Cybersecurity

Report by Nicholas Young (S3793515) – Group 14

In the modern age, society has built up an incredible reliance on technology. People use it to work, shop and communicate with others while Businesses rely on it to operate effectively. Business or otherwise, almost all of our most important and sensitive information is now stored somewhere online. Bank details, addresses, emails – all of it is stored somewhere on the internet, managed by companies that we trust to protect it from people with malicious intentions. This is where cyber security comes into play. Just as locks, vaults, alarms and armed guards protect the physical premises of a building – cyber security has become a crucial aspect of the effective operation and safety of all businesses and organisations with a network or online presence.

## What Does It Do?

Cyber security refers to the practice of defending the systems, networks and programs that hold that sensitive information from people looking to gain access to it for nefarious purposes. These offenders who perform attacks on systems are generally out to achieve such goals such as gaining access to information, extortion, identity theft or general disruptive behaviour to whatever degree. There are various means for these offenders to gain access to systems or to extract information out of these systems or even people.

Ransomware and malware for example are types of malicious software also known as a “virus” which allows an attacker access to your computer, though in this case for different means. Ransomware is designed to extract money from victims by preventing user access to certain files or their entire computer until the ransom is paid. Malware is software designed to gain access to your computer in order to carry out malicious actions. While possibly the most commonly known, malicious software downloaded to your computer is not the only type of threat users can experience. Offenders can employ a practice known as social engineering – which through deception and trickery, allows them to gain money or access to sensitive information from unsuspecting victims. Similarly, a tactic called “phishing” – the act of sending false emails disguised as emails sent from sources the recipient would generally trust – can be used to gain sensitive information such as bank details or user passwords, generally for the services the phishing email is attempting to emulate.

While practices such as using anti-virus software is effective for the common user, it is not an adequate security measure for businesses and organisations. These entities constantly face much larger and more direct threats from individuals looking to attack their networks for malicious purposes. They must be prepared to detect and prevent threats looking for access to their networks in order to perform actions that could be anywhere from damaging to catastrophic. Currently, there are multiple types of cyber security measures which can be employed by businesses and organisations to mitigate threats and keep their networks secure. These measures include but are not limited to:

* Network Security – Controls incoming and outcoming connections to protect network traffic, preventing threats from entering the network or spreading throughout the network.
* Data Loss Prevention – Classifies and protects important information in order to prevent the accidental or purposeful sharing of said information.
* Cloud Security – A set of security measures that work together to protect cloud-based information and systems.
* Intrusion Detection Systems / Intrusion Prevention Systems – Identifies activities that could be classified as malicious. There are two types of Intrusion Detection Systems, one host based, and one network based. Host based Intrusion Detection Systems are installed on every computer in order to monitor traffic that travels between nodes in a network – such as file access, use and transferral. Network Intrusion Detection Systems are capable of monitoring networks on a larger scale with the purpose of detecting suspicious behaviours and stopping them before any damage can occur.
* Identity and Access Management use – Limits and tracks user activity and access through authentication services in order to protect important systems from malicious activity.

Another security measure which is extremely popular with businesses and organisations in the modern age are Security Information and Event Management systems (SIEM). SIEM systems are important to network and system security as most cyber-attacks are not obvious and are more effectively detected via the log files gathered by the SIEM systems. SIEM could be considered more effective than other types of cyber security such as Intrusion Detection Systems, as while Intrusion Detection Systems are effective at monitoring packets an IP addresses and creating service logs based off of user activity, SIEM combines multiple systems for a broader and more complete overview of cyber security via real time log analysis. Information collected by an SIEM is processed and transferred to management consoles where data can be analysed, and the overall process improved based off of feedback by data analysts.

Artificial Intelligence and Machine Learning also have huge potential for cyber security. Automation will help address the general shortage of cyber security professionals, as they can effectively managed the data gathered by security tools in use by professionals. As for the cloud, businesses who host their services on the cloud can expect the effectiveness of certain types of Distributed Denial of Service (DDoS) attacks to be lessened due to the availability of a Cloud Service Provider’s bandwidth and processing capabilities.

The future of SIEM systems may also be on the cloud. The backend of Security Information and Event Management systems could shift to the public cloud infrastructure from on-premises servers. This could be done to account for the massive growth in various types of security data that businesses collect and analyse. This growth in the amount of security data collected means more infrastructure, personnel and operational tasks will be required. Currently, on site Security Information and Event Management system software is priced around the amount of data managed. With the growing amount of data being collected this has caused the price of SIEM software to raise significantly costing businesses more – and not just in money. Not paying for a sufficient capacity can cause valuable security data such as the logs gathered by the SIEM systems to be lost or purged in order to keep the SIEM within capacity.

## What is the likely impact?

The future of cyber security is linked tightly with cloud-based technology and artificial intelligence/machine learning. The shift of SIEM systems from being on-site software to cloud based software could mean that it would cost less for businesses and organisations to utilise this technology as it would allow them to effortlessly scale up as required without a need for more on-site infrastructure and personnel. The potential for higher capacity SIEM systems would mean no logs gathered by the SIEM systems would need to be purged – meaning better security for the client. Cloud service providers are also investing heavily in artificial intelligence and machine learning. These developments will naturally be of great use to cyber security practices such as analytics relating to logs gathered by security systems and software.

The impact of these developments is essentially overall improved cyber security for businesses and organisations. More affordable security capabilities for businesses through a cloud based SIEM system combined with artificial intelligence and machine learning analysing data collected by these systems as well as actively tracking and preventing threats on networks should lead to a more secure future. The downside of this development is some in the already barren field of cyber security may find it harder to gain employment – as businesses and organisations will require less personnel to oversee and maintain their security measures.

Other security measures will also evolve to combat those with malicious intentions – though it is important to remember that those who are behind these threats will also evolve to combat security measures as they grow. Businesses should regularly employ penetration testers – ethical hackers who are hired to find weaknesses in security that could be exploited by genuine attackers.

## How will this affect you?

Developments and progress in the field of cyber security can only serve to put the mind of the average person to ease. The security of the sensitive information that we provide to various businesses online should be something that people are seriously concerned about, especially considering fairly recent data breaches such as that of Yahoo in 2013, where the personal information contained in 3 billion Yahoo accounts was exposed. Or more recently in 2018, where the personal information of 500 million guests was accessed and copied by a hacker.

Cyber security is an important practice which everyone should pay attention to and participate in, even if only rudimentarily. The average computer user can make themselves safe by using anti-virus software, designed to detect and contain risks to alleviate the threats of malicious software and activity on their computer. Education in cyber safety goes a long way, knowledge on what to do and what not to do online can help prevent users from downloading potentially malicious content from unreputable sources or falling into common traps such as phishing schemes.

## Conclusion

Cyber security is now a crucial part of how society in the modern age operates. The vast majority of sensitive information belonging to people, businesses and other entities is now located online in various networks throughout the world. Maintaining data privacy, confidentiality and network security is of the utmost importance and a high standard for cyber security should be upheld by all who have the responsibility of protecting their network – potentially their entire business, as well as their client’s data. Current, state of the art and developing technologies should be utilised to ensure that this data remains secure and a watchful eye should be kept on those with malicious intentions to ensure that their security always remains one step ahead.

# References

1. Cisco. (n.d.). What Is Cybersecurity? Retrieved March 26, 2019, from <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>, No Author or Publish date mentioned.
2. Forcepoint. (n.d.). What is Cybersecurity? Cybersecurity Defined, Explained, and Explored. Retrieved March 26, 2019, from <https://www.forcepoint.com/cyber-edu/cybersecurity>, No Author or Publish Date listed.
3. Mello, J. P., Jr. (2019, February 28). RSAC 2019: Tracking the state of cybersecurity. Retrieved March 26, 2019, from <https://techbeacon.com/security/rsa-2019-tracking-state-cybersecurity>
4. Sinclair-Jones, J. (2018, November 15). Cybersecurity Trends and Threats to Watch Out for in 2019. Retrieved March 26, 2019, from <https://www.themartec.com/insidelook/cybersecurity-trends-and-threats>
5. Keary, T. (2019, February 27). 8 Best SIEM Tools: A Guide to Security Information and Event Management. Retrieved March 26, 2019, from <https://www.comparitech.com/net-admin/siem-tools/>
6. Oltsik, J. (2019, January 4). 2019 will be the year of cloud-based cybersecurity analytics/operations. Retrieved March 26, 2019, from <https://www.csoonline.com/article/3331280/2019-will-be-the-year-of-cloud-based-cybersecurity-analyticsoperations.html>
7. How to become a Penetration Tester. (n.d.). Retrieved March 26, 2019, from <https://www.cybersecurityeducation.org/careers/penetration-tester/>, No Author or Publish Date listed.
8. Yun, S. (2018, December 1). Marriott's data breach is large, but it's not the largest: These are the 5 worst corporate hacks. Retrieved March 26, 2019, from <https://abcnews.go.com/Technology/marriotts-data-breach-large-largest-worst-corporate-hacks/story?id=59520391>