences. Dr. Hamou-Lhadjis a certified Expert in Business Process Management from the Object Management Group (OMG). He is a member of IEEE Computer Society and ACM.

AbdelKrim Hamou-Lhadj (“Abdel”) has over twenty years of work experience in the software industry. He specializes in compliance and quality management, business process management, and software engineering regulations and standards. He currently leads the Regulatory Compliance and Quality Management function at Cognos (an IBM company). Abdel holds an MBA degree from the University of Ottawa, Canada, and other graduate degrees including one in software engineering. In addition, Abdel is a certified Professional Engineer from the Professional Engineers Ontario (PEO) association, a certified Manager of Quality and Organizational Excellence from the American Society for Quality (ASQ), and a certified Expert in Business Process Management from the Object Management Group (OMG).