Reflection Paper on the Human Role in Cybersecurity

Thanh Xuan Nguyen

Marymount University

**Abstract**

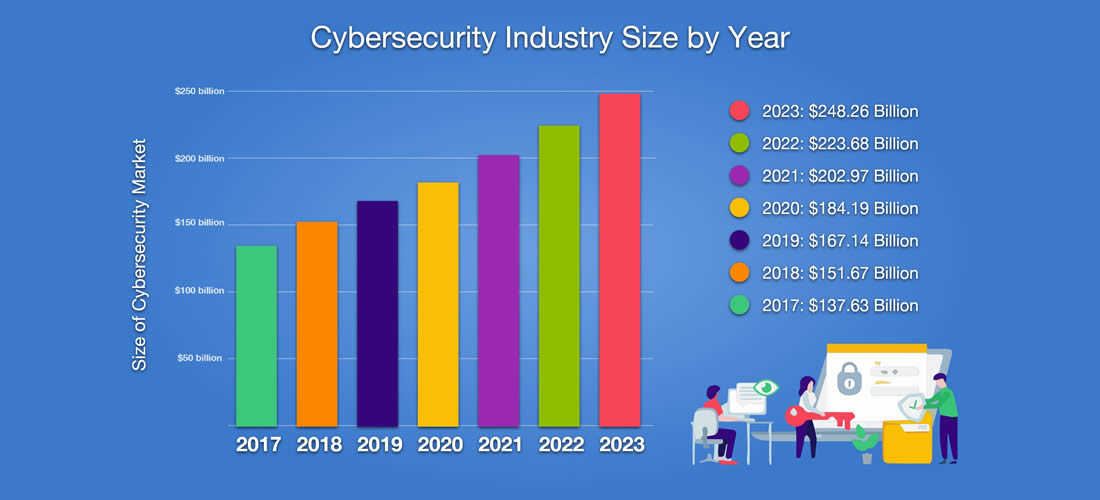


Figure 1 - Cybersecurity Industry Size by Year

The matters of cybersecurity never stop being a hot-button issue in the digital age. When online services gradually traditional ones, our daily life seems to become more and more convenient. However, it comes to IT workers with an enormous responsibility to protect users from virtually negative attacks such as malware, viruses, spams, and so on. Over the past five years, the size of the Cybersecurity Industry has kept increasing and reached up to $184.19 Billion in 2020. It indicates the importance of computer security to the development of the world. The literature review will give you the general approach to the human role in cybersecurity among other elements such as software or artificial intelligence. This reflection paper will demonstrate the perspective of Ms. Botsman in her speech about how to trust in online services is constructed. The speech “The Biggest Issue in Cybersecurity is Humans, not Machines” is performed on the stage of *Wired UK.* Ms. Botsman, which states that the factor which is responsible for the lack of Cybersecurity are not machines but humans. They are told to play a very important part of virtual security rather than AI or anything else.

*Keywords:* Cybersecurity, AI, irresponsible and unprofessional management, sensible methods, secure administration, proactive, reactive.

Reflection Paper on the Human Role in Cybersecurity

**Introduction**

This paper is about the role of human in the field of computer security. The literature review brings about the importance of human responsibility in the field of cybersecurity. There is a discussion about the damage of businesses caused by irresponsible and unprofessional management, the efficiency of high-quality security and improving methods. The reflection paper demonstrates the perspective of Ms. Botsman towards the trust's establishment in the digital age. As she mentioned in her speech, the trust in the digital age is formed in the largest area in which it is not under the control of any referees, regulators or authorities. That type of trust is virtually built through activities on online market stores, platforms and so on. As a result, it is challenging for people to distinguish which organization or who they have found on the Internet is trustworthy.

**Literature Review**

Nowadays, our life becomes more and more convenient with modern technology. However, it leaves software developers, website administrators and especially, cybersecurity analysts more and more challenging problems towards the issue of computer security. Among many factors which effects the developing process of cybersecurity, the role of human is considered the most important element. The goal of this literature review is to indicate the importance of human's responsibility for cybersecurity. Firstly, we will investigate the damage for businesses caused by irresponsible and unprofessional management. Then, sensible methods are considered for better improvement. Finally, we will know how effective secure administration is after the methods are applied.

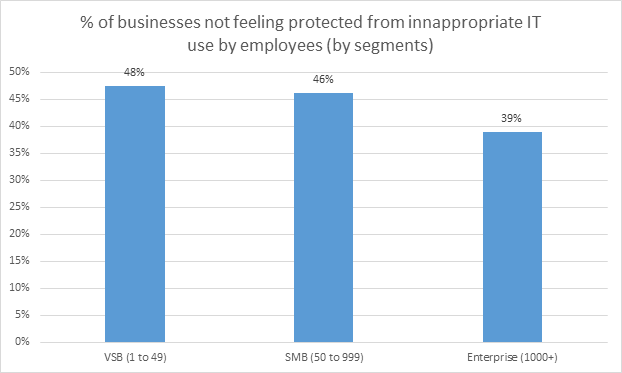


Figure 2 - Trust's Businesses towards the work of IT employees  
Source: IT Security Risks Survey 2017, global data

First of all, the damage of irresponsible and unprofessional management indicates that the majority of damages for cybersecurity incidents are caused by employees who are in charge of their role in computer security. *Kaspersky Lab*, a multinational cybersecurity and anti-virus provider, states, “in 46% of cybersecurity incidents in the last year, careless/ uninformed staff have contributed to the attack.” (Kaspersky, 2018) It comes to the fault of IT employees for several reasons. One of them is that they usually underestimate the danger of online viruses, malware and phishing attack. Besides, they lack the required pieces of training about security skills and professional methods against unexpected incidents. It is the problem many businesses are concerned with. As in many interviews, more than 50 percent of businesses claim that they are not confident in the security of their IT employees. Even they do not know how to guide their employees to react to cybersecurity incidents properly when they happen. Therefore, it is easy to know that IT staff may make mistakes that can put the computer's database and information of the businesses at risk.

To solve the problem of human role in cybersecurity, there are nothing better sensible methods for improvements. Since it is the responsibility of humans in protecting computer security, the best method is always improving the performance of IT employees. It is necessary to open more pieces of training to help them gain more experience. Also, suggest them to apply various methods so that the layers of protection turn more solid and secure. *Nibusinessinfo* wrote, "Business should use different cybersecurity measures to keep their business data, their cashflow and their customer safe online. These measures should aim to prevent risks from various sources." (Nibusinessinfo, n.d.) There is a variety of measures toward the purpose of protecting their company’s data better and better. First, it is ideal for the company to come up with a password policy so that the employees could practice. The policy should include a password reset routine and the guide of creating a strong password. Second, the firewall should be put up regularly. Also, IT employees should check its update to ensure it is fully effective. Third, it is the application of security software. Every company should own a premium edition of anti-virus and anti-malware programs. It will notice if something strange slips into their network and eliminate it before the bad things happen. And, there are many more methods to assure better protection for network security.   
 When cybersecurity is perfectly protected, it will bring about the effectiveness of security administration. About the benefit of well-performed network security from IT employees, Auvik, a famous software company, states, "Your company may have the best security software and most comprehensive office policies, but your actions play a big part in helping to keep data safe." (Norton, 2020) A secure network administration brings businesses and IT employees a lot of advantages. It is protecting data. Important data and information about the company are prevented from leaking to other companies. Also, a business's network could avoid online attacks such as unknown mails, links and other negative attacks.   
 In conclusion, the role of human is very important in cybersecurity. When IT employees lack responsible and professional skills in management, it causes tremendous damages to the businesses. On the other hand, it brings them a lot of advantages when network security is full protected with many effective methods.

**Reflection Paper**

Earlier in the timeline, Ms. Botsman and her family encountered a terrible experience. They have lived with a nanny who, later, is told to be an armed bank robber, for ten months without realization. It happens because of a lack of verified information. Therefore, Ms. Botsman stresses the importance and convenience of the Internet for our safety through her speech. Two main ideas are coming from the speech of Ms. Botsman which are the role of human in managing cybersecurity and how they do to improve it.   
 First, it is about the role of human in managing cybersecurity. Ms. Botsman told her audience about the event of an Uber driver who gets 4.7 out of 5 star-rating in Uber driver's review. No one could realize that he is under a psychotic condition. It led to the tragedy that he killed 6 passengers during his shifts. But the worst thing about this story is that, after he had strange behaviors with a few customers, and some of them posted this matter on social media and even phoned the police, his information was still on the Uber website. Every day, Uber’s customers in Kalamazoo has an opportunity to be a passenger of the serial killer. About this incident, Ms. Botsman stresses that it is the mistake of Uber's IT employees who are in charge of late updating information. It not only lowers their credibility but also endangers the safety of their customers. In the tragedy above, a lack of responsibility from the IT employees could cause the death of several customers. Therefore, the role of human in cybersecurity cannot be underestimated.   
 Second, Ms. Botsman brings how to build trust in the digital age. Rather than other trusts mentioned in the speech, trust is built in the digital age is distributed trust. It is a type of trust formed in a large area such as network, system and online market stores. This type of trust is not under any authority or regulators. In the angle of Ms. Botsman, distributed trust is constructed within three main levels. The First is trusting the idea. The idea is something not perfectly secure. However, it should be given a try even though the outcome might be good or bad. The Second is trusting the platform. It is the confidence of users when using it as well as the credibility of the developer team which releases it. The Third is individual. The term "individual" could be a human being or artificial intelligence (AI).   
 Among the three layers, the layer of the platform is considered the most important in the field of cybersecurity. According to Ms. Botsman, distributed trust is built through two factors. The first factor is “proactive”. If a platform carries a proactive characteristic, the risk of cybersecurity incidents could be reduced to a minimum. It is the preparation for any online attacks. The state of being proactive demonstrates the responsibility and capability of IT employees who are in charge of their platform's security to prepare appropriate methods for any upcoming incidents. The second factor is “reactive”. The state of being reactive is calculated based on how effective and quick are the response to the issue. For example, in the story of the psychotic Uber driver above, if they are aware of customers’ feedback as well as manage their driver’s information better, the death of 6 Uber customers may not happen. Also, businesses must improve the experience of their customers. For example, you buy an item on shopping online, but later, you realize you pick the wrong one and should return it. You can perform it instantly through customer service. It is very convenient for customers.   
 In conclusion, Ms. Botsman states that the success of cybersecurity relies on the responsibility of IT employees who work in the field of security. In the age of digital technology, the trust in the platform is considered the most important. To achieve perfect trust in the platform, the developers must assure the state of being proactive and reactive in their platform. Ms. Botsman believes that, with a proactive and reactive platform, her family will not accidentally hire a bank robber to be their nanny anymore.

**Conclusion**

The importance of the human role in cybersecurity is tremendous. Even though the company is equipped with up-to-date protecting software, or the platform is protected by a high-level system, the task of the administrators is always essential. It is compulsory for IT employees to stay alerts of online negative attacks and apply a variety of methods for better protection. It not only decides the development and success of businesses but also protects clients and customers from online risks. Ms. Botsman believes that if the responsibility of human in cybersecurity is fulfilled, the benefit for the businesses and clients is significant.

**Table of Figures & Tables**

[Figure 1 - Cybersecurity Industry Size by Year 2](#_Toc50735051)

[Figure 2 - Trust's Businesses towards the work of IT employees 4](#_Toc50735052)

References

Kaspersky. (2018). *The Human Factor*. Retrieved from http://www.kaspersky.com/: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Nibusinessinfo. (n.d.). *Protect your business online*. Retrieved from https://www.nibusinessinfo.co.uk/: https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures

Norton. (2020). *10 cybersecurity best practices that every employee should know*. Retrieved from https://us.norton.com/: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html