Cyber Security

What is cyber security and what does it do?
Cyber security covers the protection of all aspects of information technology (IT), including:

- PC (Personal Computers), Laptop, Smartphones, and other devices.
- Network Infrastructure.
- Servers/Cloud Computing.
- The physical storage of digital information on CDs, USB, and internal drives.

Cyber security must cover all 7 layers of the OSI (Overall Satisfaction Index) framework (Check Point, 2022), while also ensuring and educating the users of such systems to have due diligence regarding credentials, as if they become compromised then the system will be put at risk.

The cyber security industry that employs approximately 1 million people worldwide and ~30000 in Australia (Cisco-Portal.Com Team, 2021).

Recent cyber security attacks are a mixture of social engineering and abuse of known exploits in systems such as email phishing attacks from black hat hackers. These attacks threaten targets with damage to their computers or dispersal of their personal information if the demands are not complied with (Sujata, 2021).

On offensive cyber security:

The state of the art in cyber security is Machine Learning (Kirandeep Kaur, 2021). This could be used to bypass and dismantle cyber-security systems faster than most prevention methods and detection tools can keep up with.

On defensive cyber security:

One method of system defense is by comparing predictive logic against behavioral signals from an external source that suggests a threat. Machine learning algorithms are being employed to discover harmful network traffic. They are called Intrusion Detection systems (IDS) (Check Point, 2022).

Currently, in cyber security, the best way to secure information stored on a digital device is to ensure that network infrastructure is correctly configured, physically secured, and users are educated on the potential risks and permissions/passwords are correctly assigned (Bradly M, 2021).

When configuring devices use a strong password and change the default settings. It is also essential to avoid outdated and insecure protocols such as telnet and WPA within sensitive environments.

Physical security is ensuring that network devices and infrastructure are behind locked doors and that only authorized users are granted access with passwords.

Another major exposure point for IT environments is the users themselves. As security breaches have increased in frequency and consequence, industry has put in place many measures to mitigate the risks. As back-end security has improved, malicious actors have moved their attention to the most vulnerable component in any system, the users. All administrative controls have one major flaw, the need for human access. In a 2016 study, 93% of data breaches were attributed to human error (Evans. M et al pg .3 table. 1 [https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1657]). It is therefore essential that users are educated on attacks they may encounter and given the training and tools to identify and avoid threats.

Access to the WIFI password should be restricted to so that is not common knowledge in the office/workplace and only the network administrator/authorized personnel know the WIFI password so that someone cannot ask anyone for the password and gain admin access to the whole network.

In the Australian defence force, they use a cloud-based wide area network (WAN) network that is secured to exchange secret information (Microsoft News Center,2020)

Going forward in cyber security, nations are now performing cyber-attacks against other nations, in acts of aggression or war which can also be called a new military strategy as it is the fifth dimension of war. (Donghui, 2016).

Cyber-attacks are becoming commonplace, such as what happened in Ukraine and Russia in 2022 before war broke out a cyber-attack was performed to cripple Ukraine's economy and military (James Pearson,2022).

North Korea frequently performs cyber-attacks against South Korea as a clandestine military strategy (Donghui, 2016).

Based on these developments Cyber security attacks by a rouge actor will soon be able to perform fast, easy effective attacks against computer systems on small mobile devices as depicted in the game series Watchdogs (Jill Scharr, 2014).

In the game, a city-wide operating system "ctOS" operates many electronic devices such as ATM (Air Traffic Management), Traffic lights, and security cameras, and stores the residents personal information such as bank cards, address, age, and occupation, creating a large network containing sensitive personal information, the protagonist(Aiden) an individual who breached/hacked the ctOS system this allows him to alter the networks devices, traffic lights, for example, to change while in a high-speed chase with authorities and being able to walk up to any ATM in the city and withdraw money at a victim/NPC expense (Jill Scharr, 2014).

These developments could enable completely automated cyber-attacks without the need to have a person actively carrying out the attack. Instead by defining the intended outcome, attacks may be conducted through automated processes which enables fast and easy cyber-attacks for people with minimal computer knowledge. This would be possible through machine learning and clever application with a streamlined approach (Jill Scharr, 2014).

An example of the above is an extremely small brute-forcing device to attack a WIFI password and crack within seconds by imputing the network SSID, you can achieve this by using quantum computers which have extreme computational power far more than systems which use standard binary language binary computers thus cracking hashed passwords in seconds (McElhearn, 2020).

Soon, quantum computers and their applications regarding their computational power will make many current protocols obsolete, and methods of encryption a large part of cyber security to also become obsolete, foundations of network working such as the OSI layers will need to be completely reworked (NIST, 2016).

Even if quantum computing technology does not become available, current manufacturing technologies are likely to improve, increasing computational capacity and resulting in the same outcomes (Lawrence Berkeley, 2014).

Soon with AI (Artificial Intelligence) technology there will be a potential for AI technology to replace radio operators with Artificially intelligent Radio operators. These would be vastly superior to the human type much like the way self-driving cars theoretically would be safer than human drivers due to computers never losing focus (Techopedia, 2022). This is important to consider in the context of cyber security as computers can be hacked, unlike humans.

What is the impact development? What is likely to change?

The potential impact of easy-to-use small mobile devices for cyber-attacks creates the need for new systems and applications to be able to deal with the unique threats they present. This in turn would cause a significant need for security experts and designers to update security protocols and encryption algorithms to ensure that cyber security can be maintained, also being able to function unimpeded by a new age of hackers and security risks (Norwich University, 2021).

In the next 3 years the use of the cloud and its many potential applications and risks to cyber security, experts will have to figure out and produce new methods to allow for cyber security to be maintained (Zainab Al Mehdar, 2018). Cloud-based storage such as Drobox and Google Drive, cloud-based networks and other similar technologies are used by companies to store sensitive information. As cloud technologies become more deeply integrated into personal life and business operations, there will be a greater necessity to develop secure in this domain.

Developments with communication and data transmission technologies could potentially affect the way radio communications are conducted in the Australian Defense Force (ADF). Signals could go from command post to command post creating a network, to an extremely developed command post with extremely powerful signal equipment in Canberra, combine that with AI radio operators you have changed an entire core in the military. (Jill Scharr, 2014).

The above developments will change the demands of cyber security, network administrators, data entry workers, and office workers, all jobs where people who work with a network worth securing from cyber-attacks is necessary due to sensitive information that is stored on the network.

How will this affect you and your family or your friends in your daily life?

In my daily life cyber security matters to me because I use a computer for many functions in my current jobs (computer Technicon, personal trainer, UNI student) such as sending invoices and storage of information that is sensitive, being able to save UNI work for later and build off previous saves. This would enable me to fix something after being submitted because I have a copy of this report, for example, if I had a security breach say all my files got deleted then I would have serious work output issues, having to do this whole report again and lose all or a lot of retained information, that is not externally backed up.

Cyber security as an industry also affects my job prospects because I am looking to gain employment in cyber security via UNI studies and my cert 4 in cyber security if something big happened in cyber security such as a ground-breaking invention, then I would have to be familiar with this modern technology such as quantum computers making WPA2 networks obsolete (NIST, 2016).

Cyber security affects family members as well because they store memories in the form of digital photos on a cloud or local device. Family members may also store personal information such as copies of birth certificates, driver's licenses, or other sensitive personal information which if in the wrong hands can be used for identity theft (Sujata, 2021).

Cyber security also affects a company's reputation, the April 2021 Facebook had a breach where users' birthdates, phone numbers, and passwords were leaked by hackers, exposing personal information, and causing people to distrust Facebook changing some people's behaviors about what they share when using Facebook (Kate O'Flaherty, 2021).

In conclusion, as technologies advance, people and organizations will experience new means of cyber-attacks, and previous methods of securing networks will increasingly become obsolete, requiring cyber security experts to develop new tools and methods of securing information and technology.

References

Cisco-Portal.Com Team, 2021, How Many Cybersecurity Jobs Are There? - CISO (Chief Information Security Officer) Portal, Retrieved 05/07/2022.

Kirandeep Kaur, 2021, Role of Machine Learning in Cyber Security Retrieved 14/07/2022.

Sujata, 2021, Social Engineering Attacks, Retrieved 09/07/2022.

Check Point, 2022, What is an Intrusion Detection System (IDS), Retrieved 09/07/2022.

Bradly M, 2021, Why You Should Change Wi-Fi Network Default Passwords, Retrieved 08/07/2022.

Mark Walker, 2017, Cable's Role in Cybersecurity, Retrieved 09/07/2022.

Microsoft News, 2020 Department of Defence selects Microsoft, Retrieved 09/07/2022.

Donghui Park, 2016, North Korea Cyber Attacks: A New Asymmetrical Military Strategy, Retrieved 09/07/2022.

Jill Scharr, 2014, Could 'Watch Dogs' City Hacking Really Happen?, Retrieved 09/07/2022.

Kirk McElhearn, 2020 How Quantum Computing Will Affect Computer Security and Passwords , Retrieved 09/07/2022.

Nist, 2018, Quantum Communications and Networks | NIST Retrieved 09/07/2022.

Lawrence Berkeley, 2014, Extending Moore's Law: Shrinking transistor size for smaller, more efficient computers, Retrieved 09/07/2022.

Techopedia Staff, 2022,Are autonomous vehicles safer than cars operated by humans?, Retrieved 09/07/2022.

Norwich University, 2021, The Importance of Implementing Security Protocol, Practices and Awareness | Norwich University Online, Retrieved 10/07/2022.

Zainab Al Mehdar, 2018, Cybersecurity and Cloud Computing: Risks and Benefits | Rewind, Retrieved 10/07/2022.

Kate O'Flaherty, 2021, Facebook Data Breach: Here's What To Do Now ,Retrieved 10/07/2022.