Advisory from Professionals

Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions

Jeff Sauls
IT Operations Professional
Austin, TX, USA

Naveen Gudigantala
Operations and Technology Management
University of Portland
Portland, OR 97203, USA
gudigant@up.edu

ABSTRACT

Managing IT security and assurance is a top priority for organizations. Aware of the costs associated with a security or privacy breach, organizations are constantly vigilant about protecting their data and IT systems. In addition, organizations are investing heavily in IT resources to keep up with the challenges of managing their IT security and assurance. Therefore, the IT industry relies greatly on the U.S. higher education system to produce a qualified and competent workforce to manage security challenges. This advisory discusses some security challenges faced by global companies and provides input into the design and delivery of IS curriculum to effectively meet such challenges.

Keywords: Information assurance and security, Curriculum design and development, Computer security

1. INTRODUCTION

Information security and assurance management is vital for the success of organizations. It is particularly relevant for global companies whose customers demand a high level of security for their products. Meeting such high expectations requires companies to study security best practices, continually invest in technical and human resources, and implement a secure corporate environment. The goal of this paper is to discuss some security challenges faced by global organizations and to provide suggestions to IS academics concerning security curriculum to effectively educate the next generation IT workforce to meet these challenges.

2. SECURITY CHALLENGES FACED BY GLOBAL COMPANIES

This advisory focuses on security challenges faced by global companies. For instance, security challenges faced by a multinational company operating manufacturing plants in several countries are likely to be much different than those of a company with a manufacturing plant in a single location. The goal of this section is to present some security challenges faced by global companies.

What many companies do in terms of security is driven by the needs of their customers. For instance, consider the case of a global manufacturing company that makes hardware for a smart card. Smart cards include embedded integrated circuits and customers generally provide the manufacturer with a detailed list of functional and assurance requirements for security. The manufacturer of the hardware is expected to comply with the specifications of the customer. If the company decides to manufacture in two plants in Europe and the U.S., it becomes important for the manufacturer to have uniform security standards in both plants. These security standards may include many aspects such as how firewalls are managed, how data is encrypted, type of security policies, and implementation of security policies. Having uniform security standards in both plants makes it easier for the company to support these plants and the customer to audit the security.

Some customers require the manufacturers to conform to the Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria). Common Criteria is an internationally recognized technical standard,

which includes a framework that is used for evaluating the security of Information Technology (IT) products and technology (SANS Institute, 2003). Common Criteria assures that the processes involved in creating a computer security product have been conducted in a standard manner. The extent to which manufacturers meet specifications can be tested by laboratories. For global companies, meeting Common Criteria standards presents a challenging task because of the time and effort involved in preparing the documentation for security evaluation.

Having the ability to meet the needs of customers with high security requirements helps companies meet the security demands of other customers as well. However, achieving this high level of secure environment comes at a great expense. Research by Gartner finds that global spending on security is expected to increase 8.4% to $60 billion in 2012 and projects the spending to increase to $86 billion in 2016 (CIO Insight, 2012). Thus, organizations must incur large costs from an IT perspective to implement and maintain this high level of security environment.

Some security challenges faced by companies may not be technical in nature but related to human elements. A majority of the communication between customer and vendor is back and forth. Given that not everything can be automated in companies, the jobs performed by humans can result in mistakes. For instance, an employee could mix up the order specifications and another employee could show incorrect data to a client. Therefore, to mitigate these human errors, it is important for companies to provide training to employees on the best practices to avoid making such mistakes.

Global companies experience additional challenges when dealing with different cultures, laws, and practices. For instance, in some far eastern countries, users can be lax with passwords if they feel sharing passwords will help someone else. Typically, internal audits expose such inconsistencies and force global companies to implement uniform password policies. In addition, global companies must respect local laws before making and enforcing any security policies. For instance, creating a uniform policy for remote access control across the U.S., China, and Korea may not be a good idea because local laws must be researched and incorporated when creating such a policy in each of the countries.

The discussion so far highlights security challenges faced by global companies. The need to meet security needs of customers, use common security standards, manage technical and human security threats, and meet cultural and legal aspects of security policies require a next generation IT workforce that is well trained. The next section discusses skills needed by IS graduates and some general advice for designing IS security curriculum.

3. SKILLS REQUIRED FOR GRADUATES SPECIALIZING IN INFORMATION SYSTEMS (IS) SECURITY

The IT infrastructure of modern day global companies is very complex. The large number of systems and applications can easily be overwhelming. Succeeding in such an environment requires the IS graduates to have solid foundational technical knowledge. Different programs may offer different technical foundations. For instance, a computer science student may take different foundational courses compared to an information systems student. A computer science student may take courses in data structures, programming, operating systems, and software engineering, while an IS graduate may take courses in data communications and networking, database management, and systems analysis and design. Regardless of the content differences, the core idea is that an IS security entry level employee must be able to understand what is going on in the system when encountered with a problem. Having solid foundational technical knowledge will help graduates correctly diagnose the problem. Therefore, it is important for today's graduates to understand the IT infrastructure as a system as opposed to focusing on a specific component such as a database or a specific application.

In addition to having foundational technical knowledge, IS graduates must have analytical thinking and problem solving skills. For instance, an employee working with an Oracle product, when encountered with an issue, could first call Oracle support. However, it is advisable for the employee to first think about the causes of the problem (analytical skills help here), dig deeper into the problem, and try to solve it on his or her own before reaching out for help. This could result in a solution sooner than going through a vendor's support structure. Similarly, an entry-level programmer, in addition to writing good code, must think about the environment in which the code will run and keep the whole system in mind when programming. Therefore, foundational technical knowledge, analytical skills, and problem solving skills constitute the core competencies needed by today's IS graduates to work in the IT industry in general and IS security in specific.

4. ADVICE TO IS FACULTY FOR THE DESIGN AND DELIVERY OF IS CURRICULUM

This section presents practical advice to IS faculty concerning improvements to the IS program and curriculum. Though these suggestions may not address every challenge discussed in this advisory, some key inputs are provided to design and deliver IS security curriculum with a view to graduating a competent IT workforce.

1. The IS curriculum to prepare the next generation of security professionals must provide students with strong foundational technical knowledge. The inclusion of courses and the orientation of teaching must help students think about IT infrastructure as a system and not as an individual piece of the puzzle. The role of analytical thinking must be highlighted in solving problems.

2. There must be a strong emphasis on practical exposure to concepts in terms of hands-on experience for students. It is advisable to have each course accompanied by a lab in which students work with technologies and apply concepts. An example is a lab in which students could be divided into two teams, red and blue, with the red team enacting the role of an attacker and the blue team playing the role of a defender. The use of such hands-on activities enables students to better retain knowledge. In addition, students with

hands-on exposure tend to do well in interviews in terms of answering questions or explaining concepts.

3. Student internships must be strongly encouraged. While classroom learning is important, nothing substitutes for the knowledge acquired from real-world experiences.

4. Students must be encouraged to take electives in interdisciplinary areas. For instance, knowledge of operations management, in terms of process analysis, setting up policies, and optimization techniques can help reduce mistakes at the workplace.

5. Faculty could explore the possibility of applying for grants from National science foundation (NSF) and Department of Defense for innovative curriculum design.

6. Faculty are strongly encouraged to integrate latest knowledge concerning best practices in information security into their courses by attending the following workshops: The Colloquium for Information Systems Security Education, Information Security Curriculum Development Conference (InfoSecCD), and World Conference on Information Security Education (WISE) (Whitman and Mattord, 2004).

7. From many years of interviewing, it seems that there is a dearth of qualified technical graduates from U.S. universities. A substantial number of job applicants seem to come from foreign countries and, hence, it is very important for U.S. universities to recruit, train, retain, and place a substantial number of technically qualified degree students to meet the demands of the IT security industry.

5. CONCLUSION

While the need for global information security and assurance is increasing, it appears that the supply of qualified technical IS students is on the decline. Given the increasing necessity to protect the IT infrastructure and deliver IS assurance, organizations will become increasingly dependent on the U.S. higher education system to provide a workforce with adequate skills to meet these challenges. Therefore, the onus is on the IS academia to design a curriculum that excites students, trains them with hands-on exposure, and provides them with the necessary skills to achieve success in the IT industry. This paper presents practical advice in such direction.

6. ACKNOWLEDGEMENTS

The authors would like to thank Venkata Ramana Jetty for facilitating this work.

7. REFERENCES

CIOinsight (2012). Gartner Predicts Security Market Will Top $86 Billion in 2016, Retrieved June 24, 2013, from http://www.cioinsight.com/c/a/Latest-News/Security-Infrastructure-Market-to-Top-86-Billion-in-2016-Gartner-591583/

SANS Institute (2013). Common Criteria and Protection Profiles: How to Evaluate Information. Retrieved June 24, 2013, from http://www.sans.org/reading_room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information_1078

Whitman, M. & Mattord, H. (2004). A Draft Curriculum Model for Programs of Study in Information Security and Assurance. Proceedings of the 1st annual conference on Information security curriculum development, 1-7.

AUTHOR BIOGRAPHIES

Jeff Sauls manages corporate IT operations for a multinational company, in addition to providing architectural and policy guidance to multidisciplinary teams as they relate to IT. After graduating from Texas A&M University, he has had over 15 years of experience in various roles of system administration, software development, database administration and management. Jeff has designed large and small systems to support varying global business needs with overarching goals of reducing long term support costs while increasing security and capability.

Naveen Gudigantala is Assistant Professor of MIS in the Robert B. Pamplin Jr. School of Business Administration at University of Portland. He received his Ph.D. in MIS from Texas Tech University. His research interests include Web-based decision support systems, information systems education, and containing gray markets for Information Technology products. His work has appeared in the Communications of Association for Information Systems, Decision Support Systems journal, International Journal of Information Management, among other journals.

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096