**What does it do?**

Cybersecurity as a definition is basically a routine of protecting different computers, mobile devices, networks, and data from malicious attacks. A few categories of cybersecurity includes network security which is securing a network from any intruders, application security which is making sure that software is free of threats, information security which is protecting the privacy of data and operational security which refers to permissions users have to access data and be stored and shared.

Currently the investment in more innovative cybersecurity methods are growing with the number of leaders spending more than 20% of their IT budgets on further progressing technology has doubled in the last 3 years. Overall, the basics of cybersecurity has increased with direct attacks down 11% and security breaches down 27%. However currently there are quite a few hidden threats that specifically target the weakest links in the supply chain that are hard to detect as well as the cost of staying ahead of attackers being unsustainable. Some of these investments also are failing which leads to these unsustainable costs as employees aren’t making sure to stay protected and securing their systems. Currently leading businesses are more cyber resilient and are able to detect and stop breaches quicker and easier than non-leaders.

There are a few current technologies that are currently implemented mostly in leading businesses and one of them is a Next Generation Firewall (NGFW). A NGFW is a more advanced version of a firewall as it is able to filter packets based on applications. They are able to use a signature based IPS to differentiate between safe and unsafe applications. They can do anything a normal firewall can do however they are able to block malware from entering a network which normal firewalls could never achieve making them a key addition that is low cost for businesses in order to defend networks.

Another technology that is used is Privileged Access Management (PAM). PAM is pretty much the strategies that are used to ensure control over privileged or elevated access and permissions for different users and systems on an IT environment. This will support an organisation in the sense that it will lower the surface so to speak of being attacked which may prevent or stop damage being dealt from an attack.

One final technology implemented is Security Orchestration Automation and Response (SOAR). SOAR is compatible software programs that allows an organisation to collect data about any threats to security and act on certain security events without the need for human assistance. SOAR is made up of three components, security orchestration, security automation and security response. Security orchestration is a method of connecting different tools for security and integrating disparate security systems. These systems may include scanners, end-user analytics, firewalls and intrusion detection and prevention systems. Security automation is the automatic control of security operations. Tasks done can include scanning for issues and searching through logs without human assistance. Finally, security response ensures that analysts are shown a view of results to plan, manage and monitor a threat once detected.

Soon in the future machine learning will be much more advanced to detect malicious attacks and vulnerabilities. Right now, the best out there is just better automation with a bit of prediction. Further into the future the use of artificial intelligence will allow businesses to predict things that it needs to. AI will ultimately be able to find out what areas in a security system need to be secured from vulnerabilities and be able to decide whether an application bares malicious ability and overall scan software and make very accurate decisions as how to proceed.

Korolov, M. (2020) Are You Getting Bang for Your Cybersecurity Budget Buck?, Data Center Knowledge. Available at: <https://www.datacenterknowledge.com/security/are-you-getting-bang-your-cybersecurity-budget-buck> (Accessed: 3 May 2021).A picture containing light

Description automatically generated

**What is the likely impact?**

The potential impact that artificial intelligence will have in general is quite monumental. As more AI strategies are developed to assist with security operations it is still not pure AI where it is able to reproduce cognitive abilities to automate tasks. But as this technology emerges it will allow us to defend security systems without the need for human intervention.

As the introduction of AI is implemented, we can keep up with the malicious “hackers” of today and ensure secure business information is not leaked out into society. AI based security systems will have up to date knowledge on different threats that will allow your enterprise to prepare for a certain type of attack more than others. AI will also eliminate quite a number of devices needing to be connected which may be prone to attack, shutting off an angle of attack.

However, with such pros there are also very large cons. Mainly the fact that since most attack vectors are blocked off, the only area to attack is the AI system itself. If an entity was to take control of an AI system and corrupt it, then it will be quite disastrous as security systems will be too reliant on machine learning and will have a hard time to repel such attacks that may follow. But there will be future cybersecurity personnel that will develop techniques to detect and stop AI corruption attacks.

A big point about AI based cybersecurity systems is that many cybersecurity jobs may be made redundant as now enterprises will be reliant on AI to make all the decisions and stop attacks. In contrast to this, many jobs that rely on maintaining the AI system and counteracting AI corruption attacks may be made as this system will be the highest priority in terms of cybersecurity.

A picture containing graphical user interface

Description automatically generated

IBM to set up AI CoE with GeM (2020). Available at: https://economictimes.indiatimes.com/tech/ites/ibm-to-set-up-ai-coe-with-gem/articleshow/78496891.cms?from=mdr (Accessed: 3 May 2021).

**How will this affect you?**

With the implementation of artificial intelligence in enterprises, a better sense of security for the data of people working with the company will be brought about. People need their personal information safe while working with a business and with the use of AI in cybersecurity, this will allow a safer community in terms of digital information. The rate of cyberattacks will definitely be on the lower end as malicious entities will be forced to use very advanced techniques and overall will need to think smarter. However, if they are able to control this AI this might spell disaster for us and may even affect friends and family if they are able to trace down your family members.

As our society is becoming more and more reliant on technology, we require cybersecurity to ensure that all our information is safe. The most average users of today use social media in their day to day lives and hand over their personal information to the likes of Google and other big organisations with the expectation of having enough security to defend against unauthorised users. Therefore, we will be introduced to new security applications that are more advanced and will affect us for the better. These applications should be able to protect us by detecting threats easier and deeply clean any malicious material. After these technological advancements we will be able to hopefully live in a safer digital world.

References

* What is Cyber Security? (2021). Available at: <https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security> (Accessed: 16 April 2021).
* What is a Next Generation Firewall? Learn about the differences between NGFW and traditional firewalls (2017). Available at: <https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls#:~:text=A%20next%20generation%20firewall%20(NGFW,intelligence%20from%20outside%20the%20firewall.%E2%80%9D> (Accessed: 17 April 2021).
* What is Privileged Access Management (PAM)? (2021). Available at: <https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam> (Accessed: 17 April 2021).
* What is Privileged Access Management? (2021). Available at: <https://www.onelogin.com/learn/privileged-access-management#:~:text=Privileged%20Access%20Management%20(PAM)%20refers,value%20targets%20for%20cyber%20criminals>. (Accessed: 17 April 2021).
* *What is SOAR (Security Orchestration, Automation and Response)? A definition from WhatIs.com* (2021). Available at: <https://searchsecurity.techtarget.com/definition/SOAR> (Accessed: 17 April 2021).
* (2021) Accenture.com. Available at: <https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf> (Accessed: 17 April 2021).
* Security, M. et al. (2021) What Is the Future of Cybersecurity? , Trustwave. Available at: <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/what-is-the-future-of-cybersecurity/> (Accessed: 17 April 2021).
* What is the future of cybersecurity? | TechRadar (2021). Available at: <https://www.techradar.com/au/news/what-is-the-future-of-cybersecurity> (Accessed: 17 April 2021).