CYBERSECURITY- A REAL AND CONSTANT LOOMING THREAT

18 JANUARY 2021

NAQIZ & PARTNERS

CLIENT ALERT: CYBERSECURITY - A REAL AND CONSTANT LOOMING THREAT

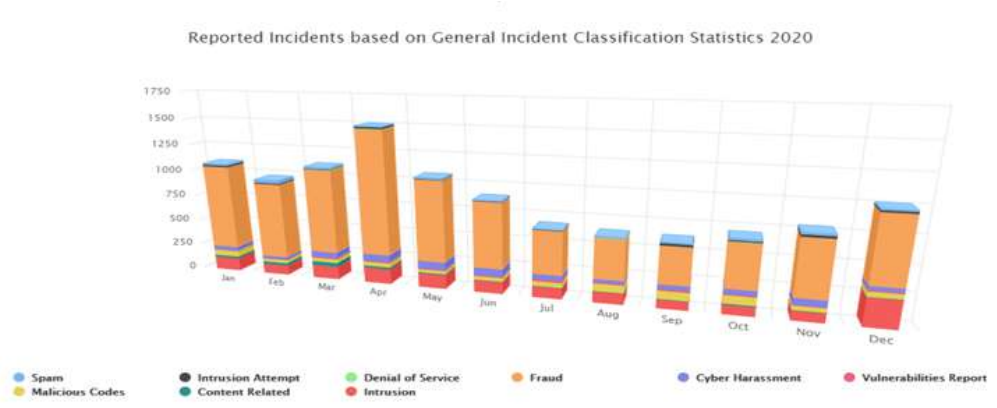
Author: Lo Khai Yi
(khaiyi@naqiz.com)

In this age of information, gone are the days when people only pay attention to financial and physical security. Cybersecurity is the new table talk topic, along with COVID-19 and WFH. So, what exactly is cybersecurity? Think of it as measures to protect digital information or data from unauthorised access or use.

Cybersecurity has become increasingly important as we are more and more reliant on technology in our daily lives. According to a survey by the Department of Statistics Malaysia in 2019, 91% of Malaysian household has access to smartphones, 72.1% has access to computer and 84.2% has access to internet. The undeniable fact is that information and communication technology have fully integrated into our lives.

The next thing we know, our personal data, sensitive information (credit card information, bank account details, identification number, health information) and corporate data (client information, trade secrets, intellectual property) are scattered across the cyberspace, in the cloud, data storage facilities and even our IT devices. This translates to cybersecurity threats as cyber attackers now have myriad of targets to lay their hands on.

The COVID-19 pandemic brought more than just new norms. It ushered in the work-from-home movement and increased reliance on cloud technology, along with rise in number of cyber-attacks. Cyber attackers made use of this perfect opportunity to target hospitals with less-than-ideal cybersecurity and infect the hospitals' IT infrastructure with ransomware, demanding payment in exchange for decryption. In addition to this, as we moved from our office environment to home working environment, it also creates more avenue for cyberattacks.



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	11	27	14	8	13	8	6	7	8	16	16	11	145
Intrusion Attempt	13	8	8	11	4	1	2	4	20	14	17	14	116
Denial of Service	0	1	3	7	1	0	0	1	0	2	1	0	16
Fraud	807	725	798	1,180	770	626	413	378	351	411	526	608	7,593
Cyber Harassment	37	27	58	65	73	69	48	32	40	50	60	37	596
Vulnerabilities Report	5	7	10	10	7	11	18	9	18	10	5	7	117
Malicious Codes	56	32	33	40	35	36	47	72	76	75	40	51	593
Content Related	23	23	42	23	9	7	7	6	7	11	7	5	170
Intrusion	122	93	125	144	133	113	101	102	81	87	88	255	1,444
	1,074	943	1,091	1,488	1,045	871	642	611	601	676	760	988	10,790

According to the cyber incidents statistics maintained by the Malaysia Computer Emergency Response Team (MyCERT), there has been a 69% increase in the number of reported cyber incidents from 2019 to 2020 in Malaysia, the year where most of us were forced to work from home.

A major contributing factor is that our IT devices and networking infrastructure are simply less secured at home than when they are in office.

WHAT CAN WE LEARN FROM THE SOLARWINDS' COMPROMISE, BREACH OF PARLER, AS WELL AS THE INSURRECTION AT THE US CAPITOL

There are of course many different ways and measures that you can put in place to ramp up cybersecurity. In this article, we are going to focus on 3 recent cybersecurity incidents as case studies on how you can enhance and strengthen your personal and enterprise cybersecurity, followed by some general tips and consideration.

Let us first look at what happened during these 3 cybersecurity incidents:

- The compromise of SolarWinds

SolarWinds is the developer of a network management software named Orion that is widely used in the US. It was confirmed in December 2020 that Orion became the target of a supply chain attack and through it, cyber attackers gained access to the network of Orion's nearly 18,000 users, including the US Treasury, Commerce and Homeland Security Department.

A supply chain attack is where the cyber attackers mount the cyberattack not directly against the victims, but rather through the victims' supplier, and in this case, through SolarWinds being the supplier of Orion. A supply chain attack is usually harder to detect by the victims themselves because customers would generally be more trusting towards their suppliers and would typically rely on the suppliers to ensure the integrity of their products.

Researchers and analysts traced the breach of Orion to as early as March 2020, albeit the breach was only detected recently in December 2020.

- Insurrection at the US Capitol

On 6 January 2021, pro-Trump rioters broke into the US Capitol and had unprecedented physical access to congressional data and devices. During the rush in evacuation, some congressional staff had left their computers unlocked and there have also been reports on loss of equipment after the insurrection.

The event has left the congressional support staff struggling to ascertain whether there has been any actual leak of national information or breach of the Capitol's cybersecurity and to what extent. There are real and irrefutable risks of congress offices being bugged and IT equipment being tampered with, since rioters had access to congress offices without any surveillance. The rule of thumb is always to assume that where there is a physical breach of space, there will always be digital compromise.

- The breach of Parler

Parler is a social media platform that promotes free speech. Following the insurrection at the US Capitol, Parler was shut down for being used as a tool to plan and coordinate the insurrection. Before the shutdown however, hackers had allegedly downloaded 99% of Parler's data.

The hack was possible because of an alleged security vulnerability in Parler's authentication system.

So, what are the practical steps that you can take to strengthen your cybersecurity?

1. Companies and enterprises should at least come up with some policies or guidelines on cybersecurity, especially now that most of us are working from home. These policies or guidelines should ideally include the following:

- Personnel's access right to company data, IT equipment and infrastructure – it is recommended that company adopts the "least privilege" concept to restrict employees' access to resources that are only absolutely required to perform routine and legitimate activities. It would be a cybersecurity nightmare if any Tom, Dick and Harry are allowed unrestricted access to IT equipment and infrastructure as demonstrated in the Capitol insurrection when rioters actually had access to congressional IT devices and equipment;
- Never leave your IT equipment unattended or unlocked – employers should stress the importance of employees locking their computers or laptops when left unattended. A locked laptop definitely decreases the risk of cybersecurity breaches even if the laptop is stolen. Understandably that the congressional staff may not have been able to do so under the panic to evacuate the Capitol building, but again, it should not have taken one more than few seconds to lock their computers;
- Incident reporting – a clear incident reporting protocol is crucial for early detection of cybersecurity breaches;
- Emergency or disaster recovery / response protocol – companies should always have a clear set of directions to manoeuvre through a cyberattack or any form of digital compromise.

2. Avoid using oversimplistic password – Now that SolarWinds' cybersecurity is under scrutiny, a security researcher has disclosed that at one point SolarWinds was even using a weak password "SOLARWINDS123" in respect of its update server.

We often compromise our cybersecurity for the sake of convenience without fully understanding what is at stake. Companies should also consider implementing multi-factor authentication system in respect of applications or equipment that provide access to more valuable or sensitive data. When dealing with sensitive and valuable data, company can also consider put in place encryption technology. "Remember password" function should also be discouraged, especially when employees are logging onto company's information system using personal devices.

3. Periodic malware and virus screening – SolarWinds' Orion was allegedly infested as early as March 2020. The breach was however only detected sometime around December 2020, and what is worse is that it was detected not by SolarWinds, but one of its customers who is also affected by the breach.

For early detection of malware or virus infection, company should consider carrying out periodic screening of its IT equipment and infrastructure or at least subscribe to decent anti-virus software which will provide basic virus scanning. If necessary, the option of penetration testing is also available to flesh out vulnerabilities in a company's cybersecurity.

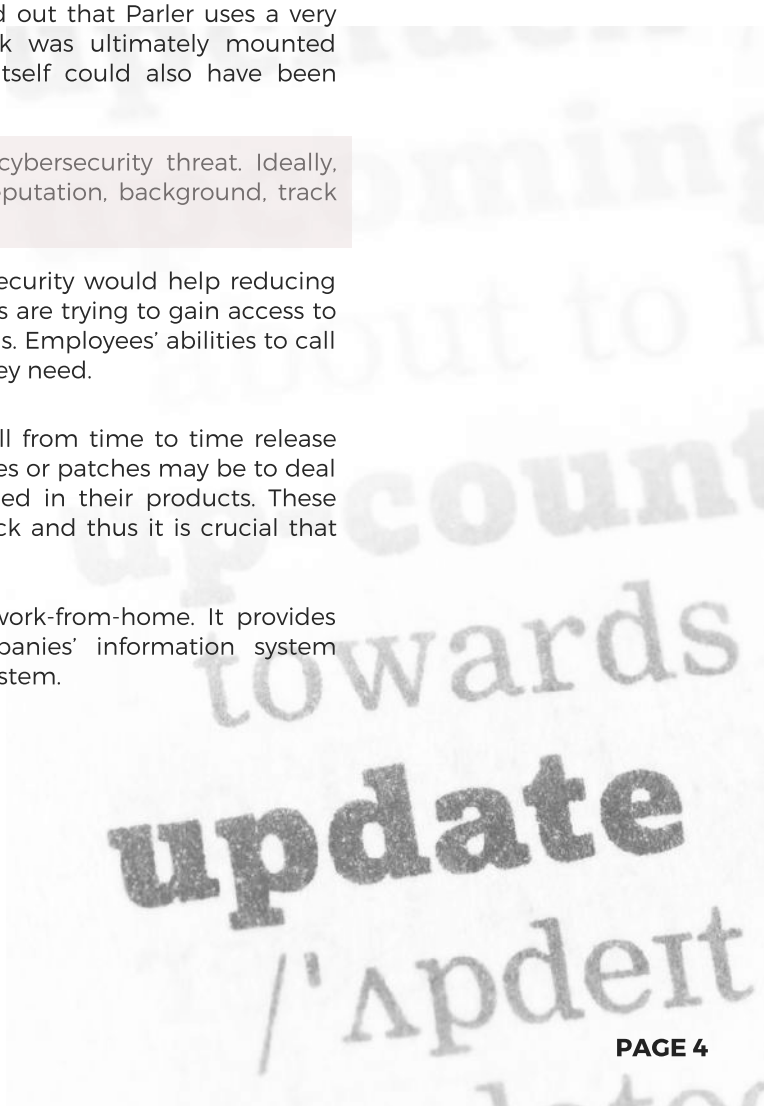
4. Encourage use of secure, accredited and approved software or applications – Users of Parler would not have imagined that their personal information would fall into the hands of hackers through their use of the platform. A security researcher has pointed out that Parler uses a very basic and vulnerable programming language. Although the hack was ultimately mounted through other security vulnerability, the programming language itself could also have been exploited by cyber attackers.

A little due diligence goes a long way in avoiding the pitfall of cybersecurity threat. Ideally, company should only employ software or application with good reputation, background, track record and relevant accreditation.

5. Education – providing employees with basic education on cybersecurity would help reducing risk of cyber threats. This is especially so when a lot of cyber attackers are trying to gain access to corporate information or corporate's network through phishing emails. Employees' abilities to call out suspicious email is key to denying cyber attackers the foothold they need.

6. Prompt update of system and software – software companies will from time to time release new updates and/or patches for their products. Some of these updates or patches may be to deal with or patched up existing vulnerabilities that have been identified in their products. These updates and patches could help to prevent possible zero-days attack and thus it is crucial that users update their software promptly.

7. Use of Virtual Private Networks (VPN) – VPN is helpful during work-from-home. It provides encrypted internet traffic when employees are accessing companies' information system remotely, either through public Wi-Fi network or home networking system.



MALAYSIAN LEGISLATIONS ON CYBERSECURITY

Unfortunately, Malaysia does not have a one-stop legislation that deals with cybersecurity. At the present moment, regulation on cybersecurity is rather fragmented and is being dealt with by various pieces of law. Some of the key legislations are highlighted below.

- Computer Crimes Act 1997

Under the Computer Crimes Act 1997 ("CCA"), unauthorised access to computer, unauthorised modification of the contents of any computer and unauthorised communications of number, code, password or other means of access to a computer would constitute punishable offences. In other words, cyberattacks such as hacking and spreading of malware are prohibited in Malaysia pursuant to the CCA and offenders are punishable with fine, imprisonment or both on conviction.

- Communications and Multimedia Act 1998

A person would be committing an offence under the Communications and Multimedia Act 1998 ("CMA") if he or she initiates a communication using any applications service with the intent to annoy, abuse, threaten or harass any person. A denial-of-service attack or even infection of IT system with ransomware would most likely be caught under this particular provision of the CMA and punishable on conviction with fine, imprisonment or both.

- Personal Data Protection Act 2010

Pursuant to the Security Principle set out under the Personal Data Protection Act 2010 ("PDPA"), a data user is obligated to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The Personal Data Protection Commissioner has also issued the Personal Data Protection Regulation 2013 and the Personal Data Protection Standard 2015 which set out specific requirement regarding the security standard of a data user.

At present, it is unclear if and when the Malaysian Parliament will enact a single piece of legislation that deals with cybersecurity. As cyber threats continue to be on rampage, and as we continue to grow ever more dependent on technology, we do believe that a cybersecurity law is ever more crucial now than ever.

"the rule of thumb is to assume that where there is a physical breach of space, there will always be digital compromise"

NAQIZ & PARTNERS

Suite 9B.02, Level 10,
Wisma E&C,
Lorong Dungun Kiri,
50490 Damansara Heights,
Kuala Lumpur

+603 2095 1188
www.naqiz.com