WARWICK
THE UNIVERSITY OF WARWICK

Original citation:
Safa, Nader Sohrabi, Maple, Carsten and Watson, Tim. (2017) The information security landscape in the supply chain. Computer Fraud & Security, 6. pp. 16-20.

Permanent WRAP URL:
http://wrap.warwick.ac.uk/91426

Copyright and reuse:
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:
© 2017, Elsevier. Licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International http://creativecommons.org/licenses/by-nc-nd/4.0/

A note on versions:
The version presented here may differ from the published version or, version of record, if you wish to cite this item you are advised to consult the publisher's version. Please see the 'permanent WRAP URL' above for details on accessing the published version and note that access may require a subscription.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

warwick.ac.uk/lib-publications

Information Security Landscape in Supply Chain

Nader Sohrabi Safa*[a], Carsten Maple[b], Tim Watson[c]
Cyber Security Centre at WMG, University of Warwick, Coventry, United Kingdom[a,b,c]
Email: n.sohrabi-safa@warwick.ac.uk[a], CM@warwick.ac.uk [b], TM@warwick.ac.uk [c]

Abstract

Information security is an important issue in supply chain. Information security breaches have serious consequences for companies, such as loss of revenue, reputation, customers, business advantages, and, in the worst-case scenario, bankruptcy. On the other hand, collaboration and integration between different parties is necessary to increase productivity in the supply chain. However, increasing the flow of information increases the risk of information leakage. To mitigate the risk of information security breach in the supply chain we need to have a comprehensive view about information security. This research aims to investigate different dimensions of information security in the supply chain. A review of literature revealed that technological, managerial, organizational, psychological, educational and awareness aspects of information security play important roles in the security of information in supply chain.

Keywords: Information security, organisation, management, policy, human aspects, employee

1. Introduction

Information security breaches have serious consequences for companies; moreover, information security breaches negatively influence national security in the domain of the military industry. Selling information concerning industrial design, organisational strategic plans, customers, experts and other valuable information for monetary benefit, getting revenge, bribery, and embezzlement are some examples of the human aspects of information security [1]. In addition, hackers use novel and creative methods to access information assets. Different kinds of phishing, social engineering, and misleading software are examples of methods typically used to achieve their target [2]. Users, intentionally or unintentionally, are a source of risk for information assets. Information security threats can be divided into two categories – insider and outsider threats. Insider threat refers to the transfer of information to illegitimate parties by the employees who has access to the relevant information. Anonymity of the insider is an advantage that encourage employees to engage in illegal activities in this domain [3]. Insider threats are hard to detect and experts can only detect information security misconduct after several weeks or months in some cases. Virus, Spyware, Worm, Adware, keyloggers, Trojans, Scumware, Dialers, and Browser Hijackers are examples of technological threats in this domain. Intrusion detection play an important role in preventing the negative effect of these kinds of attacks. Cryptography also helps experts in this domain increase the confidentiality of information. We can see a wide spectrum of threats to information assets in the supply chain [4]. Companies should have a comprehensive plan to protect their information; management plays important role in decreasing the negative effect of information security threats. Motivational plans encourage employees to share their information security knowledge and increase information security awareness [5]. Information security collaboration is another effective approach in this domain. Experts believe that complying with organisational information security policies and procedures significantly mitigates information security threats [6]. Reliable reports show the growth of information security incidents, despite tremendous efforts to predict and prevent information security breaches [7]. This is due to variety of threat to information. Human, technological, managerial, educational and awareness, social, and cultural dimensions of information security should be taken into consideration when determining how to have a secure environment for information in the supply chain. This research endeavours to shed some light on different dimensions of information security for academics and practitioners.

2. Technological aspects

People, technology and processes are the main entities in information security [8]. The technological dimension of information security refers to all aspects that relate to software, hardware and process. Anti-virus, antimalware, anti-spam, anti-phishing, anti-spyware, firewall, authentication, and intrusion detection are examples of technological aspects of information security. Table 1 shows the definition of several threats that can be solved using the technological aspects of information security.

Table 1: Examples of malware on the Internet

Threats	Definitions
Adware	Programs that monitor internet users' online activities in order to initiate pop-up advertising or other targeted marketing activities.
Keyloggers	Programs that capture and record internet users' every keystroke, including personal information and passwords.
Trojans	Malicious programs that appear as harmless or desirable applications, but are designed to cause loss or theft of computer data, or even to destroy the system.
Scumware	Programs that alter the content of web sites internet users are accessing, changing the normal links to reroute them to other web sites.
Dialers	Programs typically used by vendors serving pornography via the internet.
Browser Hijackers	Programs that run automatically every time internet users start their internet browser to gather information on the users' surfing habits.

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for the purpose of malicious activity or policy violations [9]. Cryptography is another technological aspect that provides for secure data transfer. Biometric devices are pieces of hardware that measure human characteristics such as finger prints, palm veins, face recognition, DNA, palm prints, hand geometry, iris recognition, and retina patterns for authentication and access control purposes [10]. Table 2 show the pros and cons of hardware and software information protection.

Table 2: Hardware and software protection

Characteristics	Software based protection	Hardware based protection
Nature	Dynamic	Static
Maintenance cost	Low	High
Development cost	Low	High
Access to implementation	Direct and unlimited	Indirect and limited
Exploitable	High	Low
Renewable	Easy	Demanding
Deployability	Easy	Demanding
Diversity of Exploitable tools	High	Low

3. Human aspects

Experts believe that human aspects of information security should be taken into consideration in addition to technological aspects of information security in order to achieve a secure environment for information assets in organisations [11]. The human aspects of information security concern the information security risks that originate intentionally or unintentionally from human mistakes. Carrying un-encrypted organisational information by external hard disk or pen drive, sharing user names and passwords with colleagues, writing account information on sticky paper which is then placed on a monitor or desk, using social numbers as usernames and passwords, leaving unattended a system with a logged-in status, opening an unknown email and downloading its attachments, and downloading any software from the internet are examples of relevant human mistakes. Humans, intentionally or through negligence, are a great potential risk to the security of information assets [12]. Although, individuals' characteristics, psychology, awareness, and knowledge play important roles in this domain, management can use proper policies and plans to reduce these kinds of risks in organisations. Table 3 shows different reasons for employees' misbehaviour in the domain of information security.

Table 3: Different reasons for human misbehaviour

Type of mistakes	Reasons
Intentionally	Gaining benefit
	Getting revenge
	Anger
	Fear of losing job
	Pleasure and entertainment
	Bribery
	Embezzlement
	Espionage
	Sabotage
Unintentionally	Resistance
	Apathy
	Ignorance
	Lack of awareness
	Mischievous
	Negligence

4. Managerial aspects

Information security management refers to all aspects of prediction, prevention, and control of information security risks [13]. Management plays an important role in the success of protecting organisational information assets. Their plans and policies decrease the risk of information security incidents in companies [14]. Increasing information security awareness and knowledge [15], encouraging employees to collaborate in information security [16], providing and complying with organisational information security policies and procedures [17], surveillance and control of employees access [18], increasing productivity in the information security response team [19], and inculcating commitment in employees to protect information assets are examples of management roles in the domain of information security. Information security management is incomplete without considering the important role of management.

5. Educational and Awareness aspects

Technology has positively affected information security. That is why attackers have shifted their attention and efforts onto human elements in order to achieve their targets. In this dynamic environment, users' information security awareness and knowledge play an important role in mitigating the risk of information security [20]. Experts divide information delivery methods into three groups: contextual, web-based material and embedded training methods. Video-based, game-based, and text-based delivery methods are other types of methods that increase the information security knowledge and awareness of users [15].

Table 4: Awareness Approaches

Awareness Approaches	Description	Advantages/disadvantages
Conventional methods	These are paper-based and electronic-based delivery methods. Posters, newsletters, news clippings, and memos are examples of this method.	Message may be overlooked. Newsletters are periodic (e.g. monthly or quarterly) Newsletter can target a group of audience.
Instructor-led delivery methods	A variety of formal presentations (e.g. brown-bag seminars and classroom style workshops) facilitated by local or external information security experts.	One of the advantages of the instructor led delivery method is that the instructor is able to perceive nonverbal student cues, modify instructional methods accordingly, and provide timely answers to student questions.
Online delivery methods	Online delivery methods include e-mail broadcasting, online synchronous and asynchronous discussion, information uploading, blogging, animation, and multimedia.	These delivery methods are tine-independent and generally well suited for supporting multimodal teaching methods over different geographical areas.
Game-based delivery methods	Online games combine graphics, play and training concepts to create compelling training experiences.	They can challenge, motivate and engage the participants.
Video-based delivery methods	Online video is a medium that provides visual and audio learning for participants. Learners can study independently and learn at their own pace and only what they need to know.	There is no need for a classroom trainer or to have staff who cannot be reached through e-learning courseware. Learners can also start and stop the training as their schedule permits because it is not time-dependant.
Simulation-based delivery methods	In a simulation-based delivery method, users are sent simulated phishing emails to test users' vulnerability to phishing attacks and this is then followed-up with training.	A similar approach, called embedded training that teaches users about phishing during their regular use of email.

6. Social and cultural aspects

The prevention of damage, loss, unauthorised access or destruction to information is vital for organisations. External and internal threats continually grow and result in breaches. Employees' behaviour is the root of many information security breaches [21]. Reliable reports show that internal threats have significantly increased in comparison with previous years [7, 22]. Users' errors, negligence, and intentionally malicious attacks are reasons for the information security breaches. [23] categorised users' behaviour into four categories: security assurance behaviour, security damage behaviour, security risk-taking behaviour, and security complaint behaviour. The management of human error should be priority in organisations. A strong information security culture can contribute to mitigating vulnerabilities stemming from individuals' behaviour [24]. Infrequent back-up of information, using email accounts to send sensitive and confidential information, carrying unencrypted sensitive and confidential information on external hard disk or other movable devices, unlawful use of information, and unauthorised transfer of information are problems that can be solved by replacing proper information security culture [25]. Information security culture covers the entire information life cycle – collection, storage, use, and transfer. Regulatory requirements, customer preferences and expectations, and geographical distribution are external factors that influence information security culture [21]. Regulation protecting personal and financial information influences the customer information process. This determines how long customer records should be kept. Values, attitudes, norms, assumptions, beliefs and knowledge are important factors in culture formation. Protection of information and privacy is a value in information security culture. Illegal transfer of information to unauthorised parties is a negative behaviour (attitude). Everybody knows that he or she should put his/her effort into avoiding any behaviour that jeopardises information confidentiality (assumption).

7. Supply chain information security

The supply chain environment has distinctive characteristics that separate it from the environment found within a single organisation. Integration and collaboration amongst companies is necessary in order to increase productivity [21]. Consequently, the flow of information between different parties at a certain level exists in supply chains. Technical aspects of information security play an important role, but it is not enough. Movement of talented employees, disgruntled staff, use of temporary experts, the lack of awareness in complying with organisational information security policies are reasons for information security breaches [26, 27]. Selling information for monetary benefits, bribery, embezzlement, espionage, and apathy are other roots of information leakage that manifest human, managerial, educational and social aspects of information security [26]. The supply chain has an expanded environment with several layers that increase the risk to information assets. Attention to all aspects of information security is recommended by experts, in order to guarantee an environment with less risk for information assets.

8. Conclusion

In this study, we have investigated the different aspects of information security that influence the availability, confidentiality and integrity of information assets in supply chains. This investigation shows a variety of dimensions that it is necessary for experts take into consideration when attempting to mitigate information security breaches. We highlight the important points in the domain of information security as follows:

- Information security is a corporate governance responsibility for all employees
- Information security is not only a technical issue, it is a multi-dimensional discipline: technological, managerial, human, educational and awareness, social and cultural, psychological, law and enforcement, and so forth.
- Identification of risk in the supply chain is essential.
- Complying with organisational information security policies and procedures is vital.

- Information security awareness plays an important role in mitigating the risk of information security breaches.
- Control and surveillance mitigate the risk of information security incidents by employees.

Awareness plays an important role in mitigating the risk of information security, different training methods are recommended. However, information security knowledge sharing can be an effective and efficient approach. It is acknowledged that motivation for knowledge sharing among employees is not enough to engage in these kinds of activities. This constitutes the subject matter of future research.

Reliable reports show that employees do not comply with organisational information security policies and procedures. Increasing commitment, attachment to the organisation, involvement in information security and changing their belief have been mentioned as effective and efficient approaches. However, there is scant research that investigates motivational factors (intrinsic and extrinsic) on employee behaviour. This also can constitute the starting point for future research. Increasing the accuracy of threat recognition, and decreasing fault alarms can also be a topic for future research in the technological domain.

References

1. Padayachee, K. *A conceptual opportunity-based framework to mitigate the insider threat*. in *Information Security for South Africa, 2013*. 2013.
2. Safa, N.S., et al., *Information security conscious care behaviour formation in organizations.* Computers & Security, 2015. **53**(0): p. 65-78.
3. Cheng, L., et al., *Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory.* Computers & Security, 2013. **39, Part B**(0): p. 447-459.
4. Bartol, N., *Cyber supply chain security practices DNA – Filling in the puzzle using a diverse set of disciplines.* Technovation, 2014. **34**(7): p. 354-361.
5. Tamjidyamcholo, A., et al., *Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language.* Computers & Education, 2013. **68**(0): p. 223-232.
6. Sohrabi Safa, N., R. Von Solms, and S. Furnell, *Information security policy compliance model in organizations.* Computers & Security, 2016. **56**: p. 70-82.
7. Verizon, *Data Breach Investigations Report (DBIR 2015)*. 2015, Verizon: United States. p. 1-70.
8. Safa, N.S., R.v. Solms, and L. Futcher, *Human aspects of information security in organisations.* Computer Fraud & Security, 2016. **2016**(2): p. 15-18.
9. Zhou, C.V., C. Leckie, and S. Karunasekera, *A survey of coordinated attacks and collaborative intrusion detection.* Computers & Security, 2010. **29**(1): p. 124-140.
10. Yang, Y. and B. Padmanabhan, *Toward user patterns for online security: Observation time and online user identification.* Decision Support Systems, 2010. **48**(4): p. 548-558.
11. Parsons, K., et al., *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q).* Computers & Security, 2014(0).
12. Safa, N.S. and C. Maple, *Human errors in the information security realm – and how to fix them.* Computer Fraud & Security, 2016. **2016**(9): p. 17-20.
13. Soomro, Z.A., M.H. Shah, and J. Ahmed, *Information security management needs more holistic approach: A literature review.* International Journal of Information Management, 2016. **36**(2): p. 215-225.
14. von Solms, B. and R. von Solms, *The 10 deadly sins of information security management.* Computers & Security, 2004. **23**(5): p. 371-376.
15. Abawajy, J., *User preference of cyber security awareness delivery methods.* Behaviour & Information Technology, 2014. **33**(3): p. 236-247.
16. Werlinger, R., et al., *Security practitioners in context: Their activities and interactions with other stakeholders within organizations.* International Journal of Human-Computer Studies, 2009. **67**(7): p. 584-606.
17. Ifinedo, P., *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.* Information & Management, 2014. **51**(1): p. 69-79.
18. Herath, T. and H.R. Rao, *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.* Decision Support Systems, 2009. **47**(2): p. 154-165.
19. Ahmad, A., J. Hadgkiss, and A.B. Ruighaver, *Incident response teams - Challenges in supporting the organisational security function.* Computers & Security, 2012. **31**(5): p. 643-652.
20. Haeussinger, F.J. and J.J. Kranz. *Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior*. in *International Conference on Information Systems 2013*. 2013.
21. Da Veiga, A. and N. Martins, *Information security culture and information protection culture: A validated assessment instrument.* Computer Law & Security Review, 2015. **31**(2): p. 243-256.
22. Schulze, H., *Insider Threat Spotlight Report*. 2015, Information Security Community on LinkedIn. p. 1-36.

23. Guo, K.H., *Security-related behavior in using information systems in the workplace: A review and synthesis.* Computers & Security, 2013. **32**: p. 242-251.
24. AlHogail, A., *Design and validation of information security culture framework.* Computers in Human Behavior, 2015. **49**: p. 567-575.
25. Van Niekerk, J.F. and R. Von Solms, *Information security culture: A management perspective.* Computers & Security, 2010. **29**(4): p. 476-486.
26. Roy Sarkar, K., *Assessing insider threats to information security using technical, behavioural and organisational measures.* Information Security Technical Report, 2010. **15**(3): p. 112-133.

27. Albrechtsen, E. and J. Hovden, *Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study.* Computers & Security, 2010. **29**(4): p. 432-445.