cybersecurity

What does it do?

Recently, my Mum’s bank account was hacked. The company she shopped with did not have the right cybersecurity measures to keep her information safe and secure. My mum’s example illustrates how cybersecurity in a business – or more poignantly the lack of – can have a profound effect on the average person.

As our society becomes more and more dependent on computers and technology, the importance and need for cybersecurity has grown exponentially. Cybersecurity is such an essential piece of technology as a range of organisations including government, banks, medical facilities and companies (small and large) store an incredible amount of information. A significant portion of that information is extremely sensitive. Our society also has lots of specialty software and hardware that may not be available anywhere else in the world. Our dependent on computers and our advanced technology makes us a target for hackers and cybercriminals.

The absolute goal of cybersecurity is to prevent or limit the risk of a possible cyberattack. Cybersecurity must protect sensitive information from being accessed by unauthorised people, as well as protect other related vital pieces of IT. Without any form of cybersecurity, organisations and businesses will be left wide open for potential cyber-threats and cybercrime. In many countries, it is illegal for a large company to have no cybersecurity measures due to the large amounts of sensitive information they hold.

One of the major new technologies developed for cybersecurity is the use of Artificial Intelligence (AI). Cognitive computing, an advanced type of AI, is already being implemented worldwide by many cybersecurity firms. Cognitive computing uses many different types of AI technologies, such as machine-learning algorithms and deep learning networks, to analyse and learn from each threat it detects. This type of AI is an essential part of modern-day cybersecurity because it allows a better understanding of advanced threats and also enables a quicker and more decisive response to them.

The use of AI in cybersecurity allows IT professionals in the field to be more efficient. For example, experts may use AI to detect and gain information about each threat. The expert can then use the information to respond quickly and more appropriately to the threat. The AI acts like an advisor, of sorts, to the expert, effectively making the whole process quicker.

Technology grows at an extraordinary rate. Likewise, AI in cybersecurity is only going to become more prominent. In a survey conducted by the Capgemini Research Institute, 69% of organisations think AI is necessary to respond to cyber-attacks. And, three out of five firms said that using AI improves the accuracy and efficiency of cyber-analysts. This research supports the proposition that over the next few years, cybersecurity firms will continue implementing new forms of AI.

What can be done now?

Right now, there are many different ways to implement cybersecurity measures inside an organisation. These include; installing firewalls and implementation more encryption within the network. Businesses may hire cybersecurity experts and security analyst to help protect their assets against threats. Experts may seek and eliminate variabilities through such things as ethical hacking, or installing tools to monitor for intrusions, or indeed respond to security incidents. Cybersecurity experts are a vital part of the industry and any organisations, big or small, who are looking to protect themselves from cybercrime, should consider enlisting their aid.

What is the likely impact?

Cybersecurity allows organisations to protect their most valuable assets. Cyber-crime has a major impact on the world today, and the cybersecurity industry has created numerous employment opportunities in response. It is a multibillion-dollar industry with a market value of more than $120 billion. As we develop more technologies, such as cognitive computing, hardware authentication and user-behaviour analytics, the market value will increase. The industry predicts the value of the sector will to grow to $300 billion by 2024.

Experts have conflicting views on the impacts of AI technologies on employment in the field. AI technologies have already started to replace workers in many industries such as healthcare, pharmaceutical research, retail and marketing. Many experts fear that this could also happen in the field of cybersecurity. Some disagree. Aaron Levie, chief executive of cloud storage service ‘Vendor Box’ once said “If you want a job for the next few years, work in technology. If you want a job for life, work in cybersecurity”.

Tech enthusiasts and some cybersecurity specialists believe that advancements in AI for cybersecurity will not remove cybersecurity jobs, but it will drastically change them. In the not so distant future, we could see humans and AI working together to complement each other. An example of this would be AI responding to a malware attack, quickly researching characteristics of the malware and recommended a course of action. AI relieves the analysts from any time-consuming manual research. In theory, this will speed the process of responding to a threat dramatically, then making the analyst’s job more enjoyable. Experts already working will have to upgrade their skills to keep pace with these new technologies.

How will this affect you

A common misconception is that cybersecurity is something that only big organisations have to worry about. But in reality, cybersecurity has a profound effect on everyone who connected to the internet. As someone who likes to be protected when browsing online, these advancements in cybersecurity bring me peace of mind. We all must trust organisations with our private and sensitive data. It’s of utmost importance that they stay up to date with the current technologies to keep our information safe

Even though my family and friends do not know all that much about cybersecurity, the recent advancements are going to benefit them greatly. Now, and from here forth, anything is online. What happened to my Mum could happen to yours, or a small business, or a large corporation. Organisations need to invest in proper cybersecurity measures to protect themselves, their clients and our society.

Hashed Out by The SSL Store™. (2020). *Artificial intelligence in cyber security: The savior or enemy of your business? - Hashed Out by The SSL Store™*. [online] Available at: https://www.thesslstore.com/blog/artificial-intelligence-in-cyber-security-the-savior-or-enemy-of-your-business/ [Accessed 8 Jan. 2020].

SEEK. (2020). [online] Available at: https://www.seek.com.au/job/40673900?type=promoted#searchRequestToken=555cdc83-a9c5-495f-9ca4-a4c114bddefc [Accessed 8 Jan. 2020].

TechBeacon. (2020). *Top 5 emerging information security technologies*. [online] Available at: https://techbeacon.com/security/5-emerging-security-technologies-set-level-battlefield [Accessed 8 Jan. 2020].

Ecpi.edu. (2020). *How Cyber Attacks Affect Individuals and How You can Help Keep them Safe*. [online] Available at: https://www.ecpi.edu/blog/how-cyber-attacks-affect-individuals-and-how-you-can-help-keep-them-safe [Accessed 8 Jan. 2020].

Ibm.com. (2020). *Artificial Intelligence for Smarter Cybersecurity*. [online] Available at: https://www.ibm.com/au-en/security/artificial-intelligence [Accessed 8 Jan. 2020].

Laurence, A. (2020). *The Impact of Artificial Intelligence on Cyber Security*. [online] CPO Magazine. Available at: https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/ [Accessed 8 Jan. 2020].