Year 1

The Importance of Security in Information Systems and Some of the Threats that the Human Factor Presents to Information Systems Security

STUDENT NAME: DAN-MARIUS BRADEA
STUDENT ID: 20044497
COURSE: INTRODUCTION TO INFORMATION SYSTEMS (CC4057)

STUDENT EMAIL: DAB1108@MY.LONDONMET.AC.UK

SUBMITED TO: DR. ALEXANDROS CHRYSIKOS (LECTURER)
MS SUBEKSHA SHRESTHA (ASSOCIATE LECTURER)

DATE:

Table of Contents

Chapter 1: Introduction

As we moved through the 20th century and into the 21st century, we used to say that technology was more and more present in our lives, but it is obvious that today this is an understatement because society would not be as it is today without technology and all its intricacies. Its presence dominates absolutely every aspect of our life making it impossible for civilisation to move on without, hence the need for systems to organise and use all the information that is being generated. All these delicate connections that arose from this constant dependency on technology and these systems are called Information Systems.

The two papers discussed in this essay show the evolution and importance of Information Systems, in particular the role that Information Systems Security plays in everyday work life. Information Systems emerged to improve the financial system, in essence helping companies of all sizes to increase their wealth making it possible for them to enhance business operations, facilitate management decision-making, deploy business strategies and more. Today Information Systems have exponentially more applications, being involved in every operational and organisational aspect of modern companies.

Chapter 2: Research methodologies

The research methods employed in this essay are integrative review and historical review.

2.1 Integrative Review

Onwuegbuzie defines the integrative review as "a form of research that reviews, critiques, and synthesizes representative literature on a topic in an integrated way such that new ideas and opinions on the topic are generated. The body of writings includes all studies that address related or identical hypotheses or research issues." (Onwuegbuzie, 2016)

2.2 Historical Review

Most things have an historical precedent and historical literature reviews aim to analyse research throughout a set course of time. (Onwuegbuzie, 2016) Onwuegbuzie continues to explain that "the purpose is to place research in a historical context to show familiarity with state-of-the-art developments and to identify the likely directions for future research." (Onwuegbuzie, 2016)

Even if the body of scientific literature on the subject of Information Systems Security is limited and some of it is outdated, according to modern standards, relevant information can still be found through non-academic resources. The only downside to this approach is that the interested party must corroborate all information and decide which piece of data is more relevant to the task at hand, a daunting task considering the fact that not all information comes from a high value source.

Chapter 3: Literature Review

3.1 What is Information Systems Security

A simplified definition of the purpose of Information Systems Security is "keeping confidential information, confidential" (Auffret, 2014).

Auffret chose to use the definition provided by the dictionary of Military and Associated Terms of the US Department of Defense: "The protection of information and information systems against unaccredited access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security " (Auffret, 2014).

3.2 Who were the main employers of Information Systems

In the beginning there was one, the financial district which has always been at the forefront of technological innovation, always searching to optimise the way they do business (Atreyi Kankanhalli, 2003). Ever since the financial system came into existence, managers have been looking for systems to gain a competitive edge, constantly investing in new ways of collecting, transporting and using information, which in the current context has become data, but at the same time investing very little in the security of set systems (Atreyi Kankanhalli, 2003). The increased use of this virtual medium increased the number of attack surfaces accessible to malicious parties.

Currently Information Systems are employed in every business, financial or not, making it possible for multiple corporations to serve the same sector of population allowing each company to target a specific subsegment of that population concomitantly without interfering with each other.

3.3 Threats to Information Systems

Like any other system in the realm of cybernetics Information Systems are exposed to a plethora of threats like worms, viruses, trojans, ransomware, phishing, etc. from a variety of different sources such as criminal groups, hackers, corporate spies, hacktivists, malicious insiders but the most dangerous threat of them all is the non-compliance of employees with IS security policies due to lack awareness, interest, and investments in training towards diminishing set security risks (Willison, 2009).

Firstly, managers may make a deliberate decision to invest little in Information Systems Security because they think the risk of Information Systems Security abuses is low and because of the lack of tangible evidence to show an impact on the classical model of business (Willison, 2009). Secondly, managers may be skeptical about Information Systems Security effectiveness due to the difficulty in evaluating the benefits (Atreyi Kankanhalli, 2003).

3.4 Physical Deterrents put in place to combat breaches in Information Systems Security

Depending on the size of the business, managers might invest in Information System Security differently. Data suggests that this is wrong and no matter the size of the business, Cyber security should be a priority from the point of conception to point of launching of any business (Atreyi Kankanhalli, 2003).

Research shows that bigger organisations tend to invest more in physical security and preventive measures to effectively deny unauthorised access to facilities, equipment, and resources, while smaller companies tend to neglect Information Systems Security as being a non-priority especially in the infancy of their company (Willison, 2009). Some physical security measures include, but are not limited to, access control, CCTV, locks, RFID scanners and many more (Atreyi Kankanhalli, 2003). As these are the most

visible measures managers are not very keen on investing in software solutions to work in tandem with their physical security solutions.

3.5 Non-Physical measures taken to prevent future breaches

Even if managers are reluctant to investing in cyber security for their corporation, the inevitable is bound to happen with the increase in technological literacy (Atreyi Kankanhalli, 2003). Companies must not ignore the fact that the attack surfaces have also rampantly increased with the increase of numbers of users. Physical security remains a very important aspect of security and by no means should companies ignore it. However, with the constant development of Information Systems, the focus should be on developing more adequate software security solutions such as firewalls, risk specific software and policies put in place to educate managers and employees about the risks that lack of awareness present to the Information Systems that they employ (Willison, 2009).

3.6 The human in Information Systems Security

The insider threat has frequently been called the greatest menace to Information Systems Security, and yet this is generally overlooked in a rush to defend the physical space to the detriment of the digital space of the company with ever-increasingly complicated perimeter controls. Greater attention when hiring, educating and motivating employees to act securely will bring about a great payoff for the organizations that pursue this strategy (Atreyi Kankanhalli, 2003).

Diverse approaches and angles have been used to examine enterprise Information Systems Security management. The focus of this certain issue is on the individual computer user, the workgroup, and the organisation and its actions as they relate to the pursuit of Information Systems Security (Atreyi Kankanhalli, 2003). Companies commonly develop and carry out plans, policies, protocols, and procedures for establishing the security of information resources, along with user training curriculums and administration structures to advocate for compliance with security policies and measures (Willison, 2009).

Chapter 4: Discussion of Findings

4.1 What can be done to improve Information Systems Security

A number of actions can be taken to improve Information Systems Security some more important than others. From investing in research, exploring all aspects of Information Systems and their vulnerabilities, investing in software and firewalls to protect set Information Systems to the most important aspect of them all, investing in the increasing of awareness and education regarding the security of Information Systems (Atreyi Kankanhalli, 2003).

4.2 What can be improved in the future

Recommended consensus among organizational aspects, Information Systems Security methods, and Information Systems Security effectiveness must be evidence-based in practical data (Willison, 2009). By offering a theoretical basis for empirical results, the study on which the research is based, offers a theory on Information Systems Security efficacy that informs Information Systems managers about what kinds of Information Systems Security measures may be more efficient and what types of companies need to pay more attention on Information Systems Security (Willison, 2009).

Organisations with the necessary expertise can be set up to audit companies on the use of Information Systems assets, and support set companies with creating and implementing new policies related to

Information Systems Security and the severity of sanctions relating to the misuse of Information Systems assets can also be increased (Atreyi Kankanhalli, 2003).

The stringency of the security measure does not seem to affect Information Systems security overall. Applying more severe penalties for IS abusers, who are caught in the act, does not seem to discourage IS misuse (Willison, 2009). A logical reason may be due to the fact the maximum penalty for IS abuses tends to be less severe than those for the crimes concerning human casualties (Willison, 2009).
Greater deterrent efforts and greater preventive efforts have been effective in contributing to better IS security (Atreyi Kankanhalli, 2003).

4.3 Who needs to take charge in combating Information Systems Security breaches and attacks

Change needs to start from the top and efforts should be made for this change to trickle down in the mentality and overall approach of each and every employee in everything relating to the security of Information Systems and their use but not only relating to them (Atreyi Kankanhalli, 2003).

Lack of management awareness about the impact of deterrent and preventive efforts suggests that some form of management and user education may be necessary in the context of IS security. The constant infusion of funds into increasing set awareness is crucial for the improvement of the security of these Systems (Willison, 2009).

As for preventive solutions, management needs to be made aware about the value of deploying advanced security software to protect IS resources (Willison, 2009). Besides offering better access protection and intrusion detection through more sophisticated firewalls, advanced security software can detect unauthorized IS activities through surveillance mechanisms and automatically log all unauthorized activities and generate an exception report based on different scenarios (Willison, 2009).

Chapter 5: Conclusion

Now that organisations rely increasingly on IS for strategic advantages and operations planning, more research is needed in to IS security in order to develop a healthy and safe environment for companies to grow and prosper unhindered by the increase in cybercrime associated with the rise in computer literacy.

IS Security should be the area of research that companies should focus the most energy on, being that this aspect of IS is the most vulnerable due to lack of understanding on behalf of the managers but this can only be changed by improving the way companies educate their employees making them aware of all aspects of security and the role they, as individuals, play in the Security of the Information Systems of set company.

Chapter 6: Recommendations for Further Improvements

There are a lot of improvements that come with practice, and which are going to be implemented in future papers. I would like to improve on avoiding repetition through more in-depth research and dedicating

more time on researching the subject that I want to write about. I also identified the need to work on expanding my vocabulary in order to develop a more complex and varied sentence structure.

This can only be done by taking more time and scheduling my time in such a way that the research is thorough, and I have a good grasp on the concepts that the journal is presenting.

Chapter 7: Learning reflection for the year so far

Looking back to the start of this year I can only say that the experience has been an overall neutral one, starting with the organisation of the courses and the allocation of classrooms on campus. Even if I understand the fact that the change in lockdown policies and regulations can complicate things, I consider that the University should have enough resources to manage the situation in such a way so as not to confuse students or take from the energy that we should dedicate to absorbing the information presented to us, especially in the context of the first year. I would also like to address the dedication of some of the tutors in university as I do not consider that some of them have the drive to make students understand the information they present during lectures and simply want to get through the material and call it a day as comfortable as possible.

And the final matter I would like to address would be the focus on written coursework for a bachelor programme that should focus more on the technical aspect of learning, given the field it is meant to prepare us for, with the pretext that “You should learn how to write documentation for your future programming roles”. I do not consider this to be the most important aspect of this course and it takes time from actual practice of more technical aspects as it takes a lot of resources to write academically.

Thinking about the positive I do believe that the all the staff that I have come I contact with at the university have been most helpful and have done everything possible to navigate the lack of organisation to help in the best way that they could.

Although the online platform built by the university for students to use is not very user friendly and not really up to spec with the latest UI standards, I do find this platform to be very well structured and populated with useful information. It takes some time to get used to but taking in to account the complexity of the programming behind it is a very useful piece of software that makes students’ life easier.

References

Atreyi Kankanhalli*, H.-H.T.B.C.Y.T.K.-K.W. (2003) An integrative study of information systems security effectivness. *International Journal of Information Management*, 23(2), p.139–154.

Auffret, J.P. (2014) *business.gmu.edu* [Online]. Available from: https://business.gmu.edu/ [Accessed 17 October 2021].

Onwuegbuzie, A.J.a.R.F. (2016) *libguides.usc.edu* [Online]. Available from: https://libguides.usc.edu/writingguide/literaturereview [Accessed 11 October 2021].

Willison, M.W.a.R. (2009) Behavioral and policy issues in Information System Security: the insider threat. *European Journal of Information Systems*, 18(2), p.101–105.