Proceedings of Informing Science & IT Education Conference (InSITE) 2016

Cite as: Dreyfuss, M., & Giat, Y. (2016). Identifying security risk modules in a university's information system. *Proceedings of Informing Science & IT Education Conference (InSITE) 2016*, 41-51. Retrieved from http://www.informingscience.org/Publications/3436

Identifying Security Risk Modules in a University's Information System

Michael Dreyfuss and Yahel Giat
Jerusalem College of Technology, Jerusalem, Israel

dreyfuss@jct.ac.il; yahel@jct.ac.il

Abstract

We develop a two-stage model for identifying IT system modules with high security risks. In the first phase, we identify the subsystems that pose the highest risk and which require further investigation. In the next phase, we identify the high-security-risk modules using a more detailed approach. The output of this model helps managers decide on how to invest efficiently in improving the security of their IT system. We describe an application of this model to an IT system in an academic institution in Israel. In the first phase, three of ten subsystems are found to be very risky. In the next phase, we highlight the critical modules within those subsystems. The results of our application in the academic institution indicate that security breaches for the purpose of cheating are a greater threat than other types of security issues.

Keywords: Information security, risk management, academic institutions, composite risk factor, information technology systems.

Introduction

When it comes to information security, universities are in quite the conundrum. On the one hand side, universities promote inclusiveness, openness and the dissemination of information and knowledge. Indeed, Mensch & Wilkie (2011, p. 91) find that "universities openly share a substantial amount of information and data, web sites are rarely banned and message content is not filtered". On the other hand, universities store valuable information in their systems such as information about thousands of students and faculty, research data and patent information. This information must be protected diligently, with as little as possible interference to the academic spirit of free access to information. It is therefore very challenging to design a security system that balances these requirements.

To avoid an overreaching security system, it is important for the security staff to focus on the riskiest elements of their information system. Doing so achieves a number of goals. The first is the aforementioned goal of enabling the dissemination of academic knowledge without allowing malicious entities from exploiting this welcoming environment. The second goal is that by identifying the riskiest system components managers may use their budget better by focusing only on those components that are in the most need for security improvement. Third, university managers may use this knowledge to understand the types of

Editor: Eli Cohen
Submitted: November 29, 2015; Revised: February 10, February 14, 2016; Accepted: March 11, 2016

information-related threats they face – such as student cheating, propriety rights ownership (i.e., industrial espionage), people's privacy, and so forth.

The goals of this research are twofold. First, to develop a risk-management model that quantifies the risk level of the components and sub-components of an organization's information system. Specifically, we develop with the institution's IT staff a generic questionnaire as a tool for assessing the risk level of each of the IT system's components. Additionally, we build on existing research to formulate how the questionnaire's results are used to quantify the risk level. The second goal of this paper is to apply this model to a college and identify the security-related needs according to the model's results. This application was initiated by the need of the school's IT manager to improve the IT system's security.

Accordingly, we propose a two-step risk management model to identify the critical components of an academic institution's information system. In the first step, we identify the subsystems of the institution's information system and identify the riskiest subsystems using a simple risk management model. In the next phase, we focus on the riskiest subsystems only and identify the modules that compose each risky subsystem. We use a composite risk index model to identify the riskiest modules within each of these subsystems. The model is applied in a technology-oriented academic institution and its output is used to help security managers identify the riskiest components of their system and decide on how to distribute their investment to improve their system security.

Literature Review

Universities in the US report hundreds of thousands of cyber-attacks per day. These attacks originate from all over the world with China the leading location (Pérez-Peña, 2013). Indeed, university computers store valuable data that includes information about people, research and other intellectual property. This valuable information must be protected with sophisticated IT security means, see, for example a survey of research in this area by Zafar & Clark (2009). Lemos (2002) explains that the reason that hackers are so attracted to universities is that universities are public organizations with limited budgets and an open access philosophy and therefore do not invest enough in their security.

In contrast to most enterprises whose needs for IT security is mostly to prevent the theft of valuable information, universities must also deal with the problem of student cheating. College cheating is rampant and continuously increasing. A group of researchers in Haines et al. (1986) report that 50% of college students reported cheating, and just a decade later the same group of researchers found this number has risen to 61.2% (Diekhoff et al., 1996). More recently, Dick et al. (2003) reports that on average 75% of college students reported cheating at some point during the college studies. With the increased technology at hand, student cheating includes hacking into the information systems to change grades (see, for example, Smith, 2014). With the proliferation of E-learning courses and programs, universities' need for securing these systems is ever so important (Ramim & Levy, 2008).

Researchers have investigated the student features that affect the likelihood of computer-related crime and cheating. Our research is conducted in a college in which the majority of the student body is orthodox (religious) Jews pursuing computer sciences and related engineering degrees. Interestingly, Cronan et al. (2006) reports that computer-savvy students are more likely to commit computer crime whereas Burton et al. (2011) find that a high level of religiosity is associated with less academic cheating.

IT Risk Management

The issue of IT security is at its core a problem of risk management (Blakley et al. 2002). Straub and Welke (1998) develop a three-step model that they denote as CPC. The first step is the security risk planning model that includes the recognition of the problems, the risk analysis, the generation of alternatives and the decision and implementation of solutions to the problems. The second step is the security awareness program which trains managers and employees to be proactive and to look forward to potential threats. In the last step, the effectiveness of different security options is evaluated using the model's four countermeasures: deterrence, prevention, detection and remedies. Our model differs from Straub & Welke (1998) in that we are attempting to quantify the exposure to risk of sub-systems in the IT system in order to rank them from highest to lowest security risk.

Whitman (2003) identifies twelve types of threats to information security. Using this list of threats, Sumner (2009) surveyed 102 IT professionals' perceived impact, probability and preparedness to these threats. Each threat is mapped into an information-security-risk grid, whose axes are the impact and the probability for the threat. The threats that are identified as high impact and high probability are considered to be the riskiest. Sumner compares whether the reported risks are aligned with the IT professionals' perceived preparedness and finds that this is not generally the case.

In this paper, we follow Sumner (2009) approach about quantifying risk as a two dimension vector of probability and impact. More precisely, we quantify risk using a composite risk index in a similar manner to Meng et al. (1999). We differ from Sumner (2009) in that we use the composite risk index approach to quantify the risk index of subsystem so that the IT system managers identify which systems require enhanced security measures. Furthermore, Sumner uses a Whitman's (2003) list of twelve types of security breaches as the basis for her questionnaire. In contrast, we design our questionnaire to focus on the outcomes of security-related event and not on the type of breach that may lead to such events.

According to Chaudhry et al. (2012) one of the critical foundations of information security is controlling access to the systems. Indeed, Boss et al. (2009) find that the real cause to most security breaches is the human interaction with the systems. Similarly, Posey et al. (2011) and Bishop et al. (2014) stress that insider threats by employees or users are the main source for breaches. Thus, the probability of a breach can be approximated by the number of users of the system itself and the systems connected to it.

Another approach to IT security in an academic institute is Sridhar & Ahuja (2007) who present an implementation of security management infrastructure in a business school in India. The risk management idea can be further extended to include strategic considerations. For example, Cavusoglu et al. (2004) consider the strategic game between hackers and IT security managers. When a system's security is improved then the hacker's cost to breach it increases and therefore the hacker changes his behavior (i.e., he may choose not to hack it). Our model abstracts from these considerations since our goal is identifying the elements of the system prone to risk rather than dictating an exact investment policy.

Shedden et al. (2010) claim that the business practices and culture of the organization must be considered to evaluate the organization's IT security risk. Similarly, Drevin et al. (2007) apply Keeney's (1994) model of value focused thinking to improve IT security awareness at a university in South Africa.

In contrast to the aforementioned views, Verendel (2009) claims that quantifying risk does not work. They provide a comprehensive survey of research and show that there is not sufficient empirical evidence to corroborate the hypothesis that computer and information "security can cor-

rectly be represented with quantitative information" (Verendel, 2009, p. 37). In our paper, we do follow the numerous researchers attempting to quantify IT security risks (e.g., Feng & Li, 2011; Ryan et al., 2012; Rebollo, et al., 2015). This quantification may be used to construct a relationship between improvement and investment and allow gradual, optimal investment as in Giat (2013). Notwithstanding, we acknowledge that this quantification must be used with the proper caution. We therefore propose that our model is used mainly as a decision support tool to the IT security staff.

Risk Management IT Model

Model Overview

This model serves as a decision support tool for managers in their need to improve their IT security. The output of the model will not explicitly dictate how to distribute the budget across all the information systems, but rather display to managers in a very illuminating manner, which systems are the most critical in their exposure to risk, so that they place the necessary emphasis on these systems.

The first phase of the model focuses on the sub-systems of the organization's IT system. In the second phase the subsystems that were identified riskiest are further analyzed. We identify and characterize the risk-related variables of the modules of each high-risk subsystem and highlight the modules that require the highest investment.

Phase 1: Subsystems

We begin by identifying the different systems of the organizations' IT system. The person in charge of each subsystem is asked to complete the Subsystem Questionnaire. This questionnaire is given in the appendix and assesses the risk-associated characteristics of the subsystem. The questionnaire was developed through multiple meetings with IT staff members and management. Staff members offered criteria based on their experience. After discussion, the various criteria were integrated into a unified system-independent questionnaire. Since the IT is rapidly changing, a system-dependent questionnaire may be irrelevant within a short time, whereas a generic questionnaire may still be adequate.

The first eight items of the questionnaire are general questions regarding how severely the organization is affected if the sub-system is breached. The value of each item ranges between 1 (no adverse effect) to 5 (very severe).

The ninth item asks whether the information in the sub-system is protected by penal law. This item is a dichotomous variable, accepting 0 or 1.

The tenth item asks whether the information in the sub-system is critical to the organization's survival. This item is also dichotomous, accepting 0 or 1.

The eleventh item is the subsystem's number of users and the last item is the number of users authorized to make edit changes in the system.

The subsystem's Severity variable is the weighted average of the questionnaire's first ten items in the following manner:

$$S = 0.1 * \left(\frac{1}{8} \sum_{i=1}^{8} Item(i) \ + Item(9) + Item(10) + 3 \right). \qquad (1)$$

In the above, the maximal possible value of S is 1 and the minimal possible value is 0.4

Following research that stresses that insider human factor is the greatest cause to security breaches (e.g., Boss et al., 2009; Posey et al., 2011; Bishop et al., 2014) we let the subsystem's exposure to risk to depend on the number of people who have access to it. This information is given in items 11 and 12 of the questionnaire. The answers to these items are normalized to be in the range [0,1] by taking it as a percentage of the subsystem with the biggest value. If the highest value of item 11 among all the subsystems is 4000, then item 11 of all the subsystems is divided by 4000. The subsystem's Exposure is now given by:

$$E = \frac{Normalized\ item(11) + Normalized\ item(12)}{2}. \quad (2)$$

Finally, the subsystem's Impact is given by

$$C = S^{1-E}. \quad (3)$$

That is, Impact increases with the Severity and the Exposure (recall, S <1) and ranges between 0.4 and 1.

Phase 2: Modules

Once the subsystems with the greatest risk factor have been identified, we limit our attention to these subsystems and proceed with the following steps. We begin by identifying the modules of the subsystem. This is typically done by interviewing the IT staff and constructing the subsystem as a collection of separately functional modules. For each module, the relevant IT personnel are asked to complete the Module Questionnaire, which is provided in the appendix. This questionnaire comprises the Subsystem Questionnaire and eight additional items numbered items 13-20. These questions ask about the likelihood of a risky event with regard to the tested module. The value of each item ranges between 1 (not likely at all) to 5 (very likely).

At the module level the questionnaire attempts to capture a deeper understanding of the IT risks. For this reason we expand the questionnaire. At the subsystem level there is no need for such precision. The purpose of the first phase is only to highlight the subsystems that warrant a more careful analysis.

We now use the first part of the questionnaire (items 1-12) to establish S, E and C using (1), (2) and (3), respectively. The *Probability* variable is the probability for a risky event. It is derived using the second part of the questionnaire (items 13-20) and is given by

$$P = \frac{1}{40}\sum_{i=13}^{20} Item(i). \quad (4)$$

Similarly to Meng et al. (1999), the module's Risk Factor is a composite risk index. Specifically, it is modelled as the product of its Impact and Probability:

$$RF = P * C. \quad (5)$$

Model Application

This research was conducted in an academic institute in Israel. The school's student body is approximately 4000 in four different campus locations. The school offers bachelor degrees in engineering, exact sciences and management and also has successful accounting and nursing programs. Currently, the school has two graduate programs, in computer science and business.

We use the model described above to provide the school's IT staff with a decision support tool as to how to invest in improving the IT security. Together with the head of the IT department we first establish the different information subsystem. In the next, step we ask the manager of each of the subsystems to complete the Subsystem Questionnaire. In Table 1, we enumerate the subsystems and summarize the responses to the questionnaire. Item 11 describes the subsystem's number of users. The Student Administration subsystem has 4000 users, which is the greatest number of users. Therefore, to normalize item 11, we divide the number of users of each subsystem by 4000. Similarly, to normalize item 12 (the number of users authorized to edit the content of the subsystem) we divide it by 600.

Table 1: The questionnaire's results for the school's IT subsystems

Subsystem	Sum of items 1-8	Sum of items 9-10	Item 11	Subsystem
Dormitories	14	1	337 (8.4%)	2 (0.3%)
Student Administration	34	1	**4000 (100%)**	60 (10.0%)
Endowments & Contributions	17	1	334 (8.4%)	5 (0.8%)
Parking	11	1	335 (8.4%)	5 (0.8%)
Procurement	26	1	50 (1.25%)	50 (8.3%)
General Maintenance	26	1	1500 (37.5%)	3 (0.5%)
Student Employment	14	0	500 (12.5%)	500 (83.3%)
Salaries & Personnel	16	0	600 (15.0%)	**600 (100%)**
Library	24	1	2000 (50.0%)	7 (1.2%)
Computer Services	16	0	2000 (50.0%)	10 (1.7%)

Table 2: The risk components of school's IT subsystems

Subsystem	S	E	C	Rank
Dormitories	57.50%	4.38%	58.91%	7
Student Administration	82.50%	55.00%	91.71%	1
Endowments & Contributions	61.25%	4.59%	62.64%	5
Parking	53.75%	4.60%	55.31%	10
Procurement	70.00%	4.79%	71.21%	4
General Maintenance	50.00%	19.00%	57.04%	9
Student Employment	72.50%	47.92%	84.58%	3
Salaries & Personnel	72.50%	57.50%	87.23%	2
Library	47.50%	25.58%	57.47%	8
Computer Services	50.00%	25.83%	59.80%	6

In Table 2 we describe the Impact and its components for each subsystem. These are computed from the data in Table 1 and equations (1) – (3). It can be seen that the subsystem with the highest impact is the Student Administration subsystem. Indeed, this subsystem is large and complex, and involves many aspects of the school's activities. There are two more subsystems that require additional attention due to their risk characteristics. These systems are Salaries & Personnel and Student Employment. The next phase of the model should be applied to these three subsystems, since only they require the most attention. In this paper, however, we demonstrate the application of the Student Administration only.

The risk analysis of the Student Administration subsystems included an interview with the Student Administration IT manager from which we established that this subsystem comprises 18 modules, given in the first column of Table 3. Each module's manager was asked to complete the Module Questionnaire. The model variables computed from the questionnaires is provided in Table 3.

Table 3: The risk factor and its components of the modules of the Students Administration subsystem

Module	S	E	C	P	RF	Rank
Personal Records	90.00%	62.50%	96.13%	60.00%	57.68%	3
Class Registration	62.50%	21.32%	69.09%	52.50%	36.27%	8
Grades	85.00%	43.38%	91.21%	82.50%	75.25%	1
Exam Registration	51.25%	15.44%	56.82%	87.50%	49.72%	4
Certificates	48.75%	2.50%	49.63%	50.00%	24.82%	11
Exam Appeals	48.75%	37.50%	63.82%	57.50%	36.70%	6
General Appeals and Requests	62.50%	50.00%	79.06%	45.00%	35.58%	9
Graduation Form	42.50%	15.44%	48.50%	37.50%	18.19%	16
Forms	40.00%	2.50%	40.93%	25.00%	10.23%	17
Credit Card Payments	53.75%	2.50%	54.59%	40.00%	21.84%	13
Account Statements	70.00%	7.94%	72.01%	52.50%	37.81%	5
Payment Vouchers	82.50%	15.44%	84.99%	72.50%	61.62%	2
Printing	66.25%	12.50%	69.75%	52.50%	36.62%	7
Extracurricular Attendance	45.00%	2.50%	45.91%	52.50%	24.10%	12
Dormitory Registration	47.50%	5.00%	49.30%	42.50%	20.95%	14
Fitness Room Registration	61.25%	5.00%	62.77%	50.00%	31.38%	10
Storage Cubicles Registration	43.75%	5.00%	45.60%	40.00%	18.24%	15

In Figure 1, we depict the Criticality, Probability and Risk Factor of the modules. For expositional reasons we omit some of the less-risky modules. Although the Impact of the Personal data module is the highest, it is not the first in the list to be invested. The damage which might be caused through a leak in the Marks module is higher and the risk score (the size of the balls) is also higher.

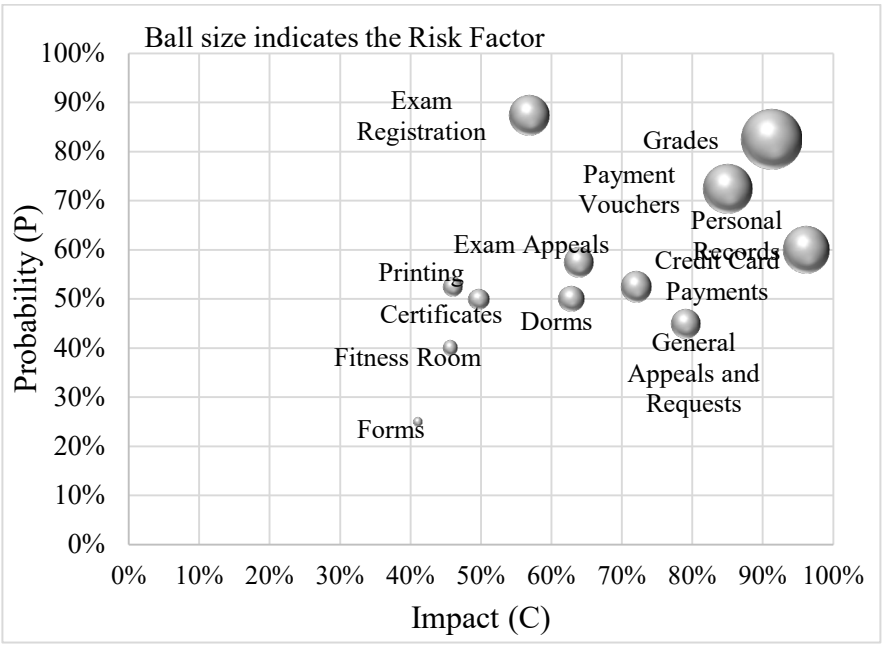

Figure 1: An example of figure.

The school in which this research was done comprises mostly of religious Orthodox Jewish students, which are characterized by a high level of religiosity. Burton et al. (2011) find that a high level of religiosity is associated with less academic cheating. Our finding that the Grades module is bears the highest risk should be true in other higher education institutions with less religious students. This could be explained by the fact that the school's students take multiple computer classes and the majority of the students are pursuing engineering and computer sciences degrees. These types of students were found by Cronan (2006) to be more associated with computer hacking for the purpose of cheating. Indeed, the IT staff described to us a number of security breaches by students. In one event, engineering students used a phishing scam to retrieve a final exam. In another example, information science students used a Trojan horse malware to obtain a lecturer's password.

Conclusions

In this paper we describe a model for identifying critical modules in an IT system. At the first phase, risky subsystems are identified by use of a basic questionnaire and simple risk-management approach. In the second phase, the critical modules of each of the chosen subsystems are highlighted using a more comprehensive questionnaire attempting to capture the probabilities and severities of risky events.

We apply our model to the IT system of a large college in Israel. We find that there are three candidate subsystems that merit investment in improving their IT security. Further, we demonstrate an examination of one of these subsystems and show how only certain modules within the subsystem require special attention.

The model therefore serves as a decision support tool when they face the problem of improving their IT system's security under a constrained budget. In lieu of spending the money in overall system improvement, they can use our model for pinpointing the actual modules that need improvement, thus achieving effective improvement in their overall security while avoiding excessive spending.

References

Bishop, M., Conboy, H. M., Phan, H., Simidchieva, B. I., Avrunin, G. S., Clarke, L. A., Osterweil L. J., & Peisert, S. (2014, May). Insider threat identification by process analysis. In *Security and Privacy Workshops (SPW),* 2014 IEEE (pp. 251-264). IEEE.

Blakley, B., McDermott, E., & Geer, D. (2002). Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms*, ACM, 97-104.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. (2009). If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164

Burton, J. H., Talpade, S., & Haynes, J. (2011). Religiosity and test-taking ethics among business school students. *Journal of Academic and Business Ethics*, *4*, 1-8.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87-92.

Chaudhry, P. E., Chaudhry, S. S., Reese, R., & Jones, D. S. (2012). Enterprise information systems security: A conceptual framework. In *Re-conceptualizing Enterprise Information Systems* (pp. 118-128). Springer Berlin Heidelberg.

Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, computer crime, and IS misuse at the university. *Communications of the ACM*, *49*(6), 84-90.

Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T., & Laxer, C. (2003). Addressing student cheating: Definitions and solutions, *ACM SigCSE Bulletin*, *35*(2), 172-184.

Diekhoff, G. M., LaBeff, E. E., Clark, R. E., Williams, L. E., Francis, B., & Haines, V. J. (1996). College cheating: Ten years later. *Research in Higher Education*, *37*(4), 487-502.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, *26*(1), 36-43.

Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing, 11*(7), 4332-4340.

Giat, Y. (2013). The effects of output growth on preventive investment policy. *American Journal of Operations Research, 3*(6), 474-486.

Haines, V. J., Diekhoff, G. M., LaBeff, E. E., & Clark, R. E. (1986). College cheating: Immaturity, lack of commitment, and the neutralizing attitude. *Research in Higher education*, *25*(4), 342-354.

Keeney, R. L. (1994). Creativity in decision making with value-focused thinking. *Sloan Management Review*, *35*, 33-41.

Lemos R., (2002, May 3). University systems a haven for hackers. *CNET.* Retrieved November, 19, 2015 from http://www.cnet.com/news/university-systems-a-haven-for-hackers/

Meng, L., Maskarinec, G., Lee, J., & Kolonel, L. N. (1999). Lifestyle factors and chronic diseases: Application of a composite risk index. *Preventive Medicine*, *29*(4), 296-304.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, *14*(2), 91.

Pérez-Peña, R., (2013, July 16). Universities face a rising barrage of cyberattacks. *The New York Times.* Retrieved November 19, 2015 from http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?_r=0

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, *30*(6), 486-497.

Ramim, M., & Levy, Y. (2008). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. In H. Nemati (Ed.), *Information security and ethics: Concepts, methodologies, tools, and applications* (pp. 2139-2148). Hershey, PA: Information Science Reference.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57.

Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., De la Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research, 39*(4), 774-784.

Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: Towards a business practice perspective. In *8th Australian Information Security Management Conference*, 119-130.

Smith, G., (2014, August 3). Why study? College hackers are changing F's To A's, *The Huffington Post*, retrieved November 19, 2015 from http://www.huffingtonpost.com/2014/03/05/student-hacking_n_4907344.html

Sridhar, V., & D. K. Ahuja. (2007). Challenges in managing information security in academic institutions: Case of MDI India. *Journal of Information System Security*, *3*(3), 51-78.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 441-469.

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26*(1), 2-12.

Verendel, V. (2009, September). Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 workshop on New security paradigms workshop*. Paper presented at the New Security Paradigms Workshop, Oxford, UK (pp. 37-50). New York: ACM.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91-95.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, *24*(1), 34.

Appendix – Questionnaire

Part A – to be filled for subsystems and modules

Instructions for items 1-8: For each item assign a value between 1 (none/very low) and 5 (very high).

1. To what degree will exposing or corrupting the information in the subsystem/module result with higher operational costs?

2. To what degree will exposing or corrupting the information in the subsystem/module cause work delays?

3. To what degree will exposing or corrupting the information in the subsystem/module result with damages to customers, other organizations or other systems related to the school?

4. To what degree will exposing or corrupting the information in the subsystem/module result with giving the school's competitors a considerable advantage?

5. To what degree will exposing or corrupting the information in the subsystem/module hinder future plans or operations of the school?

6. To what degree will exposing or corrupting the information in the subsystem/module cause panic among the public?

7. To what degree will exposing or corrupting the information in the subsystem/module result with severe disruption to the schools activities?

8. To what degree will exposing or corrupting the information in the subsystem/module hurt the school in the event of a state of emergency?

Instructions for items 9-10: For each item assign 1 (yes) or zero (no).

9. Are there in this category sensitive information requiring protection according to Protection of Privacy Act?

10. Is there in this category sensitive business information which the system depends on?

Instructions for items 11-12: For each item write an integer number.

11. How many people use the subsystem/module?

12. How many people are authorized to make changes or edit the subsystem/module?

Part B – to be filled only for modules

Instructions for items 13-20: For each item assign a value between 1 (none/very low) and 5 (very high).

13. How often were there attempts of attack / use the information in the module?

14. What is the degree of risk in the module compared to the business environment?

15. How motivated would be competitors to steal the information in the module?

16. How motivated would be inside people to steal the information in the module?

17. In the past, were there any threats or rumors about misuse of the information in this module?

18. What is the level of importance of the information in this module?

19. Are there materials or information in the module that are known only to authorized personnel that could leak out?

20. Are there any new risks that were not taken into account?

Biographies

Dr. Michael Dreyfuss is a tenured faculty member in the Department of Industrial Engineering and Management in the Jerusalem College of Technology. He holds a Ph.D. and an MSc. in Industrial Engineering from the Ben Gurion University of the Negev, a B.Sc. in Computer Sciences and B.Sc. in Industrial Engineering and Management from the Jerusalem College of Technology.

Dr. Yahel Giat is a tenured faculty member in the Department of Industrial Engineering and Management in the Jerusalem College of Technology. He holds a Ph.D. and an MSc. in Industrial Engineering from the Georgia Institute of Technology, an MSc. in Economics, a B.Sc. in Electrical Engineering and B.A. in Computer Sciences from the Israel Institute of Technology.