https://doi.org/10.48009/3_iis_2019_151-157

Issues in Information Systems
Volume 20, Issue 3, pp. 151-157, 2019

A MODEL GRADUATE ENTERPRISE SECURITY COURSE

Manouchehr Tabatabaei, Georgia Southern University, mtabatab@georgiasouthern.edu
James K. Harris, Georgia Southern University, jkharris@georgiasouthern.edu

ABSTRACT

The importance of security is increasingly important and this is particularly true with advancement and widespread use of technology. Further, the enterprise systems have gained popularity in recent years. These systems are transforming organizations significantly and have introduced many advantages and challenges to organizations including facilitating integration, internationalization and gaining competitive advantage. However, these complex enterprise systems call for more extensive security plans in the organizations. Therefore, a good understanding of security and risk management has become essential for organizations and modern managers. The purpose of this paper is to emphasize the importance of enterprise security and introduce a model for offering security education in graduate curricula.

Keywords: Security, Enterprise Systems, Security Education, Graduate Curriculum, Risk Management, Software Assurance, MSIS/MSES

INTRODUCTION

Enterprise systems have been introduced and have benefited organizations for many years (Davenport, 1998). In recent years, they have revolutionized and given organizations strategic advantages and new ways to compete in the industry. The silo organizations are increasingly seeking to integrate and improve their cross-functional processes. The enterprise solution is to improve efficiency and effectiveness of business processes and incorporate best practices (Davenport, 2000).

Institutions of higher education are reacting to the popularity and increasing demand for enterprise systems. They are offering undergraduate and graduate courses in Enterprise Resource Planning (ERP) and SAP, which is the leading vendor of ERP. In addition, institutions are now offering graduate degrees in Enterprise Systems such as Master of Science in Enterprise Systems (MSES). Further, institutions are offering ERP graduate certificate programs for those who want to learn about ERP and ERP implementation. The Enterprise Systems courses and programs are increasingly designed and delivered online. Like most graduate programs, the MSES consists of ten courses, including a course in Enterprise Security. Figure 1 shows an example of MSES curriculum based on the graduate courses in Information Systems (IS), Information Technology (IT), Computer Science (CS) and Master of Business Administration (MBA). Institutions with graduate programs in IS, IT and CS are typically offering most of these courses shown in Figure 1. These existing courses may need updates and changes to the content and titles to make them suitable for MSES. Therefore, only a few new courses such as Enterprise Security need to be developed.

The Enterprise Security course is included as a required course in the MSES curriculum because of the demand by the industry and employer. The inclusion of the security course is also encouraged by the alumni and advisory boards. Further, the MSIS (Master of Science in Information Systems) Model Curriculum (MSIS, 2016) recognizes the importance of the security topic for the MSES degree. Many institutions because of great interest in security topic and demand (Antonucci et al., 2004) increasingly offer the graduate Enterprise Security certificates.

MSES – 30 hours
Required Courses (24 hours), Elective Courses (6 hours)

Required Courses
CISM 7330 – Information Technology Management
CISM 7331 - Enterprise Systems Analysis & Configuration

CISM 7332 – Enterprise Data Management
CISM 7335 - Business Intelligence
CISM 7336 – Enterprise Information Systems
CISM 7434 – Enterprise Security
CISM 7231 - ERP Business Process Analysis using SAP
CISM 7431 - Project Management

Elective
CISM 7235 – ERP Customization for SAP
CISM 7333 – Business Data Visualization & Analytics
CISM 7334 – Enterprise Systems Implementation)
CISM 7339 - ERP Certification Review

Figure 1: Master of Science in Enterprise Systems (MSES)

In addition to the proposed MSES curriculum presented in figure 1, the Enterprise Security is also suggested as an essential course in the Systems and Software Assurance Curriculum (Jovanovic et al., 2016). In their paper *A Model System and Software Assurance Graduate Curriculum* the proposed Enterprise Security Course is used as a cross-departmental elective in the curriculum (Figure 2).

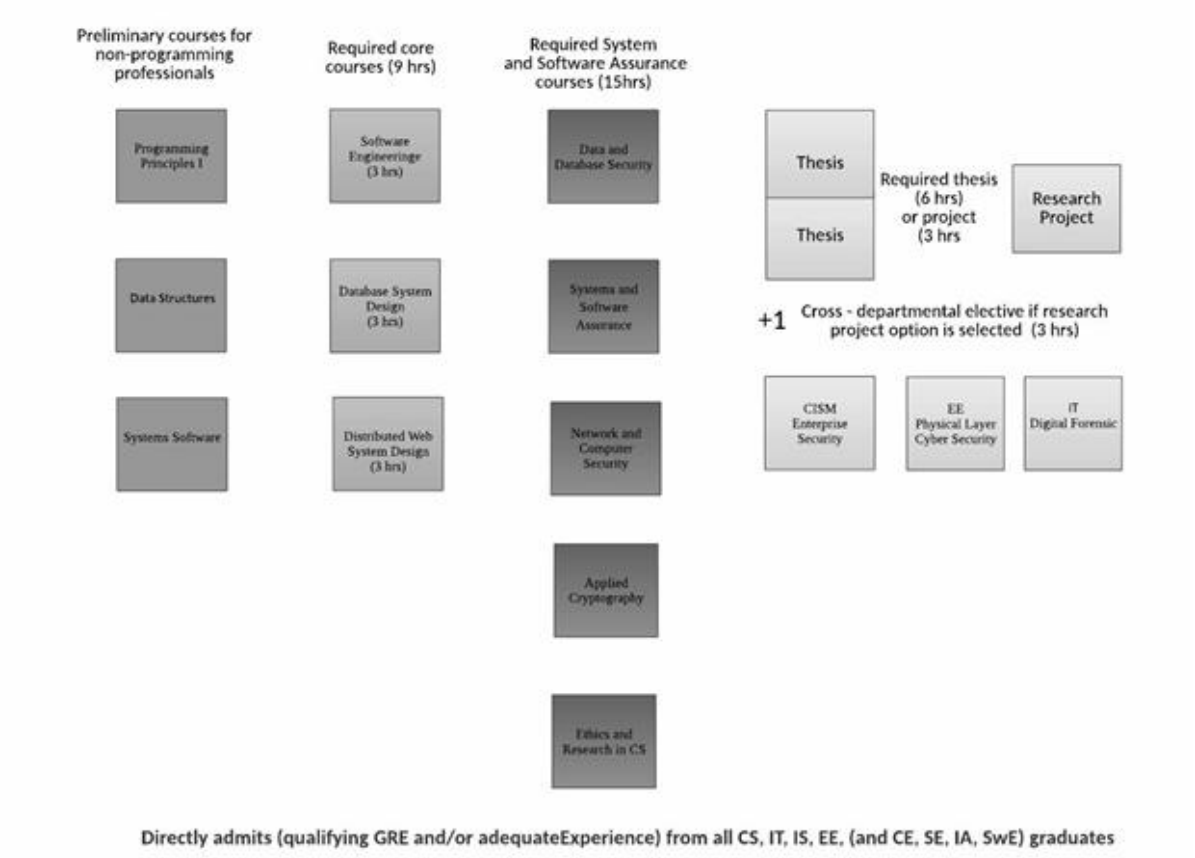

Figure 2. Systems and Software Assurance Curriculum (30 hours)

The Enterprise Security course in the System and Software Assurance graduate program is for CS Masters level students who are planning to graduate with a non-thesis option. The course is primarily for those students interested in software assurance applied to enterprise applications (McGraw, 2006; Ranome & Misra, 2014; Shostak, 2014). The course provides students with important domain knowledge about the objectives, the architectures, the policies and procedures, the methods of risk assessment, and the common methods of attack in enterprise security (Mowbray,

2014). This course should be taken before the System and Software Assurance course so that students can apply the principles taught in the System and Software Assurance course to the applicable software in enterprise systems. According to (Geneca, 2017), only 55% of software developers feel that the business objectives of their projects are clear to them, and the Project Management Institute (PMI, 2014) reported a survey that found that 37% of all organizations reported inaccurate requirements as the primary reason for project failure. Having a clear understanding of enterprise security requirements beforehand can make the difference between success and failure in order for developers to create secure enterprise software systems.

The importance of security cannot be overemphasized. Computer security concerns are nothing new; they were born along with the introduction of computer systems and technology in organizations. However, with advancement of technology and widespread adoption of internet, cloud computing, mobile and digital devices these concerns have amplified (Ammar, 2018; Sfar et al., 2018,). The ease and user friendliness of technology have increased vulnerability over the years. The computer security industry is estimated to be in the billion-dollar range, with Gartner research estimating worldwide security spending at about $96 billion in 2018.

Therefore, security issues need to be addressed when an organization is planning to adopt new system to add value and gain strategic advantage. Organizations should make conscious decisions about privacy and security risk management (Culnan, 2006; Heng et al., 2011; Piccoli, 2006). They will have to implement more security or accept higher risks, and determine whether or not they want to be proactive rather than be reactive. Currently, the consensus is that the amount of money spent on security is insignificant in organizations, but the consequences can be significant. The findings of a survey given by ComputerWorld and InfoWorld (ComputerWorld & InfoWorld Security Report) concerning the amount budgeted for security and the confidence level of organizations are astonishing. Half of the organizations who responded spend less than 5% of their IT budget on security; while 50% of those in charge of their organization's security are only "somewhat confident" in their enterprise security. However, security breaches have significant business impacts (Burztein, 204; Harrison, 2015; O'Brien, 2016; Zeller, 2014). Many organizations with security breaches, such as the much publicized Equifax security breach, have lost billions in each incident (Cavusoglu et al., 2004). Further, firms like FedEx are alerting shareholder that cyberattacks are costing each company hundreds of millions of dollars (Megaw et al., 2017).

Funding security is rather difficult as it produces no revenues and no ROI can be calculated for the investment. Also, no one is recognized and rewarded if nothing bad happens, while many will be blamed if something bad does happen. Therefore, organizations should make security a management priority and not just make security the responsibility of the IT department. They should focus on prevention rather than reaction when it comes to security. Organizations should examine the confidence level of their most knowledgeable IT experts and see how confident they are with their security efforts and enterprise security. A more recent study found that security was the main priority among surveyed organizations with 70% of them expecting to increase their IT spending on Security (Scavo et al., 2017).

COURSE DESCRIPTION

The Enterprise Security course primarily focuses on the importance of security for business continuity and security issues and mechanism for enterprise systems, especially enterprise resources planning (ERP) systems.
This course will instill the importance of security, and will equip students with the skills needed in securing enterprise systems. Students are introduced to risk management and a broad range of security topics to ensure confidentiality, availability and integrity of enterprise systems. The course will cover different approaches to assessing, planning, implementing and monitoring enterprise security. Further, this course is designed to provide knowledge of issues and techniques surrounding the proper safeguarding of different components of enterprise systems. Information security is focused as a management issue and not just a technical issue in this course.
This course will provide an overview of enterprise systems, security architecture, and the appplication of layered security models to enterprise systems. It will deepen student understanding of enteprise systems' vulnerability assessment, risk assessment frameworks, security policies and security measures used to ensure the availability, confidentiality, and integrity of enterprise systems data. Special attention will be devoted to securing enterprise resources planning (ERP) systems. Specific methods for assessing, planning, implementing and monitoring ERP security will be presented.

COURSE GOALS AND OUTCOMES

The following are student learning outcomes for this security course. After completing this course, students will be able to:

- Demonstrate an understanding of Layered Security (Defense in Depth) models by describing perimeter, network, server, application, and data vulnerabilities and security mechanisms used at each layer
- Demonstrate an understanding of the human side of enterprise system security by describing "enemies" and their motivations, knowledge, and tools.
- Demonstrate the ability to apply appropriate vulnerablity assessment methods for an enterprise system in a business case.
- Demonstrate the ability to conduct a risk assessment for an enterprise system within a business case.
- Demonstrate the ability to calculate "return on security investment (ROSI)" for an enterprise system business case
- Demonstrate undestanding of structured security monitoring systems for enterprise systems by designing a structured monitoring system for an enterprise systems business case.
- Demonstrate understanding of the application ERP security mechanisms via hands-on exercises that provide exposure to security-focused SAP ERP security codes

LEARNING ASSESSMENT

The suggested student learning outcomes identified above primarily will be assessed with direct measures including embedded discussion items on exams and required individual and group assignments. Required activities for enterprise systems cases will be employed to assess student ability to conduct vulnerability and risk assessment and the calculation of ROSI. Structured hands-on exercises within SAP ERP will be used to assess student ability to use SAP transaction codes to secure the ERP system.

COURSE CONTENT

The followings are a list of possible topics that can be covered in the course:

- Objectives of Enterprise Security
- Enemies and their Motivation: What Hackers Know and Use
    - Social engineering
    - Commonly used hackers tools and methods
- Enterprise Systems Security Architectures
- Layered Security Models
- Defense in Depth Security
    - Perimeter vulnerabilities and defenses
        - Firewalls
        - Proxies
        - Demilitarizes Zones
    - Network vulnerabilities and defenses
        - Compartmentalization
        - Intrusion detection systems
    - Server vulnerabilities and defenses
        - PKI and Certificates
        - Mitigating DDOS attacks
        - SQL Injections
        - Cross-site scripting
        - Cross-site request forgeries
        - Web application vulnerabilities and defenses
    - Data vulnerabilities and defenses
        - Determining risk
        - Policies and procedures for handling data

    - Current encryption standards
- Assessing Vulnerabilities
    - Guaging your risk as a target
    - Internal vs. external threats
- Risk Assessment Frameworks and Methods
    - OCTACE
    - FAIR
    - NIST
    - TARA
- Return on Security Investments (ROSI)
- Developing Enterprise System Security Policies and Procedures
- Structured Enterprise System Security Monitoring
- Responding to Intrusions and Attacks
- Addressing Disruptive Technology Security Issues: Enterprise Security in the Era of Big Data and Mobility
- ERP Vulnerabilities and Defenses

COURSE TEXTBOOKS AND MATERIALS

It is suggested that the students in this Enterprise Security course read current and related articles in addition to the assigned textbooks. Also, they should read, analyze, present and discuss related case studies. The instructor should possibly adopt more than one textbook. There are many possibilities for textbooks adoption (e.g., Johnson, 2016; Linkies & Karin, 2010; Scholz, 2013; Talabis & Martin, 2013; Vasileiou & Furnell, 2019) and the instructor should choose the textbooks based on the course focus.

CONCLUSIONS AND FUTURE WORK

The importance of security education cannot be overemphasized for today's modern managers. This importance is increasing with the advancement and widespread use of technology in organizations. In recent years, more organizations are turning to enterprise systems for competitiveness and strategic reasons. Therefore, understanding of security and risk management has become essential for organizations and modern managers.

The focus of this paper is on security and emphasizes the importance of security education. It offers a model for a graduate security course in computing fields. The specific guidelines are provided for offering the Enterprise Security course in graduate curricula. However, changes may be required to tailor and customized the course to a specific curriculum. The examples are given to show how this security course can be used in different graduate curricula.

The future plans are to collect data from students and faculty about the significance and enhancements of this course. The course will also be compared to other courses related to security. In addition, the assessment data will be collected and analyzed for validation of the course as well as student learning outcomes.

REFERENCES

Ammar, M., Russello, G., & Crispoa, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 8-27.

Antonucci, Y. L., Corbitt, G., Glenn, S., & Harris, A. L. (2004). Enterprise Systems Education: Where are we? Where are we? Where are we going?. *Journal of Information Systems Education*, 15(3), 227-234.

Bursztein, E. (2014). Handcrafted fraud and extortion: Manual account hijacking in the wild. *ACM Press*, 347-358.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet Security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 69-104.

Culnan, M. J. (2006). Privacy in search of governance. *Cutter Benchmark Review*, *6*(1), 5-13.

Davenport, T. H. (1998). Putting the enterprise into enterprise system. *Harvard Business Review*, 121-131.

Davenport, T. (2000). Mission critical: Realizing the promise of enterprise systems. *Harvard Business School Press*.

Geneca (2017). Why up to 75% of software projects will fail. https://www.geneca.com/why-up-to-75-of-software-projects-will-fail/, Jan 25.

Harrison, V. (2015), Nearly 1 million new malware threats released every day. CNN Money, retrieve from http://money.cnn.com/2015/04/14/technology/sercurity/cyber-attack-hacks-security/.

Heng X., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798-824.

Johnson, L. (2016). *Security controls, evaluation, testing, and assessment handbook*, Elsevier.

Jovanovic, V., Harris, J. K, & Tabatabaei, M. (2016). A Model system and software assurance graduate curriculum. Journal of Issues in Information Systems, 17 (III), 116-123.

Linkies, M. & Karin, H. (2010). *SAP security and risk management*. SAP Press.

McGraw, G. (2006). *Software Security – Building security in*. Addison Wesley.

Megaw, N., Bland, B., Reed, J., Olearchyk, R., Mundy, S., & Foy, H. (2017). Cyberattack hunt focuses on initial Ukraine infection. Financial Times, retrieved from https://www.ft.com/connect/0ead41a6-5bdb-11e7-b553-e2df1b0c3220.

Mowbray, T. J. (2014). Cybersecurity: managing systems, conducting testing, and investigating intrusions. Hoboken, New Jersey: Wiley.

MSIS (2016). Global competency model for graduate degree programs in Information Systems. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/msis-2006.pdf

O'Brien, S. A. (2016). Widespread cyberattack takes down sites worldwide. CNN, retrieved from http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/index.html.

Piccoli, G. (2006). Doing privacy right: Using data and preserving trust. *Cutter Benchmark Review*, 6(1), 3-5.

PMI (2014). Requirements management-A core competency for project and program success. https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/requirements-management.pdf, August.

Ransome, J., & Misra, A. (2014), *Core software security*. CRC Press

Scavo, F., Wagner, D., Dunlab, T., Newton, B., Scavo, J., & Longwell, J. (2017). IT spending and staffing benchmarks 2017/2018: IT budget and cost metrics by industry and organization size. Computer Economics, retrieved from https://www.computereconomics.com/page.cfm?name=IT%20Spending%20and%20Staffing%20Study.

Scholz, J. (2013). Enterprise architecture and information assurance: Developing a secure foundation, CRC Press, Taylor & Francis Group.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 118-137.

Shostak, A. (2014). *Threat modeling: Design for security*, Wiley.

Talabis, M., & Martin, J. (2013). *Information security risk assessment toolkit*. Elsevier.

Vasileiou, I., Furnell, S. (2019). *Cybersecurity Education for Awareness and Compliance*. IGI Global.

Zetter, K. (2014). Sony got hacked hard: What we know and don't know so far." Wired, retrieved from http://www.wired.com/2014/12/sony-hack-what-we-know/.