EasyChair Preprint

№ 5882

The Influence of Cybersecurity on Modern Society

Mitchell Hancock

June 23, 2021

The Influence of Cybersecurity on Modern Society

The history, development and importance of cybersecurity in a modern world

Mitchell Hancock
Fundamentals of Computational Intelligence
Flinders University

hanc0169@flinders.edu.au

Abstract

Cybersecurity is an important aspect of the modern world. As more devices are invented and connected to the internet or utilize web-based services, cybersecurity must evolve in order to keep these devices safe from cyber threats. This paper will investigate a brief history and development of cybersecurity and cyber threats followed by the influence, importance and current challenges of cybersecurity. This in turn will inform what cybersecurity may look like in the future.

1 Introduction

In the modern world, people can send information in the blink of an eye whether it be an email, an instant message or video. Working in the background of all operating systems, devices, software applications and networks is cybersecurity. Cybersecurity has many varying definitions however "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (ITU, 2009). Cybersecurity has become a focus of government and business organisations in the past few decades as emerging technology has changed the requirements of cybersecurity due to the ever-changing methods of cyber threats.

2 History and Development

Cybersecurity was not developed when the first digital computer was made in 1943. The theory of cybersecurity was put forward in the 1940s, but it was not until 1967 that the first defensive measures were created when a company invited students to try out their new system. The students managed to learn the systems language and gain access to other parts of the system (Chadd, 2020).

It was not until the 1970s that cybersecurity started gaining traction as an important aspect of computing. The 1970s saw the development of several common cybersecurity methods such as "administrator privileges, file systems permission and hashed passwords" (Warner, 2012). Data encryption was also invented in the 1970s. These methods were created as a result of the computer program called CREEPER, invented by researcher Bob Thomas. CREEPER travelled across the ARPANET (The Advanced Research Projects Agency Network) and a program was designed by Ray Thomilson which deleted CREEPER bringing about the first instance of antivirus software (Murphey, 2019).

3 Evolution of Cyber Threats

CREEPER was the first known computer worm. After the creation of the internet in 1983 and subsequently the creation of email, cyber threats began to evolve. In 1988, Robert Morris designed a worm to propagate across networks but due to a programming error, it resulted in clogged networks and slow internet causing all connected systems to crash (SentinelOne, 2019). This was the first computer related virus that got global coverage. The Morris Worm resulted in the rise of the antivirus industry and this in turn caused cyber threats to evolve.

1999 saw the introduction of the Melissa virus which caused millions of dollars' worth of damage (Chadd, 2020). As cyber threats have evolved terms such as malware, viruses, worms, phishing, ransomware Trojan and root kits are now familiar. The creation and evolution of these threats has made governments, organisations and businesses place an emphasis on the importance of

cybersecurity and now cybercity influences the day to day lives of many people.

4 Influence of Cybersecurity

The Computer Misuse Act was enacted in 1990 in the United Kingdom which marked it as one of the first legislations that dealt with cybersecurity in the world (Fafinski, 2019). Other countries soon followed suit placing more importance on how to be cyber secure.

Cybersecurity is everywhere even if it is not consciously thought of. The internet handles online transactions, emails, compiling information, clouds, social media etc. (singer and Friedman, 2014). Sensitive information is now stored online with no physical copies as backups. The operating systems of all devices connected to the internet have inbuilt protections in their programming to prevent them being vulnerable to cyber-attacks. Anti-virus software is encouraged to be installed in all devices. Security protocols and encryption are used on the internet, online data and multi-factor authentication is used extensively. These initiatives are just some examples of how cybersecurity is in our everyday lives, however cybersecurity still faces many challenges today.

5 Current Challenges of Cybersecurity

As a whole, cybersecurity faces many challenges in the modern world. Some challenges have been mentioned such as the list of cyber threats in Section 3. Another challenge is the existence of flaws and vulnerabilities in major software (Schmidt and White, 2017). These vulnerabilities will be exploited. An example of this was the Equifax hack in 2017 in which 143 million were affected when their personal data was exposed. The company was later found to be using out-of-date software with known vulnerabilities (Schmidt and White, 2017). In addition to out-of-date software, the biggest challenge to cybersecurity is the knowledge of all individual users of computer systems.

An employee that does not have a basic understanding of cybersecurity can introduce flaws or viruses into the system. Examples of this may include phishing emails and introducing infected media, such as USBs, into the system. Such incidents have made many governments, organisations and businesses focus on teaching employees about proper cybersecurity methods. Cybersecurity education will no doubt continues as the world of technology evolves.

6 Future of Cybersecurity

Technology continues to evolve and cybersecurity will continue to evolve with it. One cybersecurity practice gaining traction is the development, security and operations method or DevSecOps. DevSecOps “is about introducing security earlier in the life cycle of application development thus minimising vulnerabilities” (Constantin, 2020). This ensures that security patches and updates are pushed out more frequently and as soon as vulnerabilities are known. Artificial intelligence and machine learning will be incorporated more into cybersecurity, but these methods will also help cyber threats to attack systems with more ease.

Another factor to consider is the human factor. As mentioned previously, users who are not cybersmart are ore likely too cause security incidents. As a results, cybersecurity education will continue to be an important aspect of the many governments, organisations and businesses in the world. Additionally, how people interact with devices and how they are influenced by them is an important aspect of cybersecurity now and in the future (Dawson and Thomson, 2018). How people interact with each other online is unique as people create their own personas that do not reflect their real-world interactions (Castronova, 2008). The human factor as well as the evolving technology factor will make it challenging in the future for cybersecurity to handle all threats.

7 Conclusion

As mentioned in the history of cybersecurity, it was not until the 1960s that the first defensive measures were created. From that time technology has come forward in leaps and bounds incorporating both advanced cybersecurity methods and the advancement of cyber threats. Major legislation has influenced several organisations and businesses to enact cyber policies and educate personnel on the importance of being cyber smart. Finally, cybersecurity faces many challenges in current times which no doubt will increase in the future. However, with methods such as DevSecOps, cyber education, artificial intelligence and machine learning, cybersecurity will still influence society in the future as being cyber secure is more important than ever.

References

Castronova E. (2008) *Synthetic Worlds: the Business and Culture of Online Games*, [eBook] Chicago: The University of Chicago Press, p 107. Available at:. https://books.google.com.au/books?hl=en&lr=&id=0OHVdwE5Kb0C&oi=fnd&pg=PR7&ots=i1n_vmoXZ0&sig=cWhxJfLr9ww-iAbY1IRn0zY_v9s&redir_esc=y#v=onepage&q=persona&f=false (Accessed: 19 Mar 2021)

Chadd, K. (2020). 'The History of Cybersecurity', Avast Blog, 24 November 2020. Available at: https://blog.avast.com/history-of-cybersecurity-avast (Accessed: 17 Mar 2021)

Constantin L. (2020) 'What is DevSecOps Why it's hard to do well', CSO, 23 July 2020. Available at: https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html (Accessed: 09 Apr 21)

Dawson J. and Thomson R. (2018). 'The Future of Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance', Frontiers in Psychology, Available at https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full (Accessed: 19 Mar 2021)

Fafinski, S. (2014) *Computer Misuse: Response, Regulation and the Law*, [eBook] New York: Routledge, p 13. Available at https://books.google.com.au/books?hl=en&lr=&id=MTF05ayt7OkC&oi=fnd&pg=PR1&dq=computer+misuse+act&ots=bdLLraHuv4&sig=CJKgiL55pSyIGy3yC6T-xv--yfc#v=onepage&q=computer%20misuse%20act&f=false (Accessed: 18 Mar 2021)

ITU. (2009). *Overview of Cybersecurity. Recommendation ITU-T X.1205*. Geneva: International Telecommunication Union (ITU). Available at: http://www.itu.int/rec/T-REC-X.1205-200804-I/en (Accessed: 17 Mar 2021)

Murphey, D. (2019) 'A history of Information Security', IFSEC GLOBAL Blog, 27 June 2019. Available at https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/ (Accessed: 17 Mar 2021)

Schmidt, D. C. and White, J. (2017). 'Why don't big companies keep their computer systems up-to-date?', THE CONVERSATION, 27 September 2017. Available at https://theconversation.com/why-dont-big-companies-keep-their-computer-systems-up-to-date-84250 (Accessed: 08 Apr 2021)

SentinelOne.com (2019). 'The History of Cyber Security – Everything You Ever Wanted to Know', SentinelOne Blog, 10 February 2019. Available at https://www.sentinelone.com/blog/history-of-cyber-security/ (Accessed: 17 Mar 2021)

Singer, P. and Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know.* [eBook] New York: Oxford University Press, p 2. Available at https://books.google.com.au/books?hl=en&lr=&id=f_lyDwAAQBAJ&oi=fnd&pg=PP1&dq=Cybersecurity&ots=Dnl1QOvGlk&sig=twhZ-3UkSQ1qzbIJVog8PERhdFc#v=onepage&q=Cybersecurity&f=false (Accessed: 17 Mar 2021)

Warner, M. (2012). 'Cybersecurity: A Pre-history' *Intelligence and National Security,* [online] Volume 27 (5), p 781-799. Available at https://www.tandfonline.com/doi/full/10.1080/02684527.2012.708530?scroll=top&needAccess=true (Accessed: 17 Mar 2021)