Human Role in Cyber Security

Mushkan Adhikari

Marymount University

**Abstract**

Computer Security is becoming more and more important in present time because the world is highly interconnected with networks which are used to carrying out confidential transactions. Human relationships with technologies are rapidly growing and becoming complex day by day. One of the biggest threats in cybersecurity world is humans, to be specific employees in an organization. We can control the technical aspect no matter how complicated it might be and we have all the answers however, we cannot predict the human behavior towards technologies. This paper discusses how human trust towards technology can be misleading and how human behavior risk their lives with their careless decisions within the world of cyber security. The article is compiled based on the current research in cyber security and in reference to speech made by Racheal Botsman which talk about biggest issue in cyber security is human.

***Key words:*** Domain, Unconditionally, conceptualize, implement.

Contents

[Introduction 4](#_Toc63634218)

[Literature Review 4](#_Toc63634219)

[Reflection on the topic 5](#_Toc63634220)

[Conclusion 6](#_Toc63634221)

[Reference 7](#_Toc63634222)

Table of Figures

[Figure 1: Cyber Security 7](#_Toc63618820)

[Figure 2:Human role in Cyber Security 7](#_Toc63618821)

# Introduction

The increasing alliance of technology innovation from digital computing to smart phones is changing the nature of human technology relation in today’s world. As Racheal Botsman mentioned in her speech on “The Biggest Issue in Cyber Security is Humans, not machine” she states “our need for online trust has increased dramatically over the last 25 years”. In last few years, Information Security management has become common and regular within the public domain, many unconditionally trust in their computer security and make use of digital services sometimes without realizing the consequences that might follow. Although information systems research has shown to have largely positive impact on different contexts such as electronic markets, e-commerce, website design however, trust has also been conceptualized and resulted in negative consequences (Jason Bennet Thatcher, 2020). The problem here is not the computer systems or security, instead it is the human behavior on how much we put trust on our security system while neglecting its security procedures. As a result, having our information stolen.

# Literature Review

Cyber security plays a very important role in the field of information technology. Cyber security protects networks, devices, private information and programs from attacks, damage however, in present day protecting/securing the information has become a biggest challenge. It is very easy for us to be able to send messages, emails or even receive data with just click of a button, but how can we trust if our data is securely transmitted or not? Cyber security answers all those questions. In today’s world internet is the fastest growing infrastructure, however, due to such rapidly growing technologies we are unable to safeguard our private information in effective way and hence causing cybercrimes.

So, what can we trust, if not internet and how can we trust? Racheal Botsman states that trust starts from local- which is within a small community and villages where almost everyone know each other. Then, if we move to a big city or states we get institutional trust, for example: trusting the insurance companies and lastly distributional trust where trust flows through different networks, platforms and social medias such that good and bad cannot be differentiated (Botsman Video). These all ideas of trust are a part of human role or human behavior that affects our action against our life security, more importantly cyber security. Moreover, these problems occur mostly in organizations, human compliance in cyber security is a huge problem for organizations. Organizations develop complex cyber security systems that rely on technology and people. According to Kaspersky daily article, “the top three cyber security fears are all related to human factors and employee behavior” (Kapersky, 2021). Businesses are aware of how easy it is for employees/human error to impact their company’s security. The report by the Kaspersky daily article shows that 47% employees share inappropriate data via mobile, 46% of the physical loss of mobile devices exposing their company to risk and 44% use inappropriate IT resources (Kapersky, 2021).

Furthermore, Botsman stated “trust is the currency of interaction”, trust is human process. She further states trust has three levels, one, having trust in the idea, second, having a trust in platform and finally, trust in another individual. It is predicted that trusting in platforms can cause biggest risk issue in next five years. We tend to rely on internet and assume that confidential information and computing resources are protected and we fail to detect cyber-attacks. As a result, we face the consequences. Hence, cyber security has both bright and dark side, we just have to be aware of which side we are heading towards.

# Reflection on the topic

It is not simply enough to have Cyber Security in place to protect your business or to research information, instead it is our responsibility to follow such policies and reconfirm before agreeing to insert our private information online. Technology is fascinating and it has changed many of our lives countlessly, however technology also has a dark side to it. One of the relationships we have with technology is trust relationship. An inspiring quote by Racheal Botsman state that “trust have two enemies: one is bad character and the other is poor information (Botsman Video). we simply believe that the information we get in online is all true and can be trusted or even if we know the information is unsecure, we tend to ignore the policies and input our private information in digital services. For example, due to carelessness of an employee in a business or as Bostman mentioned in her speech about the criminal uber driver, we expose ourself so carelessly to others knowing that it might endanger us.

There isn’t a single person in the world that does not make mistakes and it is alright to make mistakes because it is a human experience and we learn from such mistake; however, in Cyber Security world such mistakes are a biggest risk for personal and public safety. Unfortunately, nowadays such actions are overlooked. We use digital world as efficiency and would not realize that this efficiency is the enemy of trust. Research found that human behavior is not consistent and can be influenced by relationships, there is also belief that bad things happen to other people; due to which many people willingly undertake the risk practices (Mark Evans, 2016).

Is that behavior of taking risk appropriate or significant? Do you think such behavior is safe for an individual or company? Human role plays significant part of digital world, it is our responsibility to be aware of the action we are taking. Whether it is hiring a nanny, researching on a particular company or inputting your information online, we must always follow procedure and policies on Cyber security. Moreover, companies can implement a training program for their staff to follow security follows. Actions such as using strong passwords, managing social medias settings, teaching children the basic knowing on internet and updating anti-virus software can help one enormously against cybercrime. Furthermore, as Racheal Botsman mentioned, platforms which are proactive, responsive and reactive can help ensure the safety in once privacy.

# Conclusion

Finally, this report describes that how a human trust can lead to harmful action towards an individual and society. As technology is expanding, many people use digital world as their safety net and convenience without realizing that cyber security also have a dark side to it.

As Racheal Botsman mentioned in her speech “we are outsourcing our capacity to trust an algorithm, and technology is changing the way we trust strangers”, we should wait for a moment and think carefully before we click the ‘Confirm’ button. The responsibility not only lies in the hand of an individual but also the companies. Companies have to build a trustworthy atmosphere which will affect their employees to behave carefully and thoughtfully in the platform.

Therefore, cyber security should and will continue to progress and develop in coming years but we should not forget that the risk associated within the systems and our role as a human in regards to trusting the digital world.

 

*Figure 1: Cyber Security Figure 2:Human role in Cyber Security*

# 

# Reference

Jason Bennet Thatcher, D. P. (2020). *Can trust be trusted in Cyber Security?* Retrieved from ScholarSpace: https://scholarspace.manoa.hawaii.edu/bitstream/10125/64264/0422.pdf

Kapersky. (2021). *The HUman Factor in IT security: How employees are making busniesses Vulnerbale from within*. Retrieved from Kapersky: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Mark Evans, L. A. (2016). *Human Behaviour as an aspect of Cyber Security Assurance*. Retrieved from arvix journal article .

*The Biggest Issue in Cybersecurity is Humans, Not Machines*. (2018, April 4). [Video file]. Retrieved from https://www.youtube.com/watch?v=15lS2SfW4pM