Information Security between Standards, Certifications and Technologies: An Empirical Study

Y. Benslimane [a], Z. Yang [a], B. Bahli [b]
[a] School of Information Technology, York University, Toronto, Canada
[b] Ted Rogers School of ITM, Ryerson University, Toronto, Canada

younes@yorku.ca
zyang@yorku.ca
bahli@ryerson.ca

Abstract— **This paper investigates the relative role of security standards, professional security certifications and technological tools in the protection of organizational data. Findings from the content analysis of 100 job postings for information security analysts and managers show that in general, organizations give more importance to knowledge validated by relevant professional certifications and to the working knowledge of IT products and solutions for the management of their information security than to the knowledge of a particular security standard. Details for such findings and their implications for research and practice are discussed.**

Keywords: Information security; Security standards; IT security certifications; Security tools and solutions

I. INTRODUCTION

Information Security (hereafter InfoSec) refers to the processes and methodologies that help protect the confidentiality, the integrity and the availability of private and sensitive information or data in its electronic and paper-based forms [1]. In today's context of organizations' heavy dependence on computer-based information systems and of more frequent and more severe computer security breaches, InfoSec has become a key challenge for researchers and practitioners alike. Previous research has shown that InfoSec remains a complex issue that involves human, organizational and technological factors and their interactions [2][3][4][5]. From this perspective, an organization's overall InfoSec is as strong as its weakest link.

An effective InfoSec requires a vast amount of knowledge from multiple domains to be systematically applied and updated [6][7][8][9]. The objective of this paper is to assess and analyze the relative importance of three categories of knowledge that has the potential to improve the quality of InfoSec in organizations, (i) the knowledge of best practices security standards promote, (ii) the knowledge covered and validated by specialized professional InfoSec certifications that complement a formal education in the field of Information Systems, Information Technology (hereafter IT) or Computer Science and (iii) the working knowledge of products and solutions used as technical controls to help protect IT assets.

The rest of the paper is organized as follow: Section 2 reviews the relevant literature on knowledge requirement for InfoSec practice, Section 3 describes the methodology used in this research, Section 4 presents the findings and discusses their implications for research and practice, and Section 5 concludes this paper.

II. LITERATURE REVIEW

Effective InfoSec requires that professionals working in that area of IT possess the knowledge necessary for the successful fulfillment of their duties. This paper focuses on the relative role for InfoSec practice of (i) knowledge based on best practices security standards promote, (ii) knowledge validated by professional InfoSec certifications and (iii) of working knowledge of InfoSec products and solutions.

Research on InfoSec and Information Security Management Systems (hereafter ISMS) has looked at international security standards such as ISO/IEC 27001, BS 17799, PCIDSS, ITIL, COBIT and national or regional standards such as NIST SP 800 series and GASSP as a comprehensive set of best practices that can help organizations effectively manage the security of their data and IT assets [10][11][12][13][14][15][16]. Research on ISMS has also covered the relatively low adoption of security standards and identified the reasons for this, including the time and cost involved in their implementation, their complexity and lack of implementation guidance [12][17][18][19], their excessively generic nature [20], the fact that compliance with security standards does not guarantee effective security [21][22] and the fact ISMS certifications do not improve an organization's stock market value or bottom line [14][18][23]. However, for organizations that did adopt a security standard, security cost reduction, security incident avoidance, implementation of best practices and pressure from customers, partners and competitors were the key drivers of that adoption [14][15][17].

Research on skill requirements has covered the importance for IT professionals to possess relevant and current knowledge that allows them to fulfill their duties successfully. It has argued that the ever-changing technology and the somewhat rigid curricula in formal Information Systems, IT and Computer Science post-secondary education programs tend create knowledge gaps and obsolete knowledge that force IT professionals to continuously complement their degrees with specialized certifications (which need to be maintained) in order to remain operational

978-1-5090-5493-0/16/$31.00 ©2016 IEEE

[24][25][26]. Typically, in the field of IT, third party organizations which include IT vendors, educational organizations and professional associations grant specialized professional certifications to individuals who pass a specific exam and, in some cases, possess a specific work experience, hence validating those individuals' skills and expertise [26].

Finally, technical and socio-technical approaches in InfoSec research have shown that IT products and solutions (such as firewalls, intrusion detection systems, identity access management systems, cryptography systems, security information and event management systems, etc.) and the related hands-on technical expertise are -or should be- part of any effective InfoSec program [27][28][29]. These tools and solutions are used as technical controls that are reviewed, selected, configured, tested, implemented and later audited in order to prevent unwanted security events, detect them or recover from them. In some cases, these technical controls are specified in security standards such as ISO/IEC 27000 series and NIST SP 800 series but all organizations -even those that do not adopt such standards- tend to apply them.

III. Methodology

The main objective of this paper is to examine the relative importance and role of security standards, of professional certifications and of technological tools for InfoSec practice. In principle, all three can help improve InfoSec and this research will provide a picture on how organizations use these three categories of knowledge to protect their data and other IT assets.

For that purpose, a random sample of 100 relevant job postings (50 with the key words "Information security analyst" and 50 with the key words "information security manager" in "job title") published during the month of June 2016 by the US site monster.com was selected and the content of those ads was analyzed to identify the key domains of knowledge used to manage InfoSec in practice. The coding for the content analysis of the 100 job postings involved two researchers to avoid any bias in the study. The frequencies (added in the following tables and sections) indicate the number of times the knowledge of a particular security standard (and a particular task of interest linked to that standard), of a particular professional certification or of a particular type of IT products or solutions is listed as required or desired in the postings for each job category.

Knowledge related to relevant university degrees and to relevant work experience was not considered as these qualifications were required or desired in most postings. It is worth noticing that knowledge related to relevant work experience is captured by some professional certifications like the ones for CISSP, CISM and CISA, which require passing an exam and submitting verified evidence of appropriate work experience. This study did not consider knowledge related to US regulatory frameworks such as HIPAA, SOX, GLBA, HITECH either as compliance with such pieces of US regulations and legislations does not equal compliance with an ISMS standard.

This examination of the job postings will explore the relative role of security standards, professional certifications and IT products and solutions by identifying and analyzing the related knowledge requirements and responsibilities for entry-level and managerial-level InfoSec positions.

IV. Findings and Discussion

Table 1 summarizes the findings related to InfoSec knowledge required or desired in the areas of security standards, professional certifications and IT products. In terms of relative significance of the three domains of knowledge, findings show that, in general and for both job categories considered, organizations give more importance to relevant professional certifications and to familiarity with IT products and solutions for the management of their InfoSec than to the working knowledge of a particular security standard. However, findings show some overall differences within the InfoSec job categories considered. Hence, compared to analysts, managers are more often expected to be knowledgeable of security standards (62% versus 54%) and to be certified (82% versus 74%). There was no difference between analysts and managers in terms of overall (i.e., as measured and presented in Table 1) knowledge requirement related to InfoSec tools.

TABLE I: InfoSec Knowledge Required or Desired

	Analyst (N = 50)	Manager (N = 50)	Total (N = 100)
Security standard			
- **Yes**	27 (54%)	31 (62%)	58 %
- **No**	23 (46%)	19 (38%)	42%
Professional certification			
- **Yes**	37 (74%)	41 (82%)	78%
- **No**	13 (26%)	9 (18%)	22%
IT products and solutions			
- **Yes**	38 (76%)	38 (76%)	76%
- **No**	12 (24%)	12 (24%)	24%

A. Importance of Security Standards

Table 1 shows that knowledge related to security standards is required or desired in 54% of the postings in the case of analysts and 62% in the case of managers, averaging 58% in our sample. Also, in the majority of the cases (81.5%, for the analysts and 61.3% for the managers) when knowledge of a security standard was required or desired, the posting listed more than one standard. However, because the certification of compliance with security standards is not always mandatory [18], this content analysis could not differentiate organizations that formally adopted such security standards with the objective of obtaining the related certification and/or accreditation from those that, partially or fully, applied the knowledge related to a security standard without seeking the related certification and/or accreditation.

Table 2 presents the key security standards whose knowledge is required or desired. Findings show some small differences in the ranking of standards between the InfoSec positions considered but, overall, the most common standard is NIST (National Institute of Standards and Technology) SP (Special Publications) 800 series, a US federal government standard that describes a risk management framework and

computer security policies, procedures and guidelines [10]. This relative predominance of NIST SP 800 series -as a US standard- may be explained by the fact that this research uses US job postings only. PCIDSS (Payment Card Industry Data Security Standard), an international standard that specifies security requirements for payment data [10][11] and ISO 27000 series, an international standard that specifies the requirements for an ISMS applicable to any type of organization [10][11] are both ranked second. In forth position comes SSAE 16 (Statement on Standards for Attestation Engagements 16), a US framework that provides guidance for evaluating and reporting on internal controls at a service organization followed by COBIT (Control Objectives for Information and Related Technologies), a set of -international- best practices for IT governance, including IT risk management developed by ISACA [11], and by ITIL (Information Technology Infrastructure Library), an international IT Service Management standard that also covers aspects of security management. This research has also identified other US federal and North American standards (such as HITRUST, FFIEC, DODI 8500, NERC CIP) whose knowledge is required or desired, but their frequencies were marginal.

TABLE 2: KEY SECURITY STANDARDS REQUIRED OR DESIRED

	Analyst	Manager	Total
NIST SP 800 series	23	17	40
PCIDSS	13	19	32
ISO/IEC 27000 series	13	19	32
SSAE 16	10	6	16
COBIT	4	6	10
ITIL	1	2	3
Other	7	4	11

Next, tasks and responsibilities in the postings requiring or desiring knowledge of security standards were analyzed to determine how these frameworks eventually shape some of InfoSec professionals' duties. This subsequent analysis focused on two specific tasks and their related frequencies. The results presented in Table 3 show that only 6% of all postings list "supporting and maintaining the certification and accreditation requirements" as a duty for InfoSec professionals, which most likely suggests that only a very small percentage of the organizations in our sample formally adopt a security standard and seek the relevant certification and/or accreditation. The results also show that some organizations use the standards' guidelines to optimize their InfoSec processes and implement best security practices (15% of all postings). The rest of the tasks and responsibilities listed in the postings could not be mapped exclusively to security standards and were therefore excluded from this subsequent analysis related to security frameworks.

TABLE 3: SPECIFIC TASKS RELATED TO SECURITY FRAMEWORKS

	Analyst	Manager	Total
Support certification process	3	3	6
Improve InfoSec processes	11	4	15

B. Importance of Professional Certifications

As indicated in Table 1, knowledge related to professional InfoSec certifications is required or desired in 74% of the postings in the case of analysts and 82% in the case of managers and averages 78%. Furthermore, it was noticed during the content analysis that when a job posting listed an InfoSec professional certification as required or desired, it enumerated more than one certification. Table 4 provides the details for the key desired or required professional certifications identified in this study.

TABLE 4: KEY INFOSEC CERTIFICATIONS REQUIRED OR DESIRED

	Analyst	Manager	Total
CISSP	25	40	65
CISM	11	26	37
GIAC Security Essentials	12	14	26
CISA	10	14	24
CEH	5	5	10
Security +	5	3	8
GIAC GCIH	6	1	7
Other GIAC certifications	12	6	18
Various Cisco certifications	7	8	15
Various Microsoft certifications	7	6	13

Findings show that vendor-neutral certifications are the most commonly required or desired. They also show some differences between entry-level and managerial InfoSec positions. Overall, the CISSP (Certified Information Systems Security Professional) certification which currently covers 8 security domains (including risk management, network security, security assessment and testing and security operations) and requires up to 5 cumulative years of full-time relevant work experience is by far the most frequently required or desired for both job categories. CISM (Certified Information Security Manager) certification which focuses on InfoSec, covers topics such as governance, compliance and InfoSec program development and management and also requires up to 5 years of full-time relevant work experience is ranked second overall. GIAC (Global Information Assurance Certification) SEC (Security Essentials) -or GSEC- and CISA (Certified Information Systems Auditor) certifications rank third and fourth respectively. GSEC covers more or less the same content as the CISSP certification but does not require any relevant work experience, whereas CISA covers topics related to IT auditing including IT security and requires up to 5 years of full-time relevant work experience.

Other vendor-neutral certifications identified include Certified Ethical Hacker (CEH), an intermediate-level credential specialized in ethical hacking, Security+ which covers more or less the same domains of IT security as the CISSP certification, followed by certifications for analysts specialized in penetration testing and ethical hacking, in incident handling, in intrusion analysis and in forensics and by certifications for managers in ethical hacking and in management of security.

With regards to the vendor-specific credentials, Cisco certifications and Microsoft certifications are the most common and refer to the importance of optimal

configuration of IT products (in these cases networking devices and network operating systems) for InfoSec practice.

C. Importance of InfoSec Products and Solutions

Findings from Table 1 indicate that knowledge related to InfoSec technological tools is desired or required in 76% of the postings for analysts and for managers. Here as well, it was noticed during the analysis of the job postings that when an ad listed an InfoSec tool whose working knowledge was required or desired, it enumerated more than one of such products or solutions. Table 5 summarizes the details for findings related to InfoSec tools.

TABLE 5: KEY INFOSEC PRODUCTS AND SOLUTIONS IDENTIFIED

	Analyst	Manager	Total
Traditional security products	**98**	**70**	**168**
- Firewalls, IDS & IPS	34	19	53
- Network operating systems	11	13	24
- Access control systems	17	6	23
- Antivirus & anti-malware	10	6	16
- Bus. continuity & incident mgt	6	10	16
- Encryption systems	8	6	14
- Other products	12	10	22
Advanced security products	**38**	**40**	**78**
- SIEM & monitoring tools	17	23	40
- Pen-test & vulnerability scan.	17	14	31
- Computer forensics tools	4	3	7

Results from this study show that job postings refer to various types of security tools that protect IT assets connected an organization's computer networks. Findings also show that, overall, knowledge of traditional security products such as perimeter technologies (which include firewalls and intrusion detection and protections systems), network operating systems and identity and access management systems is more frequently required or desired than knowledge of advanced security products such as security event monitoring tools, vulnerability scanning tools and computer forensic tools, but this may be explained by the classification itself used in Table 5 since the "Traditional Security Products" category includes more types of products than the "Advanced Security Products" category.

An analysis at the level of individual types of products shows that the top 5 varieties of security tools job postings refer to are (i) traditional perimeter technologies (firewalls, intrusion detection systems and intrusion protection systems) that serve as a first line of defense against threats to resources on a network, (ii) SIEM (Security Information and Event Management) tools that provide advanced real-time monitoring and analysis of security events detected by network hardware and applications, (iii) penetration testing and vulnerability scanning tools that complement each other to identify possible weaknesses and prevent security attacks and violations, (iv) network operating systems and (v) identity and access management systems, two controls that protect against unauthorized access.

Results also show that professionals at entry-level positions are, in many cases, expected to be familiar with more InfoSec tools than professionals at managerial-level positions.

D. Implications for Research and Practice

Although it cannot differentiate the organizations that have formally adopted a security standard with the objective of obtaining the relevant certification from those that use such standards in an informal fashion, this study shows that, organizations tend to rely more on knowledge validated by specialized professional certifications and on the working knowledge of IT products and solutions than on knowledge from security standards to protect their data.

Despite promoting best practices and possibly improving InfoSec awareness and quality, security standards are in general given a relatively lower importance in practice. This is consistent with findings from previous research showing the low adoption of security standards [12][18][19][20]. However, this relatively lower importance given to security standards does not mean that organizations do not have an ISMS since InfoSec professionals typically develop, enforce and review security policies, manage security awareness and training programs, perform risk assessments, develop relevant security controls and audit them, monitor and analyze security events and resolve the security issues encountered daily [30]. It means however that their ISMS is not always in compliance with a recognized set of coherent best practices, and that, as a result, it can be improved [12][13]. In this context, researchers and practitioners must look for ways to reduce the complexity of security standards and make their perceived benefits more evident in order to increase their adoption rate.

This study also shows that, besides their -probably nonstandard- ISMS, organizations tend to rely heavily on the knowledge validated by some key specialized certifications and on the working knowledge of crucial IT products and solutions to protect their data.

V. CONCLUSION AND FUTURE RESEARCH

This paper focuses on the relative role of security standards, professional certifications and technological tools for InfoSec practice. A key findings from the analysis of relevant InfoSec job postings is that organizations tend to rely more on the knowledge professional certifications validate and on the working knowledge of IT products for the protection of their data than on the working knowledge of a security standard. The picture of InfoSec practice this study provides can guide researchers' and practitioners' improvement efforts in that area of IT.

Future research can be expanded to also include postings from other countries to avoid the possible bias related to the exclusive focus on US job ads. Future research can also link the aspects of knowledge requirements covered in this paper to the quality of InfoSec in organizations. Finally, future research can investigate how security standards are used in organizations that do not seek the related certification.

REFERENCES

[1] https://www.sans.org/

[2] Z.A. Soomro, M.H. Shah and J. Ahmed: "Information Security Management Needs a More Holistic Approach: A Literature Review", International Journal of Information Management, vol. 36, 2016, 215-225

[3] M. Silic and A. Back: "Information Security: Critical Review and Future Directions for Research" Information Management & Computer Security, vol. 22, 3, 2014, 279-308.

[4] R. Werlinger, K. Hawkey and K. Beznosov: "An Integrated View of Human, Organizational and Technological Challenges of IT Security Management", Information Management & Computer Security, vol.17, 1, 2009, 4-19

[5] S. Kramer, P. Carayon and J. Clem: "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities", Computers & Security, vol. 28, 2009, 509-520

[6] A. Zuccato, N. Daniels and C. Jampathom: "Service Security Requirement Profiles from Telecom: How Software Engineers May Tackle Security", 6th Conference on Availability, Reliability and Security, Vienna, Austria, 2011, 521-526

[7] S. Kesh and P. Ratnasingam: "A Knowledge Architecture for IT Security", Communications of the ACM, vol.50, 7, 2007, 103-108\

[8] Q. Ma, A. Johnston and J.M. Pearson: "IT Security Management Objectives and Practices: A Parsimonious Framework", Information Management & Computer Security, vol.16, 3, 2008, 251-270

[9] A.J.T. Chang and Q.J. Yeh: "On Security Preparation against Possible IS Threats across Industries", Information Management & Computer Security, vol.14, 4, 2006, 343-360

[10] C. Gicas: "A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards", Information Security Journal: A Global Perspective, vol. 19, 2010, 132-141

[11] H. Susanto, M.N. Almunawar and Y.C. Tuan: "Information Security Management System Standards: A Comparative Study of the Big Five", International Journal of Electrical & Computer Sciences IJECS-IJENS, vol.11, 5, 2011, 23-29

[12] A. Gillies: "Improving the Quality of Information Security Management Systems with ISO27000", The TQM Journal, vol. 23, 4, 2011, 367-376

[13] A. Tsohou, S. Kokolakis, C. Lambrinoudakis and S. Gritzalis: "A Security Standards' Framework to Facilitate Best Practices' Awareness and Conformity", Information Management & Computer Security, vol.18, 5, 2010, 350-365

[14] T. Wander: "Positive and Negative Findings of ISO/IEC 17799 Framework", 18th Australasian Conference on Information Systems, Toowoomba, Australia, 2007, 622-631

[15] R. van Wessel, X. Yang and H.J. de Vries: "Implementing International Standards for Information Security Management in China and Europe: a Comparative Multi-Case Study", Technology Analysis & Strategic Management, vol. 23, 8, 2011, 865-879

[16] G. Ataya: "PCI DSS Audit and Compliance", Information Security Technical Report, vol. 15, 2010, 138-144

[17] K. Hone and J.H.P. Eloff: "Information Security Policy – What Do International Information Security Standards Say", Information Security Policy, 2002, 402-409

[18] V.V. Fomin, H.J. de Vries and Y. Barlette: "ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption", 3rd European Conference on Management of Technology, Nice, France, 2008, 1-13

[19] M. Siponen: "Information Security Standards Focus on the Existence of Process Not its Content", Communications of the ACM, vol.49, 8, 2006, 97-100

[20] M. Siponen and R. Willison: "Information Security Management Standards: Problems and Solutions", Information & Management, vol.46, 2009, 267-270

[21] B. Duncan and M. Whittington: "Compliance with Standards, Assurance and Audit: Does this Equal Security?", 7th International Conference on Security of Information and Networks, Glasgow, 2014, 1-8

[22] T. Wiander: "Implementing the ISO/IEC 17799 Standard in Practice – Experiences on Audit Phases", 6th Australasian Information Security Conference, Wollongong, Australia, 2008, 115-119

[23] C. Hsu, T. Wang and A. Lu: "The Impact of ISO 27001 Certification on Firm Performance", 49th Hawaii International Conference of Systems Sciences, 2016, 4842-4848

[24] B. Prabhakar, C.R. Litecky and K. Arnett: "IT Skills in a Tough Job Market", Communications of the ACM, vol.48, 10, 2005, 91-94

[25] M.J. Gallivan, D.P. Truex and L. Kvasny: "Changing Patterns in IT Skill Set 1988-2003: A Content Analysis of Classified Advertising", The Data Base for Advances in Information Systems, vol. 35, 3, 2004, 64-87

[26] J.W. Gabberty: "Educating The Next Generation of Computer Review of Security Professionals: The Rise and Relevancy of Professional Certifications", Review of Business Information Systems, vol. 17, 3, 2013, 85-98

[27] S. Ji, J. Wang, Q. Min, and S. Smith-Chao: "Systems Plan for Combating Identity Theft - A Theoretical Framework", IEEE International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 2007, 6402–6405.

[28] T. Kayworth and D. Whitten: "Effective Information Security Requires a Balance of Social and Technology Factors", MIS Quarterly Executive, vol. 9, 3, 2010, 163–175

[29] R. Young and J. Windsor: "Empirical Evaluation of Information Security Planning and Integration", Communications of the Association for Information Systems, vol. 26, 1, 2010, 245–266

[30] A. Patel, Y. Benslimane, B. Bahli and Z. Yang: "Addressing IT Security in Practice: Key Responsibilities, Competencies and Implications on Related Bodies of Knowledge". IEEE International Conference on Information Engineering and Engineering Management, Honk Kong, 2012, 899-903