The information security landscape in the supply chain


Nader Sohrabi Safa


Carsten Maple


Tim Watson

Nader Sohrabi Safa, Carsten Maple and Tim Watson, Cyber Security Centre at WMG, University of Warwick

Information security breaches have serious consequences for companies. And information security breaches in the defence industry negatively impact national security. Selling information concerning industrial design, organisational strategic plans, customers, experts and other valuable information for monetary benefit, revenge, bribery and embezzlement are just some examples of the human dimension 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 the methods typically used to achieve their aims.[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. Insider threat refers to the transfer of information to illegitimate parties by employees who have access to sensitive information. The anonymity of the insider is an advantage that encourages 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. Viruses, spyware, worms, adware, keyloggers, trojans, scumware, diallers and browser hijackers are examples of technological threats in this domain. Intrusion detection plays 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 and management plays an 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 the variety of threats to information. The human, technological, managerial, educational and awareness, social and cultural dimensions of information security should be taken into consideration when determining how to create 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.

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 processes. Anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewalls, authentication and intrusion detection

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 websites that Internet users are accessing, changing the normal links to reroute them to other websites.
Diallers	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.

Table 1: Examples of malware on the Internet.

are examples of the technological aspects of information security. Table 1 shows the definition of several threats that can be solved using the technological aspects of information security.

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 fingerprints, 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.

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

Table 2: Hardware and software protection.

Human aspects

Experts believe that the human aspects of information security should be taken into consideration in addition to the technological aspects 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 unencrypted organisational information on an external hard disk or pen drive, sharing usernames and passwords with colleagues, writing account information on a sticky note that 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.

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. Management's plans and policies decrease the risk of information security incidents in companies.[14]

Increasing information security awareness and knowledge, encouraging employees to collaborate in information security, providing and complying with organisational information security policies and procedures, surveillance and control of employees access, increasing productivity in the information security response team and inculcating commitment in employees to protect information assets are examples of management roles in the domain of information security.[15-19] Information security management is incomplete without considering the important role of management.

Education and awareness

Technology has positively affected information security. That is why attackers have shifted their attention and efforts towards the human elements in order to achieve their aims. 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]

Social and cultural aspects

The prevention of damage, loss, unauthorised access to or destruction of 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]

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
	Mischievousness
	Negligence

Table 3: Various reasons for human misbehaviour.