JIN HONG, *Senior Lecturer, University of Western Australia*
https://research-repository.uwa.edu.au/en/persons/jin-hong

Dr. Hong has expertise in cybersecurity, particularly in the area of security modelling/analysis and moving target defence. For example, with collaborators, he developed security assessment solutions such as SafeLite and CloudSafe - which are patented. He continues to work closely with international collaborators from USA, NZ, Korea and Japan, as well as with the DST to develop future defence solutions.

TIP 1. KEEP YOUR SYSTEM UP TO DATE

Keeping your system up to date is the easiest and most effective way of improving your cybersecurity. You will most likely be using computers with pre-loaded OS (e.g., Windows, Linux, Android), kernels, bios etc., which have built-in protections that are updated regularly. For example, the heartbleed bug continued to be an issue for many; even though the fixed version was available on the day it was publicly disclosed.

TIP 2. CYBER SECURITY AWARENESS IS A MUST

Nowadays, everyone is a potentially vulnerable contact for hackers to approach. This could not only be via phishing emails, but it could also include:- malicious phone calls and texts, social media (luring messages and links) and various emerging social engineering methods. So, it is critical that all employees are made aware of the latest scams and hacks to ensure that they can identify them when approached, and do not become a victim.

TIP 3. KNOW YOUR SYSTEM AND ITS VULNERABILITIES

Understanding the vulnerabilities of your system is important in order to plan ahead, particularly on how to prioritise security options. With hundreds and thousands of vulnerabilities discoverable in a system, it requires an in-depth security assessment to fully understand which threats are most critical. This way, you can optimise your return on investment and prevent critical threats before they can happen.

TIP 4. HAVE A BACKUP PLAN

Cyber attacks can happen anytime and anywhere, so it is critical to have backup plans. For example, you should consider both online (e.g. cloud) and offline (e.g. hard drives) backups for all your data. Also, think about the services you are providing (e.g. would they still function under a DDoS [Distributed Denial Of Service] attack?). The continuation of service may be more important - depending on the services you provide - which may be achieved using redundancy techniques such as scaling via the cloud to handle growing or decreasing demands.

TIP 5. ROUTINELY CHECK YOUR CYBER SECURITY

Ensure that all your security mechanisms and protocols are properly implemented and working. As systems evolve over time, some security mechanisms may not function as expected due to various reasons (e.g., requirement changes, inefficient coverage). Also, people may not continue to follow security protocols strictly as time passes. So, it is recommended to have regular checks in place to ensure that all the cyber security mechanisms and protocols meet expectations.

TIP 6. ACCESS CONTROL

Control who can access what information. It is not uncommon to see workplaces where employees are requesting and sharing confidential data that they normally do not have access to. So, the way the data can be accessed needs to be secured and all users made aware of the potential consequences. Further, do not place all data on the same database/computer to avoid the possibility of a single point of failure.

TIP 7. FIND GOOD PENETRATION TESTERS

Security is expensive; but only because the return on investment is usually not directly visible. Another way of thinking about this is to assess the potential cost of damage in case of a cyber attack and compare that to the cost of a penetration testing service. Employing highly skilled and experienced penetration testers will ensure detection of a wide range of potential cyber attacks that others may oversee. And do it as regularly as possible.

TIP 8. KEEP UP TO DATE WITH THE LATEST TECHNOLOGIES

Technologies change fast, as do the way hackers use them to advance their attacks. So, keep up to date as to how new technologies can disrupt cyber security operations (e.g., most encryption standards, such as standard RSA, would become obsolete when quantum computing becomes available). Looking up the latest research trends in cyber security would also give you an advantage to see new solutions coming in the next few years.

TIP 9. CLOUD – A DOUBLED EDGED SWORD

The use of cloud computing has revolutionised the way businesses operate. Although cloud computing technology has matured, ill-configured clouds, or malicious cloud service providers, can still significantly impact cyber security. For example, threats such as side-channel attacks are still significant in the cloud. So, whenever outsourcing resources (e.g. in the cloud), be sure to regularly check the security posture -and have a swift plan ready in case something goes wrong.

TIP 10. INVEST IN CYBER SECURITY EDUCATION

Upskilling existing (and future) employees can improve their general cyber security knowledge and conduct, reducing the "human vulnerability" factor. This can be done in the form of enrolling existing employees to cyber security courses (micro-credentials etc.), collaborating in joint cyber security projects with tertiary and defence institutes, and just taking an interest in how future cyber security graduates are made.