Cyber Security

Across the IT industry a lot of the most sought after jobs lie in the Cybersecurity Industry. Cybersecurity specialists keep the protection of digital information as their main priority. In the current era of technology, there is no part of the IT industry that doesn’t require protection. The most vulnerable sectors are healthcare, finance, government, manufacturing and transport.

An example of a cyber attack:

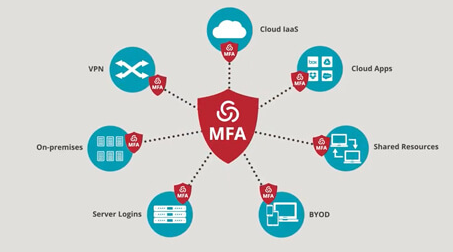
<https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html?socialshare=lightbox1>

To mitigate these threats before they happen, specialists are heavily involved in tasks such as:

* Development, testing, analysis and implementation of security systems.
* Assessment and management for system vulnerability.
* Reducing response time to security threats and attacks.
* Development of threat prevention strategies.
* Regularly generating security reports for executives.

The ACSC (Australian Cyber Security Centre) run through the Australian Government is tasked with protecting the Government, Large organisations and Infrastructure, Small and Medium Business, and Individuals and Families from cyber attacks. With each of these categories, they offer four guides each at a certain level of expertise depending on your knowledge and background in IT. In its various reports, it highlights relevant technology and steps to take precautions against becoming vulnerable:

* Use effective Multi-Factor Authentication (MFA) methods:



* Secure accounts using a Password Manager. Examples:
  + NordPass
  + RoboForm
  + Dashlane
  + Keeper
  + 1Password
* Improve Wifi router security:
  + Change router’s default username and password
  + Change default Wifi name and password
  + Use strongest Wifi encryption (WPA2, WPA3)
  + Update router to latest firmware
  + Disable remote management and Universal Plug and Play (UPnP)
* Secure Internet of Things (IoT) Devices:
  + Reboot devices regularly
  + Apply regular updates
  + Turn off device when not in use
* Encrypt your hard drive:
  + Enable disk encryption
  + macOS (FileVault)
  + Windows 10 (BitLocker)
  + Open Source: DiskCryptor, VeraCrypt, 7-Zip, Kleopatra, AxCrypt
* Enhance your Cyber awareness:
  + Periodically clean out your inbox (archive, delete)
  + Don’t let mail accumulate
  + Destroy documents containing personal information.

*Emerging Technologies*

**Hardware Authentication**

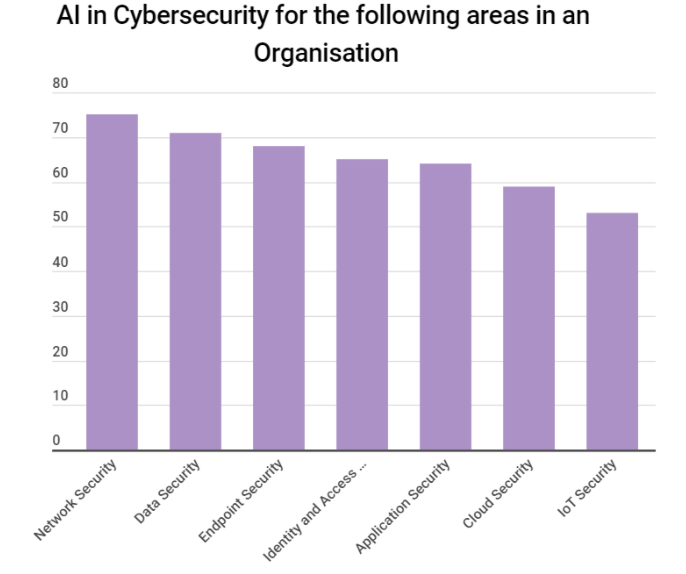
This technology is used as authentication that relies on devices like smartphones, laptops, or any hardware systems held by an authorized user. The volume of usernames and passwords are well known, so a more secure form of authentication is needed. Authentication is an important feature for Internet of Things, where networks want to ensure the user trying to gain access is a user that should be given access. A fundamental limitation of hardware authentication is that it can be lost or stolen which creates login issues for users.

**Artificial Intelligence and Machine Learning**

AI is seen as technology that emulates human performance by learning, drawing conclusions, analyzing complex information, engaging in dialogue with people, enhancing human cognitive performance and ultimately replacing people in non-routine tasks. AI technology is used to protect data against increasingly sophisticated and malicious malware, ransomware, and social engineering attacks. While AI is not conscious yet, there is a very possible future where AI cognitive autonomy predicts and mitigates cyber-attacks.

Artificial Intelligence and Machine Learning are the same in many respects. The end goal is to have the computer act independently with minimum programming.

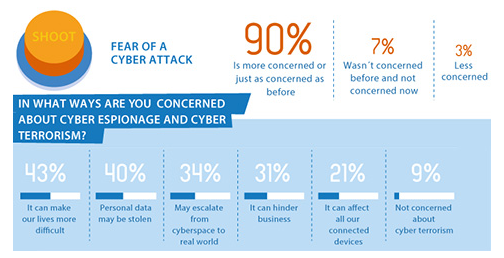
Machine Learning can potentially provide the fastest way to identify new cyber-attacks, draw statistical inferences, and push that information to endpoint security platforms. Threat intelligence is one of the few situations Artificial Intelligence and Machine Learning can be a crucial functionality for cybersecurity. Artificial Intelligence and Machine Learning can bolster identity management by cross-checking the authenticity of data across multiple databases.



**Blockchains**

Blockchains are digital currency that operate independently from a central banks. They allow anyone to send value anywhere in the world where the blockchain file can be accessed. Each chain has a dedicated online database stored in a distributed, peer-to-peer fashion. The storage devices for the database are not all connected to a common processor and each block has a timestamp and a link to a previous block. Blockchains are Internet-based, public databases where transactions can only be added once they are authenticated through equations that prove authenticity of the data. It is a public account book of all the transactions that have ever taken place. From the emergence of Blockchain technology, a security system used in a company can potentially leverage a distributed public key infrastructure system for verifying devices and workers in the company. The use of Blockchain technology with AI can create a robust authenticated verification infrastructure that can monitor potential cyber threats.

*Impact of Cyber Security*



A survey distributed through GFI Software in 2015 ascertained that increasing cyber crime was creating a less stable and more stressful business and home life. Key findings from the survey included:

* With healthcare becoming more and more digitized, concerns are that cyber criminals will turn and focus heavily on this industry.
* At least half of the respondents still believe that malware posed the greatest threat to individual and business security.

With a lot of the survey focusing heavily around the implications of attacks on businesses both large and small, cyber security is a key player in keeping these industries safe. Major corporations have been attacked in acts of espionage or geopolitical retaliation. In these scenarios, up to hundreds of thousands of people can be severely affected by the fallout of attacks. Financial hardship is a brutal result from attacks on digitized information such as usernames and passwords, credit card data and health records. Other implications and effects that cyber security technology can prevent are reputation loss, fines and civil or criminal legal proceedings.

On a more personal level, equipment such as traffic lights, CCTV cameras and traffic meters all networked to improve efficiency and reduce cost are at risk, seen by the NSA report in November 2014 which confirmed that the US power grid had been attacked by cyber criminals. Cyber security is also aiming to make normal everyday life easier, as there is a genuine fear that cyber criminals are are creating less productivity within our lives or workplaces due to unnecessary stress from a potential attack. The follow over affects include potential acts of physical crime and terrorism as well.

In terms of how will cyber security affect myself? I have had a close run in with a cyber attack, back when Sony’s PSN data had been hacked in 2011. Thankfully I wasn’t affected, as I hadn’t input any credit card details, just a basic user account setup. To think that a company as big and influential in gaming at that time in Sony could be brought to its knees so easily was a very worrying thought. At that time in my life, I assumed all sensitive data that you entrusted to any company in making an account was watertight, but that instance opened up my eyes to how easily peoples lives can be affected by poor company oversight.

My father was involved in the AMP attack during 2019. He is a Project Manager in the insurance division. The disruption that it caused was massive. My father told me that the attacks were so complex and obscure that they had to allow themselves to be attacked for a few days to understand what data the attackers were after. Once that was identified, honey pots were created to lure the attackers, but the attackers were incredibly intelligent. The attacks went on for around a week, and were only stopped when the attackers had lost interest in the AMP servers and taken what they had intended. Damage limitation was minimal, as my father explained that they had to ride the attack as best they could while putting basic prevention systems in place. A Lot of the restructuring of data security happens after the attack, as that is the best time to reevaluate the infrastructure set in place.

**References**

* 2021. [online] Available at: <https://www.cyber.gov.au/acsc/view-all-content/guidance/personal-cyber-security-advanced-steps-guide> [Accessed 11 October 2021].
* Centrify.com. 2021. [online] Available at: <https://www.centrify.com/media/4339199/mfa-explainer-video.jpg> [Accessed 11 October 2021].
* Au.cybernews.com. 2021. *Best password managers in Australia - October 2021 - Cybernews.com*. [online] Available at: <https://au.cybernews.com/lp/best-password-managers-au/?utm\_source=bing&utm\_medium=cpc&utm\_campaign=Bing\_CN\_PM\_S\_T1\_AU\_G\_EN&utm\_content=Password%20Managers&utm\_term=password%20managers&msclkid=4ae2fe845f8d1213c5149fe78ecf84a2> [Accessed 11 October 2021].
* Services, P., 2021. *What Is Network Security?*. [online] Cisco. Available at: <https://www.cisco.com/c/en\_au/products/security/what-is-network-security.html> [Accessed 11 October 2021].
* Help Net Security. 2021. *The business and social impacts of cyber security issues - Help Net Security*. [online] Available at: <https://www.helpnetsecurity.com/2015/02/26/the-business-and-social-impacts-of-cyber-security-issues/> [Accessed 12 October 2021].
* StartupTalky. 2021. *Top 5 Technologies That Can Change The Future Of Cybersecurity*. [online] Available at: <https://startuptalky.com/technologies-future-cybersecurity/#:~:text=%20Top%205%20Emerging%20Technologies%20That%20Are%20The,breakdown%20in%20traditional%20security%20models.%20The...%20More%20> [Accessed 12 October 2021].