Cybersecurity Report.

What is Cybersecurity

Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this (1). From this definition we can deduce that cybersecurity is not only just a technology it is both a practice and an end result. Without it, all of our data would be available to those who could exploit it for their own purpose.

Cyber criminals can achieve access to secured data with a variety of tools and techniques with some examples listed below:

- Brute forcing passwords with common password lists.
- Taking advantage of known exploits on unpatched systems.
- Social engineering. Tricking someone to give access or give up sensitive information.
- Using virus's.
- Building malware into websites.

Two points worth making here is that cyber criminals will usually implement a whole suite of tools to gain access to a target system, and that most attacks are opportunist based rather than with a specific target in mind. A good example of these points was the Wannacry ransomware attack in May 2017. It used a malware virus, or cryptoworm, to lock down a computer by encrypting important data on the infected machine. It then displayed a note demanding a bitcoin payment to release the encrypted files. It did this by using a range of tools and techniques.

Tools and techniques used by the Wanncry malware virus:

- The assumption that many computers had not implemented security patches on the Microsoft Windows OS.
- Use of the EternalBlue NSA exploit to gain access to these unprotected systems.
- Use of the DoublePulsar tool to load the Wannacry malware.
- Wannacry malware encrypts files and issues ransom.
- Virus then scans local and internet IP addresses to further infect machines.

Due to the fact patches were released by Microsoft before the exploit was weaponised (2), if good cybersecurity had been implemented then the Wannacry attack most likely would not have had a major impact.

Without cybersecurity, systems we would not otherwise consider important could be compromised leading to a countrywide shutdown of life enabling services such as health systems, electricity networks and water management. The attack highlighted flaws in software controlling these systems, showing cybersecurity was never initially implemented, or given a high priority (3). The lack of forethought for security in these systems made them vulnerable to attackers.

As Cybersecurity is both a practice and a result, various contexts of ‘State of the Art’ can exist. Due to this complexity, “State of the Art” could be described as anyone who has the most 0-day knowledge of exploits and potential fixes. This may be a single person in a garage somewhere or an online community that has shared its resources. The professional standard accepted by security specialists are state sponsored organisations who have pooled these types of people & resources together in a strategic deployment. This is done with the intent of having IT systems that are protected against these 0-day exploits and the ability to leverage their cutting edge knowledge against those who don’t.

There are various technological solutions available now to combat the threat posed to IT security. Common ones used by consumers being:

- Antivirus software.
- Passwords and user authentication software.
- 2FA, the use of two pieces of evidence to provide authorisation.
- HTTPS for website traffic encryption.

More professional examples used by Cybersecurity experts are:

- Kali Linux for penetration testing.
- Full disk encryption software.
- Encrypted VPN.
- User authenticated data storage systems, such as Objective.

This is a non-exhaustive list of IT security systems in use now but it does highlight that encryption is the key technology being used.

Future Technologies

A current and growing concern is the ability of quantum computers to drastically reduce the computational time required to crack current encryption technologies. Use of Public Key Infrastructure (PKI) is of particular worry. Due to this concern, institutions are preempting a possible onslaught of encryption breaking by creating quantum proof encryption. This is acheived by using algorithms that cannot be cracked by any type of computer (4).

Impacts.

A recent estimation for a viable quantum computer puts just the hardware at $10bn USD(5). This means the initial impact of quantum computing will be defined by those who can afford to use these systems and how they use them. If a quantum proof encryption algorithm cannot be found, or if it is found and not made publicly available, this may mean that where a once fair playing field of readily available encryption to all, possibly may only be broken by governments and those with the financial ability to access these quantum based systems.

In this scenario, legislation may be the only way to protect people's privacy rights online, rather than relying on software and hardware. Although, this will not prevent organisations from breaking laws, or governments creating laws to circumvent privacy based legislation (ie: USA patriot act).

It is difficult to predict the impact this will have on the general public. One certainty is that the country who leads the way in this new technology will be enabled with a key military and economic advantage over others. If this becomes China, it may tilt the global status quo in their favour (6).

With China already exerting their influence both politically and militarily, if they were also able to crack the encrypted transmissions between the USA and her allies during military operations, it would limit the capacity western allies could exert force in areas contested by China, such as the South China Sea and the greater Indo Pacific region. With China's greater influence in these regions it will be able to further interfere with political policy making ultimately flowing down and affecting the citizens of countries that exist in this region such as Australia, Indonesia, Papua New Guinea and more.

Although this example uses China as a scenario, it applies to any country that may wish to exert influence in another nation by utilising quantum computing to infiltrate that nation's encrypted networks.

I can see this as a potential threat to all Australian's way of life. Another nation with direct influence over Australian political, business and military could change the way we vote, what is available for us to buy on store shelves and even the freedoms that we all enjoy by living in this country.

Even with the future of quantum computing being uncertain, it will still significantly affect the field of Cybersecurity in the near term. It will require the field to be prepared for this potential threat to its existing defensive systems. In 2018 the USA government passed the National Quantum Initiative Act (NQIA) with the intent of accelerating quantum computing research and development, and the Quantum Computing Research Act which focuses on the Department of Defence (7). With these acts in place, cybersecurity professionals will likely be required at the forefront providing information and education to both defence and academia.

References

1. https://www.lexico.com/en/definition/cybersecurity
2. https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/
3. Weidlich, A. & Beenken, P. 2012, "Cybersecurity", *Hampton Roads International Security Quarterly,* , pp. 101.
4. https://www.forbes.com/sites/waynerash/2019/10/31/quantum-computing-poses-an-existential-security-threat-but-not-today/#1ff1107c5939
5. https://www.theguardian.com/technology/2019/aug/02/quantum-supremacy-computers
6. https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#38c01cd872de
7. https://www.hpcwire.com/2018/09/17/house-passes-1-275b-national-quantum-initiative/