**Cybersecurity**

Simply put, cybersecurity is the information technology field that focuses on protecting networks, systems, and data, including personal and corporate information from threats that expose vulnerabilities in systems and exploit them, usually done over the internet. This is done through firewalls, antivirus software, encryption tools, and anonymity tools such as proxy servers and virtual private networks (VPNs). As technology develops, many new developments are implemented into the world of cybersecurity, for not only protection but also to be utilised as means of breaching security systems.

One of the largest innovative technologies that is slowly being implemented into the world of cybersecurity is artificial intelligence and machine learning. This not only includes security features that are already implemented into technology such as face recognition, but it is also being developed into security systems that learn and develop new methods of threat detection and prevention (Ziomek, 2021). AI has the potential to learn from current and previous data such as historic attacks and prevention methods and develop methods to not only understand future attacks but also prevent the attack in whole with no interaction from people, aside from the initial setup of the system. Current methods of cybersecurity are considered rigid and not capable of adapting to new or different types of attacks, whereas machine learning can recognise patterns and adapt its own capabilities and operations as it sees fit (Kangas, 2022). Being a computer, the decision making of artificial intelligence is far faster than a human’s, meaning the prevention of attacks can take place much faster than it could if it was done by a person. The impact of this is a potential for a future of much stronger defense systems, as well as much less monitored systems, with less interaction required, only ever needed for checkups and data entry to allow the algorithm to further develop. While this will bring a new wave of security methods, it will also bring about new developments in the breaching of these systems. While the systems will be designed to adapt to different approaches, it’ll require pre-existing knowledge to develop prevention methods such as that.

Blockchain technologies are a relatively modern technological breakthrough popularized through cryptocurrency mining that has been implemented into the field of cybersecurity. They involve storing data in “blocks” between systems and devices and connecting them through cryptography chains (IBM, 2021). This works similarly to a peer-to-peer network in which data is shared between devices. This effectively makes it much more secure as there is not only one network to breach, but many would need to be breached to collect all the data. Blockchain networks can be either public, such as cryptocurrency, or private, such as a business system. This technology in terms of cybersecurity will likely not be very applicable for personal security and would better suit a business protecting its data amongst multiple servers. As of now, the technology is not utilised as much as it could be, due to the high cost of setting it up as it requires multiple servers to distribute the data between. It is also significantly less efficient than typical security methods, due to classical methods typically requiring a single server with protection through firewalls and encryption. If blockchain were to be more easily accessible for business, it would pave way for a new form of security that would be far more secure than classic methods. Unfortunately, this technology would likely not be appropriate for personal security and networks, as most personal systems do not have a decentralized network to share the data between.

A Zero Trust security system method turns the traditional approach on its head. Traditionally, security models rely on verification, but trusting the user first. This is shorthanded to the term ‘trust but verify’ (Loten, 2019). A zero-trust model however does the opposite of this, initially not trusting the user, and requiring some form of verification before any access is available. This verification can be methods such as multi-factor or multi-step authentication, data encryption or endpoint security. This also means verification has to constantly happen to continue accessing data, unlike traditional models of security that require only initial verification. This ensures less access for data breachers and means only those with constant verification are able to access all the data. For businesses, this significantly reduces breaching capabilities and even users that have breached initial access, it will require a lot more effort to maintain access, allowing the server security more time to remove their access. This again has a lesser implication in personal security, however, could be set up if need be. Most personal systems require quick access to most data, and constant verification, if requiring user input, would be tiresome and significantly slow down the efficiency of the system. Zero trust security is likely to be more valuable to a business that needs to secure important and private data.

# **Bibliography**

IBM, 2021. *What is Blockchain Security?.* [Online]   
Available at: https://www.ibm.com/au-en/topics/blockchain-security  
[Accessed 14 September 2022].

Kangas, S., 2022. *Why AI is the key to cutting-edge cybersecurity.* [Online]   
Available at: https://www.weforum.org/agenda/2022/07/why-ai-is-the-key-to-cutting-edge-cybersecurity/  
[Accessed 12 September 2022].

Loten, A., 2019. *Akamai Bets on ‘Zero Trust’ Approach to Security.* New York City: The Wall Street Journal.

Ziomek, B., 2021. *Implementing AI security solutions: A crawl-before-you-run strategy.* [Online]   
Available at: https://www.securitymagazine.com/articles/96092-implementing-ai-security-solutions-a-crawl-before-you-run-strategy  
[Accessed 11 September 2022].