# Cybersecurity

Cybersecurity is the act of securing digital data and computer systems. Cybersecurity is usually guided by three main factors - confidentially (secrecy), integrity and availability.

Confidentiality (secrecy) relates to the storage of sensitive information, such as personal information, payment details or any other sensitive data. Measures are taken to ensure information is stored securely and only viewable by authorized users or individuals. Malicious threats involve man-in-the-middle attacks, social engineering or access by unauthorized third parties.

Integrity involves ensuring only authorized people have rights to access, move, delete or modify data. Measures must be taken to ensure the users or individuals accessing the data are authorized and have the necessary rights to make such changes or view such information. Current technologies include the encryption of data during transit, use of user access controls and technologies such as checksums so end-users can check the integrity of the data received. Malicious threats involve the exploitation of invalid user permissions, avoiding of integrity checks (direct access) or use of another user’s information.

The last factor is Availability - being able to access the data you are authorized to access. In a general sense, availability is ensured through redundancy methods such as RAID arrays, failovers, etc. In a cyber security sense, threats such as distributed denial of service (DDoS) attacks must be considered.

In summary, cybersecurity is protecting sensitive digital information from cyberthreats and malicious attacks. Such threats take many forms, such as malware, ransomware, phishing, man-in-the-middle and DDoS attacks. Many state-of-the-art technologies are available today, each aiming to counter specific cyber security threats. Government agencies and private enterprises make use of all the latest technologies to ensure their systems remain secure.

Technologies such as virus scanners can be used to identify and eliminate malicious software and files before they even have a chance to execute. This in some cases can entirely prevent the destruction of data or compromising of a machine, if the data base of known viruses remains up-to-date. Maintaining virus databases is an on-going job, hackers with malicious intent are always designing new executables which virus scanners don’t yet detect. Some researchers have investigated using Deep learning to identify viruses, ensuring virus-scanner technology is always one step ahead. If successful, this would allow anti-virus creators to identify new threats before they’re even known or used maliciously, addressing the issue then.

Firewalls are a crucial technology to fight against cyberthreats this technology stops any threats from the internet trying to gain access to your local network . As mentioned previous DDoS are one such attack that a firewall can defend against by setting a Packet rate per Source maximum limit, this will monitor the source of the traffic in to your network and only allow that source to send at the rate you have set in turn stopping a source from sending to much traffic to your network and causing a DDoS attack.

With all these technologies available, the main current cyberthreat is humans. Social engineering is often used to manipulate or trick staff into giving access or providing information the individual isn’t entitled to. Technologies are slowly emerging which address this issue, such as end-to-end encryption, user-side encryption and full storage/data encryption. Such technologies ensure there’s no way for employees or third parties to access data. Even if an employee or staff member was tricked (or had malicious intent), they would not be able to decrypt or access the data without the end-user’s personal device or encryption key(s). Such technology is seen with Snapchat (where *my eyes only* memories are encrypted using a pin only the user knows) or WhatsApp (where messages are encrypted end-to-end – no server in-between can read them). Even with these technologies, human-error can still exist – if the WhatsApp user loses their phones, all the messages become available to a third party.

Deep learning will like to have huge as it will allow computer systems to protect themselves against cyberthreats without having to wait for the cybersecurity engineers to develop a patch for the vulnerability.

The changes this will have will be very impactful as it will remove the need for “zero day patches” and remove the need for a systems administrator to monitor that their security systems have to be always up-to-date. Deep Learning could even fix a flaw in a routers firewall as it would locate where the entry of the attack started and correct it.

A personal experience that I had was in 2016 when A client’s files maliciously encrypted. The attacker had encrypted the files and demanded payment for decryption (ransomware). With deep learning, this sort of action could have been detected before it happened. The original infecting file would have been detected as malicious and deleted, or the actions attempting to encrypt files would have been detected as unusual. Ultimately, this would have saved the client thousands in avoiding downtime and staffing costs in restoring from backups.

These new technologies have the potential of impacting the job market. As cybersecurity is moved towards machine-based deep learning, the need and demand for cyber security teams may fall. Cyber security experts may need to branch out into other areas of cybersecurity, such as operating, maintaining and securing the new deep learning machines. Further staffing may be required to assist in the production of algorithms, datasets and statistics for the machines. This may increase the job prospects for other IT experts.

On a personal level, these technologies help ensure my computer is secure and I remain secure online. This includes virus scanners alerting me of potential threats and encryption ensuring my personal data remains secure. In the future further technologies will assist in ensuring my computer remains protected to any new viruses or exploits which are discovered. My daily life will remain like it is now, though that’s just the point – the aim currently is to advance technologies in a way that stays one step ahead of individuals who have malicious intent.

For others less technology educated, advancements in virus scanning and security technologies may help in ensuring everyday users are better protected. This may involve more automated, simpler virus scanners, the default use of encryption on files and messages or other means of background security where minimal user input or response is required. Ultimately, this will further reduce the number of major incidents relating to malicious software, hacking or cyberattacks.

References :

<https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security>

<https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

<https://umbrella.cisco.com/blog/2013/10/08/top-ten-important-cyber-security-tips-users/>

<https://www.youtube.com/watch?v=bPVaOlJ6ln0>

<https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field>

<https://resources.infosecinstitute.com/artificial-intelligence-impact-cyber-security/>

<https://software.intel.com/en-us/articles/intel-processors-for-deep-learning-training>

https://towardsdatascience.com/decoding-deep-learning-a-big-lie-or-the-next-big-thing-b924298f26d4?gi=51389740879

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15\_0\_sy\_swcg/denial\_of\_service.pdf