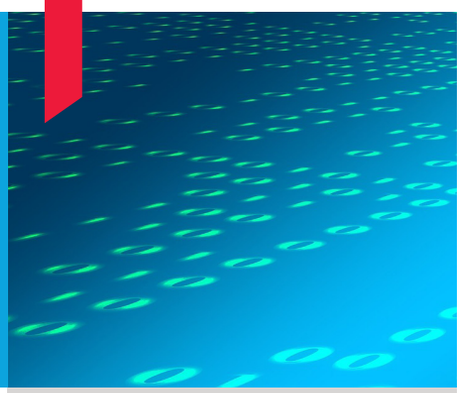
The 12 Observations of Cybersecurity Incidents in 2018

December 2018



It is the time of the year with Christmas carols playing around the clock on the radio, businesses are gearing up for the year-end shopping craze, and it is also the time to reflect on some of the cyber incidents and lessons learnt in 2018.

The BDO cybersecurity team has reviewed a number of cybersecurity incidents, both local and around the region, and made the following 12 observations taken from engaging our customers and the cybersecurity industry partners and associations. We want to take this opportunity to thank our clients and partners for their support this year and share this opinion piece.

1. Internet Separation or Operational Disruption?

Some organisations have been observed to take a hard stand to keep some parts of the business operations segregated and separated without any access to the internet. This tough stance has been chosen for reasons like due to a data breach incident to protect critical data and systems from external, or even from insider cyber threats.

However, these organisations have wreaked havoc on their business operations by taking this tough stance without careful consideration of the impact to the daily operations (which is exactly what the hackers had wanted to do). Some ingenious employees might even decide to circumvent the obstacles by using their mobile device to access the internet in continuation of the daily operation. Unfortunately, this could have created another attack surface area "that is" not monitored "or one that is" with limited or no control over by the IT security team.

2. Patches to death

At a critical business operations phase where a failure of IT systems could be disastrous or when threatened by cyber hackers, some organisations may take on a "patch-at-costs" approach. The risks could be elevated with many disparate applications, systems and platforms running together in the same breath. This is further exacerbated when ad-hoc patching is done outside the scheduled maintenance period, with insufficient time, without adequate testing of the proposed patches or the policies and procedures are not duly followed. System outages could easily occur when patches are rushed and not done in accordance following the pre-requisites and processes.

As a result, a perceived threat to the IT systems becomes a material threat causing unwarranted system downtime and outages. One of the main cyber risks is to try to treat all potential risks, and this is an illustration where such an action can become counter-productive.

3. Latest and greatest technology for use

Organisations are constantly reviewing their security posture, and in particular, after a serious cybersecurity incident, an organisation might attempt to mend the "broken fence" and as a result, falls prey to cyber marketecture pitch by a plethora of vendors. While a market leading solution comes highly recommended with many

At BDO, we have the expertise and experience in a range of cybersecurity services and solutions. Please feel free to contact us and let us know how we can assist you.

FOR MORE INFORMATION

CECIL SU
Director, Technology Risk Advisory
+65 6829 9628
cecilsu@bdo.com.sg

GERALD TANG
Business Development Lead - Cybersecurity
+65 6828 9167
geraldtang@bdo.com.sg

www.bdo.com.sg

industries leading accolades, it might not serve the purpose and intent as well due to some unique environmental set up within the organisation. As an example, many ICS/ SCADA/OT systems are of proprietary design running hardened and older versions of operating systems in the production or factory floor. It might not be a good idea to introduce the new tech toy that constantly requires a connection to the cloud running periodically to poll for the latest online updates and breaks the air-gap existence of the CPE systems.

This might introduce new cyber threats and expose the proprietary systems to new and unknown cyber threats into the air-gap systems.

4. BIG data comes with bigger data privacy responsibility

The industry 4.0 economy is no doubt data-driven, and with the advent of cloud adoption, data analytics tools and platforms that made the FANG team (Facebook, Amazon, Netflix, Google) the unrivalled data analytics leaders. Their services are now available to many through a simple cloud service subscription. From online shopping or movie downloads recommendation to ride-sharing applications, these magical platforms seems to know what the shopper is looking for before any search even begins. All this "magic" comes from crunching enormous chunks of data sourced from social media, online searches, and even communication chats between individuals.

However, the EU General Data Protection Regulation (GDPR) and many other regional and local privacy laws have made it clear any organisation that collects data from individuals must be explicit in explaining the purpose of the data collection and use and due consent must be obtained at the point of collecting the data. This makes the magical recommendation with trawling lots of data collected from the individual comes with added data privacy responsibilities that many organisations are not aware or not ready to undertake.

5. Digital Transformation into Cloud Nine

In the past year, there have been concerted efforts put together by government and cloud service providers to help small and medium enterprises (SMEs) to move to the cloud to leverage on the agility and innovations available on cloud platforms to pursue digital transformation. While cloud service providers have generally made the cloud platforms better secured and more resilient than what enterprises are doing in their own backyard, it is important to understand one of the key tenets in business/ IT outsourcing – Segregation of Duties. Depending on the cloud platforms and the native services an enterprise engages, an enterprise is generally responsible for the data and/ or application onboarded to the cloud.

Having moved the application and data to the cloud generally puts the enterprise in a better position with additional security protections undertaken by the cloud service provider – patches, endpoints, backups, monitoring and alerts. However, an enterprise has to take ownership of data protection, and the security posture and hygiene in the cloud has to be reviewed and be audited with the same rigour as with on-premise deployments in the data centre (DC).

6. Security with Obscurity

On the contrary, there are still out there business owners who feel they are the little-known companies of no interests to cyber hackers out there. Some even felt this way because their systems and processes are outdated and more analogue than digital, they are well secured with the obscure mindset.

Old Microsoft Windows operating systems, in particular, running unpatched and unprotected is a time-bomb; Microsoft no longer maintains and release patches for this end-of-life (and therefore, end of support) operating systems.

Even systems that run in an air-gap environment, cyber hackers still manage to get to these systems and exploit them as we have seen in data breaches occurring in the healthcare industry.

In addition, cyber hackers today are very much aware that the SMEs providing services in the supply chain and connected to large enterprises are easier targets for their penetration and entry. It does make perfect sense for large enterprises to review their external outsourced party policy engagement to have some form of checks and balances on these parties to exercise their due diligence.

7. Zero-trust, Zero-touch and Zero-understanding

In a recent review of the data protection policy of an enterprise performing helpdesk and repair services for mobile handsets, it had put in place a policy to erase all customer's data on the handset when it was brought to them for repair. With a zero-trust and zero-touch data privacy policy to completely wipe any data in the handset upon receiving it, the enterprise ensures the organisation and its employee are not duly held responsible for any data collection and management responsibilities on the device. It is noted that customers are expected to have their data on the handset regularly backed up so the data can be restored onto the repaired handset later on.

The approach taken is to fix the basics, protect the organisation first for what matters for the business and be ready to detect and respond. The enterprise has done well in handling customer's data under its data privacy policy, but not so when it comes to business services excellence and customer experience. This may have resulted in dissatisfaction and unhappiness for some customers who might not have the data backed up and will lose all the data after the repairs been completed. This zero-understanding and appreciation of customer's plight might not go down well with the end-users and may possibly lose some customers due to the approach taken by the enterprise.

8. A chain is as strong as the weakest link

In reviewing any cybersecurity incidents relating to data breaches, the two key causal factors that often pop up are:

- Systems misconfigurations or technical foul-ups
- End-user lack of awareness or slip-ups

For the IT systems, an enterprise has better control and could put in place security policies, processes and people to safeguard and protect these systems. On the other hand, end-users are harder to control and easy targets by cyber hackers. With the prevalence of BYOD (Bring Your Own Devices .. some says Bring Your Own Demise) allowed in enterprises, a large percentage of these devices are unmanaged and can access corporate data like emails and file storage. This presents an increasing are of attack for potential cyber hackers to exploit.

If an enterprise wants to enhance the security posture and build up a cyber responsible culture, it should avoid straining the staff to respect complex security tasks. The suggested approach is to teach them to be vigilant and provide an open feedback channel to notify and alert any anomalies.

9. Keep only what is necessary and required. Less is more

In today's data-driven economy, enterprises through omnichannel touchpoints with their customers, collect lots of data and do many experimentations running digital marketing campaigns to influence them. With PDPA, GDPR and various regional and local data privacy laws coming into force, enterprises should exercise caution and collect sufficient data only for the intended use and purpose; less is more.

In the widely publicised Google shutting down of it's Google+ social-media platform after failing to disclose user data leak, Google was fortunate to have only collected and used data what it deemed necessary for Google's social media platform less any Personal Identifiable Information (PII). In the USA, no federal law obliges Google to disclose data leaks, but there are laws at a US state (local) level to do so. In California, where Google is headquartered, companies are only required to disclose a data leak if it includes both an individual's name and their Social Security number, ID card or driver's license number, license plate, medical information or health insurance information.

If the data collected had leaked out personal data, and if the incident had not been disclosed to the authorities, there could possibly be more serious repercussions and backlash from the authorities.

10. What you don't know will not hurt you .. or will it?

Cybersecurity defences, in general, is to protect against current and foreseeable future cyber threats. It is hard to defend against any threats that you are not aware of and not knowing if you are being targeted.

In the past year or so, we are beginning to see many new cybersecurity start-ups offering Threat Intelligence Services (TIS), gathered from Surface Web, Deep Web and Dark Web. The idea is to help enterprises, or even individuals, to do a landscape scan using pertinent data relating to the enterprise to ascertain if they are under the crosshairs of any cyber hacker groups. Some of these enterprising start-ups even offer a take-down service for a fee to mitigate and remove the cyber threat.

It is prudent to reviewing and monitoring any threats received but not be over-prescriptive. An enterprise should have an established threat model to help review any vulnerabilities and threats received and deciding to respond to the threat(s) in question.

11. IoT – Internet of Things OR Internet of Threats

IoT devices have weaved into today's connected world evolved into a huge industry. However, with this evolution of IT coming on mainstream, it brings along with security vulnerabilities and considerations that need to be understood if the technology is to be harnessed effectively. Manufacturers, retailers and big businesses are all finding ways to leverage IoT platforms, combining the data that they collect with analytics and advanced reporting systems. Innovation, interconnectedness and cybersecurity by design, are key enablers to drive the value of IoT ecosystem.

"How many IoT devices exist in our own connected world today, with how many computing devices do they share data with? How many others have access to that data and what decisions are being made with this data?"

These are some of the questions we will not know but will pose as a serious threat to our connected world. On October 12, 2016, a massive distributed denial of service (DDoS) attack left much of the internet inaccessible on the U.S. east coast. The attack, which authorities initially feared was the work of a hostile nation-state, was, in fact, the work of the Mirai botnet. It's a story of unintended consequences and unexpected security threats, and it says a lot about our modern age.

Given that IoT devices are purpose-built (meaning they have a very narrow set of functions), communications outside the standard set of communications should be monitored and IT professionals should be quick to investigate communications to devices they don't normally see on their network. Network traffic analytics is well suited to address these types of attacks, but network and security professionals need to work together to mitigate the threats after it has been identified. Finally, organisations should audit the IoT devices on their network to ensure that default

passwords have been changed and have been deployed with as few privileges as required.

12. Does an enterprise need cyber insurance?

Complete cyberattack prevention is a fallacy. An organisation's cybersecurity team cannot completely and comprehensively secure misconfiguration, shadow IT, third parties, human error and rogue employee effectively. Apart from these insider threats, the everchanging external threat landscape in our connected world generates many more risks and threats beyond what enterprises can manage.

"It is not a question of if, but when?", industry experts and analysts have often cited this statement in discussing cyber attacks. Businesses large and small have been and will continue to be attacked. Cyber attacks are costly. The loss of data and confidential information leading to business disruption and regulatory violations, will not only cost the enterprise huge sums of fines but more importantly the loss of consumer trust and loyalty because of tarnished reputations and ligitations.

Enterprise can look at cyber insurance as an added layer of protection. Cyber insurance packages available today helps an enterprise to mitigate losses when a cyber attack occurs and provides protection from the costs associated with:

- Data theft
- Ransom and extortion
- Hacking
- Denial of Service attacks
- Crisis management
- Legal claims and remediation services

Cybersecurity insurance does not replace an enterprise's cybersecurity best practices. However, it can help to provide more peace of mind, and for some, it could help with the restoration of business-critical services. While it may not be possible to be fully prepared for a breach, an enterprise can take steps to alleviate some of the risk involved with purchasing cyber insurance as an additional layer of defence.

As a reminder to our clients and partners, all of us need to continuously review our cybersecurity hygiene, posture and improve any gaps in the policies, processes and even the people. We are always ready and able to offer our expertise and advice to help you to stay assured and secured.

www.bdo.com.sg