Data breaches and identity theft through hacking:

The impact and best practices to meet today's challenges

Singtel

CONTENTS

EXECUTIVE SUMMARY

The cyber security industry is expanding rapidly. But alongside the constant evolution and addition of security solutions and defence specialists, cyberattacks, data breaches and hackers also seem to be more prevalent with each passing year. More malware is being launched on a daily basis. In 2017, 360,000 new malware samples were detected daily.

Even as companies and governments invest in and deploy more resources to counter cybercrime, attackers always seem to be one step ahead.

Ginni Rometty, Chairman, President and CEO of IBM, said, "Cybercrime is the greatest threat to every company in the world." It is estimated that by 2020, the average cost of a data breach will exceed $150 million.

Clearly, no organisation today can afford to ignore the very real threat of data breaches, which result in more than just a loss of data. They also harm the reputation and financial standing of a company, and could endanger the personal information of those affected by the breach.

While there are different ways in which a data breach can occur, this paper discusses how hacking – a deliberate attack on company networks to steal data for financial gain – is one of the leading causes of such breaches today. This paper will also identify the types of data that are likely to be compromised and the fallout from such hacking attempts.

We end with some recommended best practices around safeguarding networks and assets, and mitigation measures in the event of a data breach.

THE MECHANICS: HOW DATA BREACHES AND IDENTITY THEFT OCCUR

Cybercrime is like the many-headed hydra. Even as you are protecting your company against one form of attack, two new attacks rear their heads. Cyber security teams have to stay vigilant and up to date on the latest methods used by hackers to prevent data breaches and identity theft.

Data breaches can happen in a number of ways. Surprisingly, many are the result of an oversight or negligence by the staff. Employees either accidentally send out an email containing confidential information, or leave a work computer with confidential data lying unattended in a public place. They may also conduct transactions on unsecured websites, access company resources using unsecured WiFi connections, or click on malicious links.

Hacking: The most common cause of data breaches

When it comes to deliberate data breaches, one of the most common causes is hacking – the unlawful access of information belonging to an individual or corporation. Cybercriminals carry out attacks through:

Phishing: sending emails purporting to be from an organisation that you would ordinarily trust, to trick you into submitting your personal information

Pharming: redirecting you away from the original website to a fraudulent one

Malware: tricking you into downloading malicious software that attacks and hacks into your computer

Hackers are also known to exploit network vulnerabilities. An example would be using password-cracking software to override weak passwords to gain access to systems.

The proliferation of social media accounts and online activity has made it even easier for miscreants to access personal information. Individuals share all kinds of information online – from check-in locations and important dates to personal information about themselves, their children and their pets. Hackers are nothing if not creative – the *Ocean's 11* of cybercrime, if you will. They piece together such publicly available information from a variety of sources and use this to decipher user credentials. This makes it easy for hackers to access individuals' accounts and steal data.

What is the hacker after?

A hacker’s main objective is identity theft – to access and use personal data, without consent. They seek to gain entry to:

- Personally identifiable information (PII), such as national identification or social security numbers (NRIC in the case of Singapore), phone numbers and addresses
- Financial information, specifically relating to assets, credit or bank accounts
- Credentials used to access different accounts and portals
- Health records

They then use this data, especially PII, for financial gain – for example, to demand ransom, make money by selling it to marketing firms, or impersonate the user to apply for and benefit from a loan.

The compromise of user credentials – information that verifies a person is who they claim to be – can be hugely problematic. Equipped with usernames and passwords, hackers can infiltrate users’ online profiles and shopping accounts and steal credit card information, for instance. They can even access their email and social media accounts to perpetrate phishing attacks on others.

The damage of a data breach to companies

The compromise of corporate user credentials can have grave implications for an organisation. These credentials can be used to hack into corporate networks to steal intellectual property, as well as employee and customer information.

If the breach exposes all of a company's customer information, it can damage its reputation and result in a financial loss for the company and its customers.

We have seen a number of high-profile cases of corporate data breaches and identity theft over the years – the most recent one being the Facebook data breach that had affected 29 million users at the time of writing.

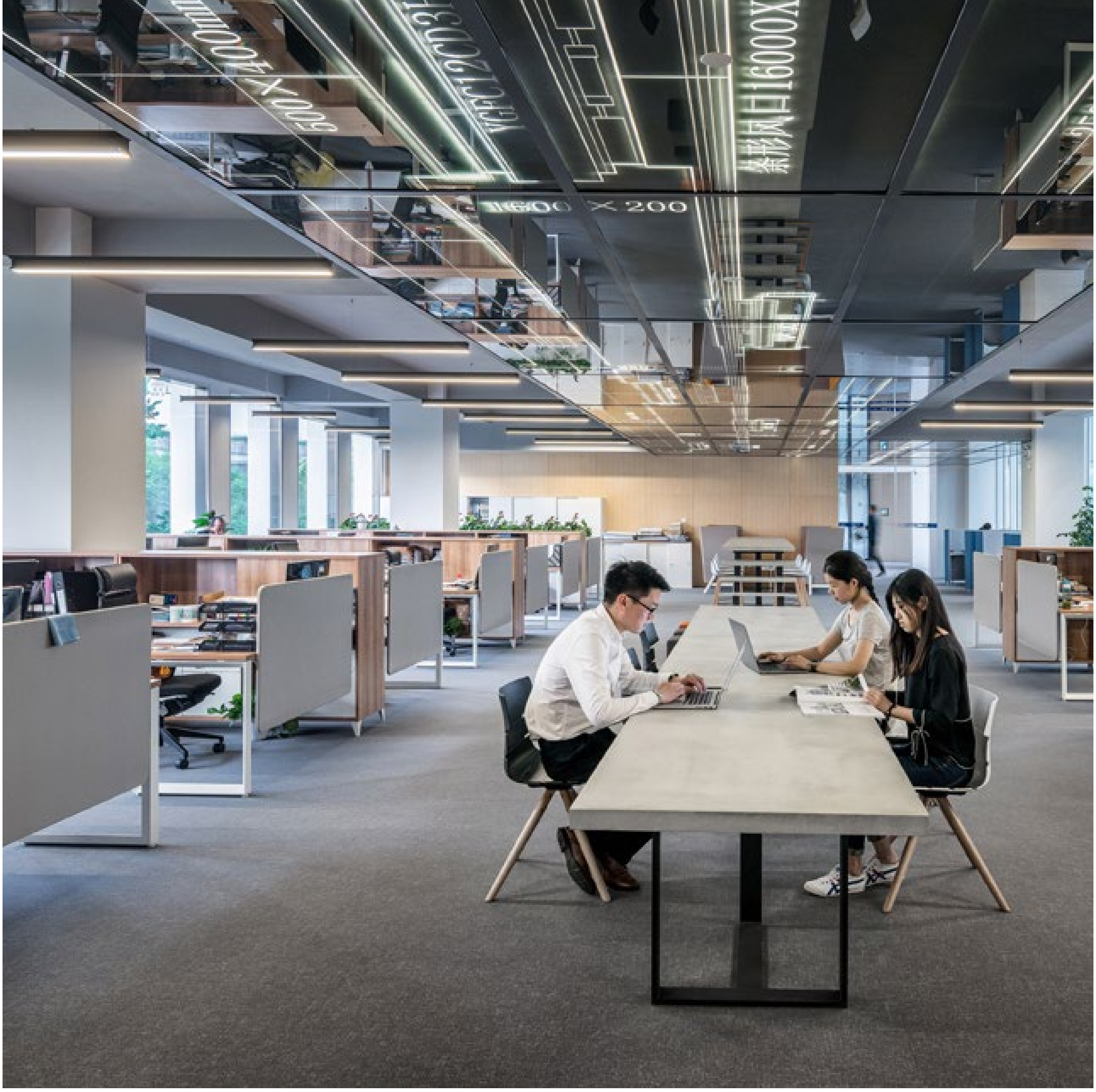
Gemalto's 2017 Breach Level Index showed that in the first half of 2017, the world saw 918 breaches. This compromised 1.9 billion data records, of which 74% were for identity theft, more than any other type of data breach.

ASEAN seems to be a hotbed of cybercrime. The region is seeing increasing mobile penetration and digital adoption, but lacks cyber security infrastructure. According to the Asia Pacific Risk Centre, hackers are 80% more likely to attack organisations in Asia for this very reason. Regulation around data security is also weak in many countries.

In recent years, Asian countries have seen a high number of data breaches, resulting in massive identity theft *(see box for examples)*.

High-Profile Data Breaches In Asia

- **2016, Philippines:** In the "biggest government data breach in history", the database of the Commission on Elections was hacked and the data of 55 million voters compromised when it was posted online.
- **2017, Malaysia:** The personal data of more than 46 million subscribers were stolen from the Malaysian Communications and Multimedia Commission and leaked onto the dark web.
- **2018, Thailand:** The identity documents of 45,000 customers of True Corp, the country's second-largest mobile operator, were compromised.
- **2018, Singapore:** The island nation faced one of its worst cyberattacks when the non-medical personal data of 1.5 million patients was stolen from SingHealth's database. Prior to this, the personal data of 5,400 customers of AXA insurance was stolen in a data breach. Soon after, Uber admitted that data belonging to 380,000 of its customers in Singapore had been leaked.



HOW COMPANIES CAN SAFEGUARD THEMSELVES: BEST PRACTICES

With security incidents and data breaches increasing annually, companies must thwart hacking attempts by implementing solutions and best practices that safeguard their networks and data.

Defining an organisational security policy

The first step is to have a well-defined data security policy in place. By detailing how data should be managed and handled, a security policy ensures that every employee is aware of best practices, guidelines and measures to be taken. Some mandatory aspects of a security policy include:

Encryption policy: Encrypting all organisational data and emails can reduce the risk of compromise even if data is exposed during a breach

Acceptable use policy: Given that every employee spends time on non-work-related websites, from social media platforms to entertainment and ecommerce sites, it is essential to have guidelines around what can be accessed from a work computer and what kinds of behaviour and data sharing are permissible. For instance, it is never acceptable to use the office computer to access pornographic material or sites that incite religious violence

Password policy: This is probably the most important policy to formulate and enforce. Passwords are widely used to access all kinds of accounts and resources, and are still the first line of defence against hacking. Implement strong password policies detailing best practices, such as combining numeric and alpha-numeric characters or having longer passwords. In fact, accessing company networks or resources using random algorithm-generated passwords comes high up on password security checklists. Additionally, all internal systems should be programmed to reject weak passwords or repeated passwords across different systems

Email policy: Guidelines explaining the types of information that can be shared via email, especially around PII or other customer data, should be established

Device policy: Vulnerabilities are often introduced into the company network through the personal devices employees bring into the workplace or when they access company data via an unsecured public network. Ensure you have a strict device policy that monitors how personal devices connect to the network and what safeguards they have in place. Additionally, any company device that is used outside of the workplace should be protected by a virtual private network (VPN)

Having a security policy in place is just the beginning. Its implementation and enforcement – through appropriate systems and a team to oversee it – is the other piece of the puzzle.

Implementing cyber security best practices and solutions

At the implementation level, there are many solutions and best practices that a company must consider to improve its overall cyber security posture.

Ensure that all software and browsers are regularly updated with security patches

Implement the necessary firewalls that deny access to websites that potentially pose security threats

Monitor and control user access rights. Limiting access to critical resources will limit potential data leaks

All business computers, systems and networks should use the latest security monitoring software. Installing built-in privacy and compliance tools will form a strong line of defence against hacking, thereby helping your company monitor, secure and protect its assets. These sophisticated solutions are helpful in:

- Getting real-time protection against advanced malicious attacks
- Protecting critical information
- Identifying users and managing their access levels
- Managing personal and company-issued devices when accessing company data
- Preventing targeted cyberattacks

Creating a cyber security SWAT team

Organise an expert response team comprising forensic security experts and legal, IT, HR and communications personnel. The team will be responsible for managing the aftermath of a data breach. Equipped with detailed guidelines and documented steps around the response to a cyber security incident, the team can act quickly and seamlessly to minimise the fallout. The response plan should typically define the roles and responsibilities of each member, who the decision-maker is, communication and notification flows, and steps to be taken to resolve the issue.

A study by Ponemon Institute states that having an incident response plan in place decreases the average cost per lost record by $14 from $148, which can translate to a lot of money when you are working with millions of records.

This is not a one-time practice. Review and revise security policies several times a year and update them as needed. This should be complemented by round-the-clock monitoring.

Do you employ hackers?

Many companies employ whitehat or ethical hackers, who are paid by the company to hack into their networks and systems. This allows the company to test for vulnerabilities within its IT system, and fix them before the real hackers necessitate it!

MANAGING STAKEHOLDERS: EDUCATING AND BUILDING AWARENESS

A company can have the best solutions and policies in place. However, all these efforts are wasted if customers and employees remain unaware of their existence or if they continue engaging in risky behaviour. More often than not, data breaches are caused by human error. It is, therefore, essential to complement operational efforts with educational and awareness-building initiatives for both customers and employees.

Training them on best practices around cyber security is as important as the fire drills that companies conduct every quarter – both ensure safety and well being.

Building awareness among customers

Customer awareness is critical if you run an ecommerce site or if your customers need to access your online systems using unique user credentials. Any interface that requires a customer to sign in and conduct transactions is at risk of being hacked. Ensure that your customers are well aware of security best practices on accessing their data online.

Create awareness around the PII that you store and let customers know that this is of critical importance and cannot be compromised

Teach customers how to identify phishing emails and unsecured websites

Raise awareness about the kinds of information they should avoid sharing on social media and other digital channels to avoid compromising their PII

Train them on password security protocols and encourage them to follow best practices for the user credentials they set up on your site

A one-time awareness or training effort is insufficient.Communicate regularly with customers, reiterating the importance of such measures and keeping them informed of what you are doing to better secure their data. This will also enhance customer trust.

Educating employees

Employees are even more critical to your data security initiatives. Raise awareness across the organisation on security best practices with a well-planned programme that covers everything mentioned above. Here are some additional steps to take.

Provide structured employee training on using the security tools and solutions that the company has implemented. Employees should be fully aware of how all systems and protocols work, as well as how to handle and protect sensitive data

Educate employees on the risks of using personal devices to access company networks and data, and set guidelines around such usage

Encourage employees to use strong and unique passwords across different social media accounts. Suggest that they use different passwords for personal and official email accounts

Be transparent with employees about the kind of PII that the company stores. Once they understand how critical this information is, they will be more motivated to take precautionary measures

Emphasise the need to immediately inform the IT security department in case of suspicious events or activities

Again, since building awareness cannot be a one-time initiative, it is recommended that companies send out regular internal emails with security tips reiterating best practices, and communicate any changes or updates to security policies and protocols.

MITIGATION IN THE AFTERMATH OF A DATA BREACH

Hackers are persistent and creative. Sometimes, despite your best precautions, data breaches will still occur. In fact, companies have a one in four chance of experiencing a data breach.

The average cost of a data breach was $3.62 million in 2017. The longer a breach goes undetected, the more loss it incurs. Clearly, this is not something to be taken lightly.

In the previous section, we outlined measures that companies can take to prevent data breaches through hacking. But if a breach occurs, you must know what to do next and how best to mitigate the fallout.

Essential steps to take after a data breach

First, conduct a thorough analysis of the data breach to get a complete picture of how much and what kind of data has been compromised. A full analysis will also indicate what kind of repair work is needed – these should be long-term solutions. While it may be tempting to work on a quick patch to get your systems up and running, this may open the door to more such incidents in the future

Once the data loss has been stemmed, review all your policies, infrastructure and systems to identify further potential vulnerabilities and fix them. Change and update all user passwords and access codes

Report the data breach to law enforcement authorities and regulatory bodies

Communicating the security incident – and its extent – to employees, customers, investors and business partners is vital to maintain goodwill. Be proactive in communicating the details and your plan to mitigate the fallout

CHECKLIST

As we've seen, the damaging after-effects of a data breach are massive. Here's a quick checklist of the actions to take to prevent it or, if the inevitable occurs, to limit the damage at your organisation:

- ✓ Define your organisation's security policy by setting up an encryption system as well as password, email and device policies
- ✓ Monitor, update and implement necessary security patches regularly
- ✓ Limit user access to important documents and systems to reduce the chances of a breach
- ✓ Create a key security committee from the HR, IT, Legal, and Communications departments to react immediately after a breach occurs
- ✓ Educate your employees through regular training and emails on security-related tips and tricks
- ✓ Encourage your customers to follow best practices in their online transactions and behaviours

STAYING VIGILANT AND BEING PREPARED

A data breach resulting from hacking is a very real threat and cannot be ignored. To beat hackers at their game, companies have to think of creative ways to stay safe. Ironically, only 38% of global organisations are prepared to handle a sophisticated cyberattack.

This is where Singtel can help. As a Microsoft Office 365 gold partner, our Security and Compliance Solutions help companies secure, protect and control their assets while ensuring regulatory compliance. Additionally, Singtel can organise workshops for your organisation, help assess your security infrastructure, and identify gaps and vulnerabilities before implementing right-fit solutions, including end-user training.

Contact us now to see how we can work together to improve your cyber security posture and defeat the many-headed cyber hydra.

Singtel

For more information on Data Security and Compliance:

https://mybusiness.singtel.com/catalogue/office-365-security-and-compliance

buysaas@singtel.com