**IT Technologies (1200-word report)**

**Cybersecurity**

**What does it do?**

Cybersecurity is the utilisation of technology to protect and reduce the risk of unauthorised entry and exploitation of computer systems, programs, devices, networks, and data (IT Governance Ltd 2021). Cybersecurity is a rapidly growing field; in response to an increase in data breaches with 1,291 breaches in 2021, compared to 1,108 in 2020 (Morris 2021). IT professionals are constantly seeking new ways to deal with cyber-attacks, leading to the development and incorporation of state-of-the-art technologies, policies, and procedures. When referring to state-of the-art, people think of new and exciting technologies. However, in the case of cybersecurity, it also encompasses an overview of the best policies and procedures on security measures. VPNHaus (2019) claims that state-of-the-art in this field refers to the best performance of a subject available on the market to achieve an object. Therefore, the state-of-the-art of cybersecurity refers to the Cyber Security Guidelines within the Information Security Manual (ISM) which instructs organisations on how to best protect their data from cyber threats (Australian Cyber Security Centre 2021). These guidelines are comprehensive, including personnel security, physical security, governance, and Information and Communications technology security matters. Alongside these guidelines, machine learning technology, and cybersecurity simulation are also considered part of the state-of-the-art of cybersecurity.

Machine Learning is a sub-field of AI, Gottsegen (2019) states that machine learning utilises previous datasets and statistical analysis to create algorithms that can make assumptions related to a computer systems behaviour. This data is used to change its actions and can even perform functions it has not been programmed to. Machine learning is increasingly being used in cybersecurity due to its ability to identify potential hazardous files and sort through millions of files in a short period of time to uncover threats and automatically deal with them (Gottsegen 2019). Machine learning uses more statistical techniques as opposed to mathematical ones to find unhidden trends, incorporating the AI tool, this data can then be used to predict future patterns and the cyber threat landscape to prevent threats (Das 2021). With the development of AI and task automation through machine learning, the cybersecurity field has greatly benefited regarding automatic Penetration Testing and Threat Hunting, which frees up IT professionals to focus on more important tasks. Alongside machine learning is cybersecurity simulations, this refers to creating simulated environments in important areas such as representative environment building, tests, evaluations and explorations, risk analysis and assessments, and exploring humans to predict threats and learn the best way to deal with them (Kavak et al. 2021).

Cybersecurity simulations are advancing rapidly, in the next few years Kavak et al, (2021) predicts that there will be processes to establish data collection and access which will inform new models, utilising existing social theories to create new theoretical constructs specific to the field of cybersecurity. This will allow the use of psychology behavioural models to be used in cybersecurity as the means to develop sociotechnical solutions. Kavak et al. (2021) argues that these simulations should play a bigger role in the field as securing cyberspace requires not only great technical ability, but also behavioural insights. For the development of these new focused simulations to be viable, behavioural complexities need to be included in cyberattack simulations rather than just focusing on the cognitive approach that is currently used (Kavak et al. 2021). Incorporating psychologists as part of the multi-disciplinary team to study behavioural patterns during cyberattack simulations is a crucial part of this development happening. Utilising the previous mentioned simulations combined with machine learning and updated cybersecurity guidelines, the prevalence of large data breaches and other cyberattacks will be reduced and cause less overall damage.

**What is the likely impact?**

With the development of new theoretical constructs that use behavioural models in relation to cybersecurity simulations, existing cyber space defence mechanisms will be greatly improved. As stated by Mejia-Ricart (2019), this approach will aid in the early detection and prevention of cyber-attacks and assist in identifying potential adversaries and repeat offenders with similar modes of operating. The potential impact of this development will be a lowered prevalence of cyberattacks due to being more aware of potential offenders, allowing cybersecurity personnel to catch them before any real damage is wrought. Mejia-Ricart (2019) believe these behavioural studies will also allow for collaborative internet-wide security infrastructures through sharing of organisational security intel and improved system security automation, further improving cyber space defence mechanisms. This approach is similar in nature to criminal investigative analysis, otherwise known as “Profiling”, currently used by law enforcement to develop a description of an unknown offender (Bonn 2017). The methods used have seen great results in predicting future offenders, which is the premise for using it for cybersecurity. This will help keep people who are vulnerable to scams and those who struggle with using technology to keep their information and details safe. Utilising these behavioural models to update the algorithms of automated threat detection systems will be ground-breaking in the field. With machine learning being used to detect key behavioural patterns, IT professionals in the field will have more time for other important tasks. The combination of machine learning and focused simulations utilising behavioural models will reduce some cybersecurity jobs due to the automation of threat detection. However, IT staff will still need to check the validity of the profiles once they have been generated and decide on a course of action, so I believe some job roles will change but not many will be made redundant.

**How will this affect you?**

The previous mentioned developments will improve cyber space safety and allow everyone to feel more secure when using computer systems~~.~~ In my daily life, I will feel more confident knowing my personal details are protected and I can share photos and details with my family and friends overseas, via social media or email, without the worry that my details or photos will be stolen and used for nefarious purposes. Since technology is increasingly integrated into our daily lives and we are becoming more dependent on it, we are also more vulnerable and at risk of data breaches. The social impact of cyber-attacks may not be as apparent as the financial impact but can still cause lasting psychological damage. With these advancements in cyber security, I will feel more comfortable using the internet without concerns for my privacy or physical safety being threatened. After Sony’s last data breach, I stopped entering my credit card details online for worry that my hard-earned money could be stolen. Labrecque et al. (2021) found evidence that consumer decisions following a data breach are adversely affected and perceptions of affected organisations are changed after social contract violations, increasing stress and anxiety levels. I look forward to knowing cyber space is safe enough again so I can order games online with confidence that my details are secure and won’t be stolen. I believe that these developments in cybersecurity will not only affect me positively, but also my family and friends. It will mean my daughter can use the internet to contact her family overseas to build and maintain her own relationships with family without relying on me to do it for her, as I won’t need to worry about censoring the information she is sharing for fear that it can be breached and used against her.

**Reference List:**

Australian Cyber Security Centre 2021, *Cyber Security Guidelines,* Australian Government, Canberra, viewed 27 December 2021, <<https://www.cyber.gov.au/acsc/view-all-content/ism/cyber-security-guidelines>>.

Bonn, S-A 2017, ‘Criminal Profiling: The Original Mind Hunter’, *Psychology Today,* blog post, 4 December, viewed 28 December 2021, <<https://www.psychologytoday.com/au/blog/wicked-deeds/201712/criminal-profiling-the-original-mind-hunter>>.

Das, R 2021, *Practical AI for Cybersecurity,* Auerbach Publishers Incorporated, ProQuest Ebook Central database.

Gottsegen, G 2019, ‘Machine Learning Cybersecurity: How It Works and Companies to know’, *Built In,* 30 June, viewed 27 December 2021, <<https://builtin.com/artificial-intelligence/machine-learning-cybersecurity>>.

IT Governance 2021, *What is Cyber Security? Definition and Best Practices,* IT Governance Ltd, viewed 27 December 2021, <<https://www.itgovernance.co.uk/what-is-cybersecurity>>.

Kavak, H, Padilla, J-J, Vernon-Bido, D, Diallo, S-Y, Gore, R & Shetty, S 2021, ‘Simulation for cybersecurity: state of the art and future directions’, *Journal of Cybersecurity,* vol. 7, no. 1, pp. 1-10.

Labrecque, L-I, Markos, E, Swani, K & Peña, P 2021, ‘When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach’, *Journal of Business Research,* vol. 135, pp. 559-571.

Mejia-Ricart, L-F 2019, *Data-Driven Adversarial Behavior Models for Cybersecurity,* College of Charleston, ProQuest Ebook Central database.

Morris, C 2021, ‘The number of data breaches in 2021 has already surpassed last year’s total’, *Fortune,* viewed 27 December 2021, <<https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/>>.

VPNHaus 2019, ‘What “state of the art” means in IT security today’ *VPNHaus,* blog post, 13 February, viewed 27 December 2021, <<https://vpnhaus.ncp-e.com/2019/what-state-of-the-art-means-in-it-security-today/>>.