CYBER ATTACKS:
Staying ahead of the bad guys

By
BENEDICT TAN
Chief Information Officer, SingHealth

With the number of cyberattacks increasing, it might seem like one's turn is next. While no one can be 100 per cent attack-proof, there are precautions and measures that individuals and organisations can and should take.

Cyberspace lies at the heart of today's society. It impacts our personal lives, businesses and government.

Unfortunately, cyber risks are also a reality of this environment. Cyberattacks can range from installing spyware on a PC to attempts to cripple an organisation, and even destroy the infrastructure of an entire nation.

Organisations and individuals cannot afford to ignore these cyber threats. Knowing what we are up against will be a good start.

The attacks can range from simple email spoofing to phishing and all kinds of malware. The most recent attacks have been "ransomware" where hackers break into a system to lock up and encrypt the data files and then demand a payment (usually money or bitcoins) to restore the system and data files. [Ed: see page xx for a list of the common attacks.]

Without doubt, most organisations would have put in place measures to deal with cybersecurity. With the increasing pace and complexity of attacks, whether this is enough is the question. The range

of measures that an organisation should adopt to counter cyberattacks is provided in the next two pages, "Defending the organisation".

However, cyber defence is everyone's responsibility. All staff should be educated with real life examples and made aware of how they can play their role in cyber defence. This would include reminding them to:

- Create strong passwords and remember them (not stick them besides the computer). See box on "The importance of passwords".
- Never give or share their passwords.
- Not open any attachments or click on any links in emails from someone whom they are unfamiliar with. When in doubt, they should check with their IT colleagues. With internet shopping and purchase getting more and more popular, cyber criminals are riding on this trend to send unsuspecting cyber shoppers phishing emails, luring them to a site on the pretext of checking their delivery.
- Be careful of "odd" emails. For example, a common scam is an email from a known party (whose email id was hacked into or is being spoofed) asking for a small sum of money for an emergency – call back the sender and check (do not respond via email).
- Backup their data and files regularly to an offline storage. (The only way to recover from a ransomware attack is to pay the ransom or to restore the locked files from a backup copy).
- Install appropriate anti-malware and do not delay security updates.

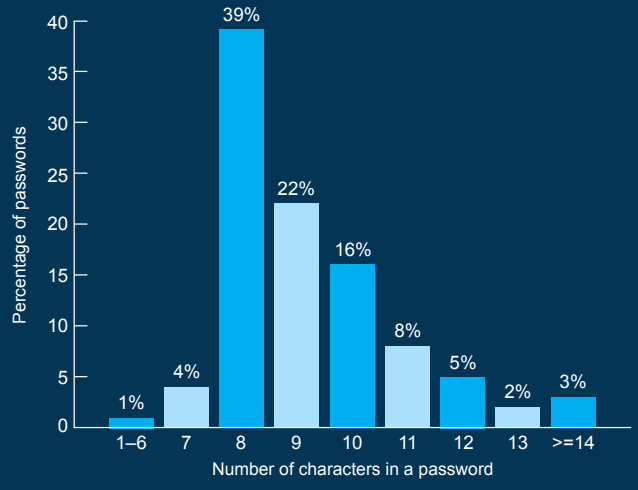
THE IMPORTANCE OF PASSWORDS

The use of common and weak passwords is a major reason for successful cyber attacks. A 2015 study by Trustwave Global Security found that after sampling 500,000 hashed passwords gathered through thousands of penetration tests, an astonishing 51 per cent of them could be cracked within 24 hours and 88 per cent within two weeks.

The top ten commonly-used passwords were found to be:

1. Password1
2. Welcome1
3. P@ssword
4. Summer1!
5. Password
6. Fa$hion1
7. Hello123
8. Welcome123
9. 123456q@
10. P@ssword1

The common password lengths



Here are three tips on having a strong password:

- The longer the password, the harder it is to crack. Consider a 12-character password or longer.
- Avoid any dictionary word, names and places. Any word on its own is bad. Even combinations of known words should be avoided.
- Mix it all up. Use variations of upper and lower case letters, numbers and letters, punctuation marks and symbols.

DEFENDING THE ORGANISATION

1. Secure the borders

If the organisational network has connections to the internet, the following should be installed:

- **Firewall.** This is the wall around the cyber perimeter. Incoming and outgoing traffic are monitored and permitted ones (based on predetermined rules) can only travel through doors, called ports.
- **Intrusion detection and prevention system.** This is like the border guards monitoring traffic that passes through the ports to identify malicious activity and attempt to block it.
- **Web proxy.** A proxy acts as an intermediary for all communication between an organisation and the internet universe. It protects the organisation by substituting the internet address of the organisation with a pseudo address when communicating with external entities in the internet. Without the actual address, cyber criminals will be more challenged to locate the organisation.
- **Anti-spam.** This software scans through all messages coming in to your organisation's email server and block spam messages from coming through. They usually deposit these blocked emails into a spam folder where the intended recipients can occasionally check if legitimate emails that should not have been but are also blocked. Typically, more than 98 per cent of the emails an organisation received are spams.

Some organisations segregate their internet access and enterprise networks. For example, IDA recently announced that there will be no internet access for public officers' work computers by June 2017. This is arguably the most secure measure against external cyber-attacks. However, organisations contemplating this approach will have the weigh the benefits of this added security against any potential drop in productivity and additional infrastructure costs (for example, issuing staff with more than one device, and having a separate network for internet access).

2. Tighten security within borders

The internal network and software should be kept secure and robust through measures such as:

- **Install Network Access Control (NAC).** With NAC, unauthorised devices will be disallowed from connecting to the internal network, even if they use a valid User ID. This prevents cyber criminals who managed to gain physical access into the premises to access computer resources and data assets through the network, as well as malicious software which can be introduced through an unauthorised endpoint (for example, inadvertently or otherwise being brought in by a staff).
- **Keep enterprise software up-to-date.** Major vendors such as Microsoft and Apple release patches regularly to remediate detected vulnerabilities in their software.

- **Regularly review and audit user ids, access levels and actual accesses.** Put in place a process to regularly review user ids. Remove those that are dormant or belong to departed employees. Ensure that staff are given the right access levels to do their work, not any higher. Finally, audit actual accesses to identify any unusual activities.

3. Protect the endpoints

Despite all the protection at the border, cyber perpetrators will always find a way to get through. Thus, the organisation needs to shore up defenses at the end-points, i.e. the devices such as notebooks, desktop computers and tablets. These include:

- **Install anti-virus software in all the endpoints.** These software detect viruses through the viruses' signature that are stored in a signature file. Companies that supply the anti-virus software update the signature file regularly with new virus signatures. Hence it is important that the IT Department keep these files updated in all the end-points. There are advanced forms of malwares knows as "Advanced Persistent Threats", which will require the installation of Advanced Threat Protection software to detect and neutralise them.
- **Control administrator rights.** Most malwares require "administrator rights" to embed itself in the end-points and to conduct their malicious work. Administrator rights allow unfettered access all system folders and files; this is not needed by all staff. By limiting the number of user ids with administrator rights, the organisation effectively limits the number of vulnerable end-points.
- **Implement a regular password change policy.** Every user without exception should be required to change their passwords, ideally every three months. Passwords should be required to comprise special characters and numbers to make it difficult to hack.
- **Encrypt all endpoints hard disks.** That way, the information stored on the disk will be safe even if the endpoint is hacked into.
- **Limit endpoint connections.** Many organisations disable the endpoints' USB ports and allow only authorised USB devices to be connected. This is to prevent malwares being introduced into the organisation through USB storage devices.

4. Prepare for breach

Despite the best of precautions, the ingenuity and persistence of cyber attackers should never be underestimated. The organisation should put in place resources and processes to control the damage and recover from an attack. These should include:

- **Contact points.** There should be one or more contact point for staffs to report and seek help if their devices are compromised. This can be the IT helpdesk line.
- **A recovery team.** There should be trained personnel in place that can be mobilised to immediately respond to the attack. The response would usually involve isolating the infected device, and investigations to determine the route of penetration. Vulnerabilities must be remediated promptly. For example, if the attack was through an email, all emails from the same source should be quarantined.
- **Incident escalation and management.** Depending on the type and extent of the breach, several of the organisation's resources will need to be mobilised to contain the breach and handle public communications. Establishing an incident escalation and management procedure will avoid confusion and provide a structured approach to manage any breaches. ■