

**CC0002: Navigating The Digital World**

***Reasons Behind Rise of Cyber Attacks and Measures to Mitigate Them***

**Tutorial Group: T025**

**Tutor: Prof Vijay Sethi**

**Group Number: 5**

**Group Members:**

|  |  |  |
| --- | --- | --- |
| **Name** | **Matriculation Number** | **Email** |
| Teng Song Heng | U2122030K | TE0016NG@.e.ntu.edu.sg |
| Lim Dong Wan | U2122455D | LIMD0030@e.ntu.edu.sg |
| Seah Yee Hao | U2121483B | SEAH0216@e.ntu.edu.sg |
| Kavita Sriram | U2120934G | KAVI0008@e.ntu.edu.sg |

|  |
| --- |
| **DECLARATION OF WORK**  “By submitting this work, we are declaring that we are the originators of this work and that all other original sources used in this work have been appropriately acknowledged. We understand that plagiarism is the act of taking and using the whole or any part of another person’s work and presenting it as our own without proper acknowledgement. We also understand that plagiarism is an academic offence and that disciplinary action will be taken for plagiarism.” |

**Contents page**

Contents

[Executive Summary 4](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881356)

[Background Information 4](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881357)

1)[**Cyber Attacks in 21st Century** 4](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881358)

2)[**Effects of Cyber Attacks** 5](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881359)

[Rise of Cyber Attacks (Body 1) 7](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881360)

1)[**Low Barriers of Entry** 7](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881361)

2)[**Emergence of Opportunities for Cyber-Attackers** 8](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881362)

3)[**Evolution of Methods - Punycode Phishing** 9](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881363)

[Human Error and Possible Mitigation (Body 2) 11](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881364)

1)[**The Effect of an Individual and ‘Human Error’** 11](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881365)

2)[**Examples of Human Errors** 11](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881366)

3)[**Cyber Attacks due to Human Error** 12](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881367)

4)[**Cybersecurity Mitigation Practices** 13](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881368)

[Conclusion 15](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881369)

[References 16](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881370)

[Appendix 20](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881371)

1)[**Elements of Cybersecurity** 20](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881372)

2)[**Types of Cyber Attacks** 22](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881379)

3)[**Cybersecurity Mitigation Practices** 24](file:///F:\NTU\School%20matters\Year%201%20school%20work\Sem%202\CC0002%20Navigating%20the%20Digital%20World\Enrichment\CC0002%20Group%20Assignment.docx#_Toc100881390)

**Executive Summary**

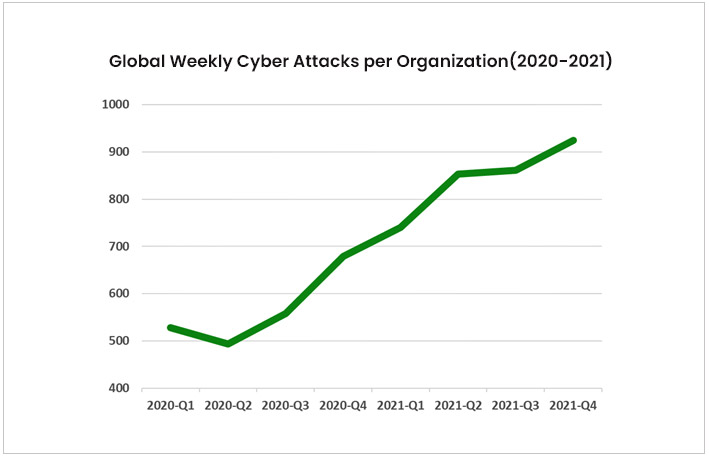
In today’s globalized world, cybersecurity has been a “household topic”. The ongoing COVID-19 pandemic has catalyzed digitalization and cybersecurity has taken centre stage (Pure Cloud Solutions, 2020). Hence, this paper aims to highlight the significance of cybersecurity in today’s circumstances and the impact of cyber attacks on people, shed light on how the attackers are able to achieve their agenda using different methods, and provide a deeper understanding of how to prepare for the age of cyber and deter cyber attacks, especially at the individual level.

**Background Information**

Cybersecurity is the practice of protecting critical systems and network infrastructure from digital attacks (IBM, n.d.; Cisco, 2021), also commonly known as cyber attacks. This has become a hot topic of discussion in recent years, given the technological advancements that have drastically improved our quality of life in many facets. From having groceries sent to our home by ordering through our phones to finding the best route to a particular destination, technology has indeed transformed our lives for the better. All these events are happening through the vast cyberspace that transcends beyond geographical boundaries - the Internet.

**Cyber Attacks in 21st Century**

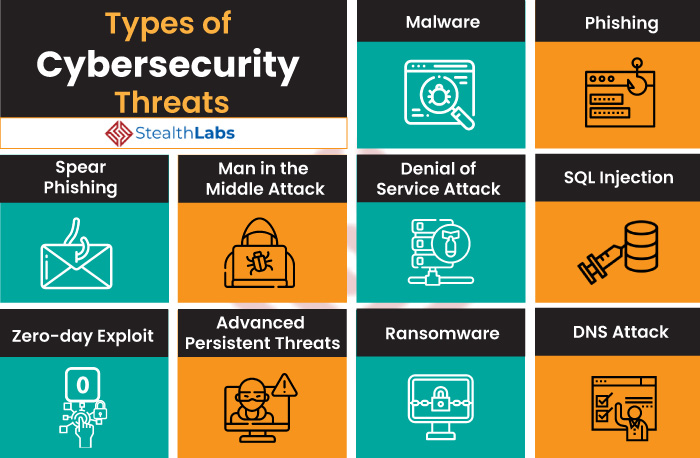
When discussing cybersecurity, a relevant threat that accompanies it would be cyber attacks, which are malicious, intentional attempts, by an individual or organization, to “steal, expose, alter, disable or destroy information” through unauthorized access to a computer system of another individual or organization (IBM, n.d.; Cisco, 2022). In today’s digitalised world, the prevalence of technological advancements has benefited humans tremendously. However, this also inevitably poses the unwanted risk of cyber attacks. In fact, the number of cyber attacks in organizations has been on the rise worldwide, more so during the COVID-19 pandemic (Figure 1), due to increased adoption of technological tools as a result of the worldwide social restrictions since 2020.



*Figure 1: Trend in global weekly cyber attacks per organization (2020 - 2021)*

**Effects of Cyber Attacks**

A plethora of categories of cyber attacks exist (Figure 2, Appendix).



*Figure 2: Common types of cybersecurity threats*

There have been a few world renowned cases of cyber attacks in the past decade, such as the 2017 WannaCry ransomware attack (Figure 3) that affected around more than 230,000 computers in more than 150 countries (Cooper, 2018), and the external intrusion attack on Sony’s Playstation network (Figure 4) that claimed the personal information of 77 million users in 2011 (Will, 2014). In Singapore, the Ministry of Defence (MINDEF) became the target of cyber-attackers in 2018. Personal details of 850 National Servicemen and staff working under MINDEF were stolen by the attackers (Tham, 2017) in what was touted as a “targeted and carefully planned” attack. If anything, this tells us that nobody is truly safe from cyber attacks, even a small country like Singapore.



*Figure 3: Wana Decrypt0r 2.0 browser in the ransomware attack*



*Figure 4: Network outage on Sony’s PlayStation*

**Rise of Cyber Attacks**

**Low Barriers of Entry**

The pervasiveness of cyber attacks worldwide is indeed worrying, but there is also a multitude of readily accessible information and resources on the Internet, covering numerous topics that serve to raise people’s awareness about cybersecurity. These include penetration testing - a form of ethical hacking that involves intentionally conducting simulated attacks to find exploitable vulnerabilities in computer systems, networks, websites or applications - and malware analysis, which identifies and analyzes malware behavior and characteristics.

However, this knowledge and tools can be used by the masses for malicious purposes as well. Such tools encompass offensive Operating Systems (OS) like Kali Linux and Parrot that contain many penetration testing tools, and cybersecurity training sites like Hack The Box (Figure 5) or TryHackMe (Figure 6) that allow one to hone hacking skills. This results in the existence of a group of hackers organizations normally refer to as “script kiddies[[1]](#footnote-1)”, who might give any company a run for their money. This is seen from a data breach in 2015, where 2 teens were arrested for having breached 156,959 accounts on the TalkTalk website costing **£**77 million.



*Figure 5: Hack The Box home page*



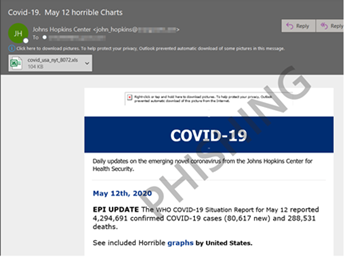
*Figure 6: TryHackMe home page*

Nevertheless, even with the low barriers of entry for script kiddies, what organizations or governments should truly look out for are hacktivists [[2]](#footnote-2)or state-sponsored attackers[[3]](#footnote-3), who usually have specially crafted payloads and tools or have them specially made from the dark web. These tools are often hard to be traced or detected by Anti-Viruses (AVs) or network intrusion detection systems. Furthermore, these state-sponsored hackers or hacktivists have goals in mind, such as data mining, website defacement or even military intelligence collection. They are empowered enough to bring down even a country, as seen in the 2007 cyberattack on Estonia where the whole country plunged into chaos, with multiple essential services taken down, from email to banking services, all through the cyber realm.

**Emergence of Opportunities for Cyber-Attackers**

Fast forward to today, there is a drastic increase in people using the Internet in light of the pandemic. Be it for entertainment purposes, work, news or online shopping, technology is dominating our lives at an alarming rate. This is exacerbated by the push for contactless activities in an effort to curb COVID-19 transmission, thereby resulting in “accelerated digitalisation” with the pandemic acting as the catalyst (CSA, p.4, 2021). For instance, many activities have been shifted online where possible, such as school lessons, industrial and office work, and even medical consultations. Many of these activities involve users inputting personal data on websites, ranging from sensitive information like their credit card information and residential addresses, to insignificant details like their height and weight. At the organization level, digitisation of their operations creates additional vulnerabilities for cyber-attackers to make their move. While cyber-attacks have always existed, the pandemic has significantly expanded the reach of these cyber-attacks, where many individuals and organizations alike were driven by circumstances to adopt technology in their operations. This creates a problem because many of such implementations usually happen without considerations of the cybersecurity issues that come with the use of technology. Moreover, it takes time for any preventive measures to be implemented, and this small window or gap is all that cyber-attackers need to work their magic. This is why cyber-attackers view the pandemic as a valuable opportunity to increase criminal activities, as they can feed off the vulnerability of individuals working from home. With lesser supervision and technical control over employees, cyber-attackers are emboldened to carry out cyberattacks in recognition of lacking data security measures (Deloitte, 2020).

Coupled with the increase in cyber usage, attackers further took advantage of the situation and created phishing emails centered around COVID-19, with the email's subject titled “Cure for COVID-19” or “New variant of COVID-19” (Figure 7). With thoughts of curiosity in wanting to know more on the latest news on COVID-19, victims are more susceptible to phishing attacks.



*Figure 7: Phishing email on COVID-19*

**Evolution of Methods - Punycode Phishing**

To make matters worse, cyber-attackers are constantly evolving at an explosive rate, to compete with security measures, attackers constantly update their methods to find a way around, one such example is punycode phishing.

In phishing emails, attackers persuade their victim to download files carrying a malware payload or to visit a link that sends the victim to a malicious website. This is usually done by creating a sense of urgency in hopes of lowering the victim's guard by diminishing their rationality, making them more vulnerable to the trap. However, in recent times, education on cybersecurity has been widely spread, lowering the chances of many from falling for such schemes, with methods such as looking at the URL of the link before clicking on it. One such example is being able to tell the between “apple.com” and “äpple.com”, one can somewhat tell that the second link is suspicious, where the “a” is replaced with “ä”, but one might have trouble telling the difference between “apple.com” and “аpple.com”. There might not look like a difference at first glance but the “a'' in the first legitimate website is being replaced by a cryillic character and has a different unicode, therefore leading to a different address from the legitimate one (Figure 8).



*Figure 8: URL replaced by cryillic characters*

This is just an example of attackers evolving their methods to bypass security measures. Thankfully, in current times, most browsers are updated to automatically block out and de-obfuscate the domain name first.

Although most browsers have been updated to counter punycode phishing, cybersecurity exists only if an exploit is discovered for humans to deter against. With just as many or perhaps more attackers out there as penetration testers, it is only a matter of time before attackers find other exploits that can circumvent the current security measures.

**Human Error and Possible Mitigation**

**The Effect of an Individual and ‘Human Error’**

As opportunities increase and techniques evolve for cyber-attackers, cybersecurity measures and software become even more robust and sophisticated. Despite this, technical security measures are effective only if humans properly utilize them (The Hacker News, 2021). The knowledge of this fact makes individuals at all levels employed by a company the major access point for cyber-attackers.

The unintentional action or the lack of action by employees and users that cause, spread, or allow a security breach to take place is known as ‘human error’. According to a study by IBM, 95% of cyber security breaches are primarily due to human error, indicating that this same amount of attacks would not have occurred, if not for human error (Ahola, 2021).

Human errors can be broadly classified into 2 categories - Skill-based and Decision-based:

1. Skill-based errors take place when the employee is aware of the correct course of action but is not able to take that action due to temporary mistakes, lapses caused by tiredness, distraction, or forgetfulness.
2. Decision-based errors take place when the employee is unaware or doesn’t have enough information about the given circumstance, thereby making a false decision. Inaction or the lack of action by an employee also comes under decision-based errors.

**Examples of Human Errors**

* Email Misdelivery:
  + According to Verizon’s 2018 breach report, misdelivery was the fifth most common cause of all cyber security breaches. It involves confidential information being sent accidentally to the wrong person due to overlooked sending details.
  + This is a skill-based error because the employee would know the correct recipients and the correct way to send the email to them but still makes an error because of negligence and lack of verification (Ahola, 2021).
* Poor Password Hygiene:
  + Even though passwords are ideally meant to protect and defend the system from a potential breach, it happens to be one of the most exploited access points by attackers.
  + According to Verizon, 61% of breaches are caused by stolen or compromised user credentials.
* Patching:
  + When software developers discover software vulnerability exploits done by cybercriminals wanting to access sensitive system infrastructure, they will fix the vulnerability and disseminate a patch to all users, which must be applied instantly to prevent breaches (Packetlabs, 2021).
  + Nevertheless, there will usually be a delay, which cybercriminals take advantage of to conduct a zero-day exploit, typically in a zero-day exploit (Appendix).
* Poor Access Control:
  + Inadequate access control allows bad actors or unauthorized persons to access secure, confidential information.
  + Cases of unauthorized access take place when important papers or devices are left unattended.

**Cyber Attacks due to Human Error**

* One of the most serious data breaches caused by human error was when a National Health Service practice revealed the email addresses of over 800 patients who had visited HIV clinics. The employee made the error of sending out an email notification to HIV patients, accidentally entering their email addresses to the “to” field, rather than the “bcc” field. (Ahola, 2021)
* The Equifax attack in the United States in 2017 is another example of human error. The company delayed the patching of a software security vulnerability. This exposed the personal information of over 140 million Americans and 8,000 Canadians to hackers. They failed to detect the vulnerable systems as they ran automatic scans instead of a manual, thorough and proactive penetration test, and hence failed to find and fix the error (Packetlabs, 2021).
* In August 2018 at Strathmore Secondary College in Strathmore, Australia, student records of more than 300 students on the school’s intranet, which is accessible by all the students and parents, were unintentionally published by a school employee. The published records exposed highly sensitive information about students with medical conditions, and whether students were on medication or had any treatment plans. This was touted as a “grave human error” (Meharchandani, 2021).

Given that employees are the “weakest link” in the chain of cybersecurity (Hoe, 2021), no company is spared from being targeted by cyber-attackers (Chalico, 2022), especially larger companies like government organizations that have larger databases, which cyber-attackers can reap more benefits from through exploitation. Coupled with the rise in occurrences of cyber-attacks in organizations over the past 2 years as a result of the pandemic (Figure 1), cyber hygiene has become pivotal in creating operational resilience. Thus, it follows that cyber security and awareness must be built at the individual level for every employee.

**Cybersecurity Mitigation Practices**

There are several cyber hygiene practices that individuals should adopt. The following list covers the more important practices and is non-exhaustive (Appendix).

1. Use Application Security Tools - AV, Firewall.
   1. AV software “blocks malware” from infiltrating one’s device and compromising one’s data. However, one should only install AV software from trusted vendors, and only run one AV tool on one’s device at any one time. Additionally, firewalls filter out unwanted incoming network traffic for one’s device, thereby protecting it from any form of malicious activity occurring in the Internet (Cipher, 2017).
2. Use Strong, Complex Passwords[[4]](#footnote-4).
   1. Having passwords of such nature is integral in enhancing cyber security of an organization, as it will help to safeguard critical data and networks against cyber-attackers. This can be easily managed using a password management tool (Cipher, 2017).
3. Protect Sensitive Personal Identifiable Information (PII)[[5]](#footnote-5).
   1. It is recommended that one should not reveal too much about oneself on open platforms like social media, given the sensitive nature of PII which can be exploited by hackers. Instead, one should consider reviewing their privacy settings across all their social media accounts (Cipher, 2017).
4. Avoid Using Public WiFi[[6]](#footnote-6).
   1. Given that public WiFi connections do not require any authentication to be established, it makes such connections more porous to everyone, including cyber-attackers, thereby making end users less secure and more vulnerable. Thus, it is recommended to use a Virtual Private Network (VPN), or keep WiFi off when not in use, so as to stay protected (Kaspersky, 2022).
5. Software Should be Constantly Updated.
   1. Patching outdated software in one’s devices, both in the OS and applications, is imperative in eliminating critical vulnerabilities that can be exploited by cyber-attackers to gain foothold in one’s devices (Cipher, 2017).

These are several cyber hygiene habits that employees should inculcate to ward off cyber threats, but it takes collective effort to prevent cyber attacks. As mentioned previously, one of the main causes of cyber attacks is human error and therefore employees are the weakest link in the chain of cybersecurity. However, they can collectively help to form a ‘human firewall’ that fights cyber threats. “A human firewall is the real-world equivalent of a traditional network firewall.” (Meta Compliance, 2021)

**Conclusion**

Cybersecurity is everyone’s responsibility, and empowerment is necessary to uphold that responsibility. The concept of a human firewall empowers the employee with the right tools and knowledge, and ensures that they are no longer an easy target for cybercriminals, but instead they are instrumental in the fight against these cyber-attackers.

(2460 words)

**References**

* Clear Insurance. (2021, September 27). *10 biggest cyber attacks in history*. Retrieved April 14, 2022, from<https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/>
* Cipher. (2021, September 20). *10 personal cyber security tips - #cyberaware*. Retrieved April 14, 2022, from<https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>
* StealthLabs. (2022, April 6). *Cyber security threats and attacks: All you need to know*. Retrieved April 14, 2022, from<https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/>
* Ahola, M. (n.d.). *The role of human error in successful cyber security breaches*. usecure Blog. Retrieved April 14, 2022, from<https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches>
* Deloitte Switzerland. (2020, December 15). *Impact of covid-19 on Cybersecurity*. Retrieved April 14, 2022, from<https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>
* BBC News. (2018, November 19). *TalkTalk Hack Attack: Friends jailed for cyber-crimes*. Retrieved April 14, 2022, from<https://www.bbc.com/news/uk-england-stoke-staffordshire-46264327>
* IMDA. (n.d.). *By households and individuals 2019*. Retrieved April 7, 2022, from<https://www.imda.gov.sg/-/media/Imda/Files/Infocomm-Media-Landscape/Research-and-Statistics/Survey-Report/HH2019_Infographics.pdf>
* Chalico, C. P. (2022, March 11). *Your employees are The weakest link in your cybersecurity chain. Are humans the weakest link in cybersecurity?* EY Canada. Retrieved April 14, 2022, from<https://www.ey.com/en_ca/cybersecurity/your-employees-are-the-weakest-link-in-your-cybersecurity-chain>
* Cisco. (2021, July 22). *What is cybersecurity?* Retrieved April 14, 2022, from<https://www.cisco.com/c/en_sg/products/security/what-is-cybersecurity.html>
* Cyber Security Agency. (2021, July 8). *Singapore Cyber Landscape 2020*. Retrieved April 14, 2022, from<https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2020>
* SingCERT. (2020, July 8). *Phishing in the time of COVID-19*. Retrieved April 14, 2022, from<https://www.csa.gov.sg/singcert/publications/phishing-in-the-time-of-covid-19>
* TryHackMe. (n.d.). *Cyber security training*. Retrieved April 14, 2022, from<https://tryhackme.com/>
* CyrusOne. (2018, March 30). *Disaster recovery*. Retrieved April 14, 2022, from<https://cyrusone.com/solutions/data-centers/disaster-recovery/>
* Cooper C. (2018, May 16). *Wannacry: Lessons learned 1 year later*. Symantec Blogs. Retrieved April 14, 2022, from<https://symantec-enterprise-blogs.security.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later>
* Empson, R. (2011, April 23). *Hack attack: Sony confirms PlayStation Network outage caused by 'external intrusion'*. TechCrunch. Retrieved April 14, 2022, from<https://techcrunch.com/2011/04/23/hack-attack-sony-confirms-playstation-network-outage-caused-by-external-intrusion/>
* Empson, R. (2011, April 23). *Hack attack: Sony confirms PlayStation Network outage caused by 'external intrusion'*. TechCrunch. Retrieved April 14, 2022, from<https://techcrunch.com/2011/04/23/hack-attack-sony-confirms-playstation-network-outage-caused-by-external-intrusion/>
* Hack The Box. (n.d.). *Hacking training for the best*. Retrieved April 14, 2022, from<https://www.hackthebox.com/>
* Cyber Security Agency. (2018, August 18). *How to Stay Safe on Public Wi-Fi*. Retrieved April 14, 2022, from<https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/how-to-stay-safe-on-public-wi-fi>
* Hoe K. W. (2021, June). *Culture and cyber security: How Cultural Tightness-Looseness Moderates the Effects of Threat and Coping Appraisals on Mobile Cyber Hygiene*. [PhD Dissertation, Singapore Management University]. Institutional Knowledge at Singapore Management University. Retrieved February 28, 2022, from<https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=1354&context=etd_coll>
* Kaspersky. (2022, February 9). *How to avoid public WIFI security risks*. Retrieved April 14, 2022, from<https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks>
* McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia*. BBC News. Retrieved April 14, 2022, from<https://www.bbc.com/news/39655415>
* Meharchandani, D. (2021, October 21). *Top 5 cyber attacks due to human error*. ThreatCop. Retrieved April 14, 2022, from<https://threatcop.ai/blog/top-5-cyber-attacks-and-security-breaches-caused-by-human-error/>
* Netcraft News. (2016, March 17). *95% of HTTPS servers vulnerable to trivial MITM attacks*. Retrieved April 14, 2022, from<https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html#:~:text=The%20remaining%2095%25%20are%20therefore,in%2Dthe%2Dmiddle%20attacks>
* Wolf & Company, P.C. (2021, April 26). *Punycode phishing - how to prevent attacks*. Retrieved April 14, 2022, from<https://www.wolfandco.com/resources/insights/punycode-phishing-how-to-prevent-attacks/>
* Palo Alto Networks. (n.d.). *What is a denial of service attack (dos)?* Retrieved April 14, 2022, from<https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos/>
* Ripley, W. (2014, December 18). *Why Sony hasn't learned from 2011 PlayStation Hack*. CNN. Retrieved April 14, 2022, from<https://edition.cnn.com/2014/12/18/world/asia/sony-hack-lab-ripley/index.html>
* Norton. (2018, May 26). *The risks of public wi-fi*. Retrieved April 14, 2022, from<https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html/>
* Packetlabs. (2021, July 26). *The role of human error in cybersecurity breaches*. Retrieved April 14, 2022, from<https://www.packetlabs.net/posts/human-error-in-cybersecurity/>
* Contrast Security. (n.d.). *What is penetration testing?* Retrieved April 14, 2022, from<https://www.contrastsecurity.com/knowledge-hub/glossary/penetration-testing/>
* Meta Compliance. (2021, September 27). *How To Build A Human Firewall To Protect Your Organisation*. MetaCompliance. Retrieved April 14, 2022, from<https://www.metacompliance.com/blog/human-firewall/>
* Touhid. (2019, March 8). *Six Key Elements of Cybersecurity*. Cyber Threat & Security Portal. Retrieved April 14, 2022, from<https://cyberthreatportal.com/elements-of-cybersecurity/>
* IBM. (n.d.). *What is cybersecurity?* Retrieved April 14, 2022, from<https://www.ibm.com/topics/cybersecurity/>
* VMware. (2022, April 9). *What is disaster recovery as a service (DRaaS)?* Retrieved April 14, 2022, from<https://www.vmware.com/topics/glossary/content/disaster-recovery-service-draas.html/>
* VMware. (2022, April 9). *What is Network Access Control?* Retrieved April 14, 2022, from<https://www.vmware.com/topics/glossary/content/network-access-control.html>
* *What is SQL injection? tutorial & examples: Web security academy*. What is SQL Injection? Tutorial & Examples | Web Security Academy. (n.d.). Retrieved April 14, 2022, from<https://portswigger.net/web-security/sql-injection>
* Imperva. (2020, July 5). *WannaCry Ransomware*. Retrieved April 14, 2022, from<https://www.imperva.com/learn/application-security/wannacry-ransomware/>
* The Hacker News. (2021, February 4). *Why Human Error is #1 Cyber Security Threat to Businesses in 2021*. Retrieved April 14, 2022, from<https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html>
* Secure Disruptions. (2019, November 8). *What Are The 7 Types Of Hackers [Explain a comprehensive list of all the types of hackers]*. Retrieved April 14, 2022, from <https://www.youtube.com/watch?v=CHb9iSKV_dI>
* ScienceDirect Topics. (n.d.). *Hacktivist*. Retrieved April 15, 2022, from <https://www.sciencedirect.com/topics/computer-science/hacktivist#:~:text=Hacktivists%20are%20groups%20of%20criminals,their%20political%20views%20or%20practices>

**Appendix**

**Elements of Cybersecurity**

There are 6 key elements in cybersecurity, namely:

* Application Security
* Information Security (InfoSec)
* Network Security
* Disaster Recovery Planning
* Operational Security (OPSEC)
* End User Security

**Application Security**

As the first key element of cybersecurity, it adds security features within applications in its developmental stages to safeguard those applications against cyber attacks. Additionally, it prevents various kinds of cyber threats, such as Denial-of-Service (DoS) and Structured Query Language Injection (SQLI) attacks, from exploiting vulnerabilities in the source codes of web-based applications and websites. Several application security tools exist, such as firewall and AV software (Touhid, 2019).

**Information Security**

InfoSec refers to the “process or methodology of preventing unauthorized access, use, disclosure, disruption, modification, or destruction of information” like personal information, login credentials and social media profile. This is anchored on 3 main principles known as C.I.A. - Confidentiality[[7]](#footnote-7), Integrity[[8]](#footnote-8) and Availability[[9]](#footnote-9) (Touhid, 2019).

**Network Security**

This deals with the restriction of unauthorized access to computer networks, especially those that are highly sensitive in nature, based on “a set of rules and configurations”. There are hardware technologies, such as VPN[[10]](#footnote-10) and Network Access Control (NAC)[[11]](#footnote-11), and software technologies like network firewalls that help to protect and monitor unauthorized access of a network or resources (Touhid, 2019).

**Disaster Recovery Planning**

A Disaster Recovery Plan (DRP), as the name implies, contains procedures describing “how work can be resumed quickly and effectively after a disaster”, particularly after a cyber incident. There are various types of DRPs that are suited based on the varying needs of companies, such as the Data Center Disaster Recovery[[12]](#footnote-12) and Disaster Recovery as a Service (DRaaS)[[13]](#footnote-13) (Touhid, 2019).

**Operational Security**

Also known as procedural security, OPSEC helps to ensure the security of sensitive information in an organization, by identifying the critical information and developing a protection mechanism around it. It also involves identifying and classifying the types of cyber threats, as well as vulnerability and risk assessments (Touhid, 2019).

**End User Security**

Humans are the “weakest link” in the chain of cybersecurity (Hoe, 2021). This is due to lack of awareness, poor cyber hygiene or weak security protocols in place. End user threats can be formed through a multitude of ways, such as through usage of social media and password creation. As such, this poses the largest cybersecurity risk in any business (Touhid, 2019).

**Types of Cyber Attacks**

The following list of types of cyber attacks, referenced from Figure 2, page 5, is non-exhaustive.

**Malware**

This is the most common type of cyber attack. It involves using malware - a malicious software, such as a virus or ransomware - to infect a system or network through various ways, such as reconnaissance (information harvesting) and preventing access to critical infrastructure in the system or network (StealthLabs, 2020).

**Phishing**

This can occur in the form of emails, text or voice messages. Attackers would make use of these media to masquerade themselves as reliable senders, thereby deceiving the end user into clicking the malicious link and believing that the information is credible. This will facilitate the propagation of the attack, by enabling malware installation or reconnaissance (StealthLabs, 2020). This form of attack is also commonplace, accounting for more than 80% of cyber-attacks that have been reported (StealthLabs, 2020).

**Spear Phishing**

A more complex phishing attack involving cyber-attackers exploiting the vulnerabilities of privileged users like system administrators, this form of attack comprises over 71% of targeted cyber-attacks (StealthLabs, 2020).

**Man-in-the-Middle**

As the name implies, this form of attack happens when an attacker acts as a middleman to intercept and interpret a two-party communication, in order to harvest critical data from the user and return unexpected responses to the user (StealthLabs, 2020). Only a small handful of 5% of HTTPS servers are immune to such attacks (NetCraft, 2016).

**Denial-of-Service**

A DoS attack aims to shutdown a machine or network, rendering it inaccessible to its intended users. This is done by flooding the target machine or network with traffic, or sending it information that triggers a crash (Palo Alto Networks, n.d.), thereby rendering the machine or network unresponsive to legitimate processes and requests. Another form of attack related to DoS is Distributed Denial of Service (DDoS) attack, an advanced form of DoS attack involving several infected machines used by attackers to infect a target system or network. 8.4 million DDoS attacks were reported in 2019 (StealthLabs, 2020).

**Structured Query Language Injection**

A SQLI is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database, so as to access data that they are not normally able to retrieve (PortSwigger, n.d.). Such attacks comprise around 65% of all web application attacks (StealthLabs, 2020).

**Zero-Day Exploit**

When a software or hardware vulnerability is announced, such attacks can occur before these vulnerabilities are patched up. This is so that hackers can take advantage of the small window of opportunity to exploit the patchless vulnerability. By 2021, it was projected that such attacks would increase to 1 per day (StealthLabs, 2020).

**Advanced Persistent Threats**

Such attacks happen when a cybercriminal is able to penetrate a system or network illegally and stay dormant for a long period of time. These attacks usually target organizations, with 45% of organizations thinking that they are vulnerable to such attacks (StealthLabs, 2020).

**Ransomware**

This is actually a form of malware attack that involves attackers encrypting a user’s data and threatening the user to “publish or block access” to data until the victim pays the demanded ransom. It was projected that such attacks could cost global businesses USD 20 billion by 2021 (StealthLabs, 2020). The most well-known ransomware attack is WannaCry in 2017.

**Domain Name System**

In these attacks, cybercriminals would exploit vulnerabilities in the Domain Name System (DNS) servers, so as to perform DNS Hijacking and DNS Tunneling. The former is the process of redirecting users to malicious sites, while the latter involves extracting data from infected systems while bypassing firewalls. Such attacks can cost up to USD 924,000 on average in 2020 (StealthLabs, 2020).

**Cybersecurity Mitigation Practices**

There are other forms of cyber hygiene practices that one should adopt, in addition to those mentioned in pages 14 and 15.

**Be Wary of Phishing Scams**

Avoid opening unknown emails, clicking on suspicious or unfamiliar links and downloading suspicious data, even if the sender is someone whom you may be familiar with. Moreover, look out for emails containing grammatical errors, which is highly indicative and disapproving of the sender’s credibility. This will prevent one’s device from getting infected with malware (Cipher, 2017).

**Backup Data Regularly**

Given the porous nature of the Internet and the inevitability of cyber breaches, critical data can be more prone to be stolen as a result, which can only be recovered by “erasing the systems” and “restoring with a recently performed backup”. Employees can follow the “3-2-1 backup rule”, which involves keeping “3 copies of data” on 2 different storage media types and “1 copy in an off-site location” like cloud storage (Cipher, 2017).

1. Script kiddies are amateur hackers who lack coding expertise and knowledge, and unknowingly run available hacking code or tools written or developed by others, without realising or understanding what the purpose and output of the code is, or caring much about the quality of the code and eventually, that of the attack. They do so primarily to “impress their friends” or “gain attention” from others (Secure Disruptions, 2019). [↑](#footnote-ref-1)
2. They are a group of cybercriminals who intend to conduct attacks collectively in order to perpetuate their political agenda (Fowler, 2016) and bring about social changes to society. They usually target governments and organizations, so as to garner attention from the masses or “share their displeasure over opposing their line of thought” (Secure Disruptions, 2019). [↑](#footnote-ref-2)
3. These hackers have been employed by the government of their country / state / nation to penetrate into other governments’ systems while bypassing security, in order to harvest sensitive, confidential data from those systems (Secure Disruptions, 2019). [↑](#footnote-ref-3)
4. Some requirements for a strong, complex password as recommended by the National Institute of Standards and Technology’s (NIST) include having “at least 8 characters” with a “maximum length of 64 characters”, of which there should be “at least one lowercase letter, one uppercase letter, one number, and four symbols” (Cipher, 2017). [↑](#footnote-ref-4)
5. Also commonly referred to as personal data, PII is any information that can be used by a cybercriminal to identify or locate an individual. Such information encompasses the individual’s name, home address, phone numbers, Date of Birth, Social Security Number, IP address, location details, or any other physical or digital identity data (Cipher, 2017).mon public amenities, such as food establishments, train stations or the airport, and they allow people to use the Internet fr [↑](#footnote-ref-5)
6. Public WiFi connections exist at common public areas like train stations, food establishments and airports, and people can connect freely without prior authentication (Norton, 2018). [↑](#footnote-ref-6)
7. Confidentiality involves restricting the access of sensitive data (ie. personal data, login credentials) to authorized users or a limited number of people (Touhid, 2019). [↑](#footnote-ref-7)
8. Integrity involves preventing unauthorized users from changing critical information, thereby retaining its accuracy and completeness (Touhid, 2019). [↑](#footnote-ref-8)
9. Availability ensures that access to critical information and resources is limited to authorized users (Touhid, 2019). [↑](#footnote-ref-9)
10. VPN keeps browsing sessions launched by a user private, such that data travelling to and from the user’s devices is encrypted. This makes it more difficult for cyber-attackers to eavesdrop on and interfere with the user’s online activities (Cyber Security Agency, 2018). [↑](#footnote-ref-10)
11. NAC is the act of keeping unauthorized users and devices out of a private network (vmware, 2022). [↑](#footnote-ref-11)
12. Data Center Disaster Recovery is a form of organizational planning to resume business operations following an unexpected event, such as a cyber attack, which may damage or destroy critical data, software and hardware systems (CyrusOne, 2018). [↑](#footnote-ref-12)
13. DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third party cloud computing environment (vmware, 2022). [↑](#footnote-ref-13)