ISCA Legal Clinic – Cyber Risks and Civil Liabilities

Jonathan Kok | 23 July 2020

withers KhattarWong LLP

Introduction

Withers KhattarWong LLP is amongst the largest international law firm in Singapore. We are fully integrated global law firm with lawyers located across five continents in 17 offices.

Our broad global platform allows us to guide clients through the legal challenges inherent in the ever-changing international landscape. As our client, you will receive quality advice on diverse legal and tax issues through the services of one law firm with a single communication.

Internationally, we have made a reputation for ourselves as the leading law firm for private capital; our clients include public and private companies founded by successful families, MNCs, financial institutions, international brands, family offices and HNWIs, charities and not-for-profit organisations, amongst others. We pride ourselves for our role in helping our clients achieve success.

We provide market leading advice in the following areas:

- corporate
- dispute resolution
- banking & finance
- technology
- property & real estate
- tax
- mergers and acquisitions
- project finance
- capital markets
- employment
- structuring
- intellectual property
- insolvency
- funds
- sports
- family

The LEGAL 500 ASIA PACIFIC TOP TIER 2020

TOP RANKED Chambers ASIA PACIFIC 2020 Withers

TOP RANKED Chambers HNW 2019 Withers LLP

asialaw PROFILES

1974

Firm founded

180+

People

30+

Partners

Top 10

Largest law firm in Singapore (ALB, 2019)

Key Legislations on Cybersecurity

Cybersecurity Act 2018 (No. 9 of 2018) - creates a framework for *the protection of designated critical information infrastructure* (CII) against cybersecurity threats and authorises the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore; it also establishes a licensing framework for providers of licensable cybersecurity services in Singapore, such as managed security operations centre monitoring services and penetration testing services.

Computer Misuse Act (Cap 50A) (CMA) - *criminalises certain cyber activities*, such as hacking, denial-of-service attacks, infection of computer systems with malware, the possession or use of hardware, software or other tools to commit offences under the CMA, and other acts preparatory to or in furtherance of the commission of any offence under the CMA.

Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA) - imposes certain *obligations on organisations to make 'reasonable security arrangements'* to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks with respect to personal data held or processed by those organisations (Protection Obligation).

Protection Obligation under the PDPA

Section 24 PDPA An organisation shall protect personal data in its possession or under its control by making *reasonable security arrangements* to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Section 51(5) PDPA An organisation or person that commits an offence under subsection (3)(b) or (c) is liable —

(a) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and

(b) in any other case, to a fine not exceeding $100,000.

Section 56 PDPA Any person guilty of an offence under this Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part thereof during which the offence continues after conviction.

Guidelines on Data Protection

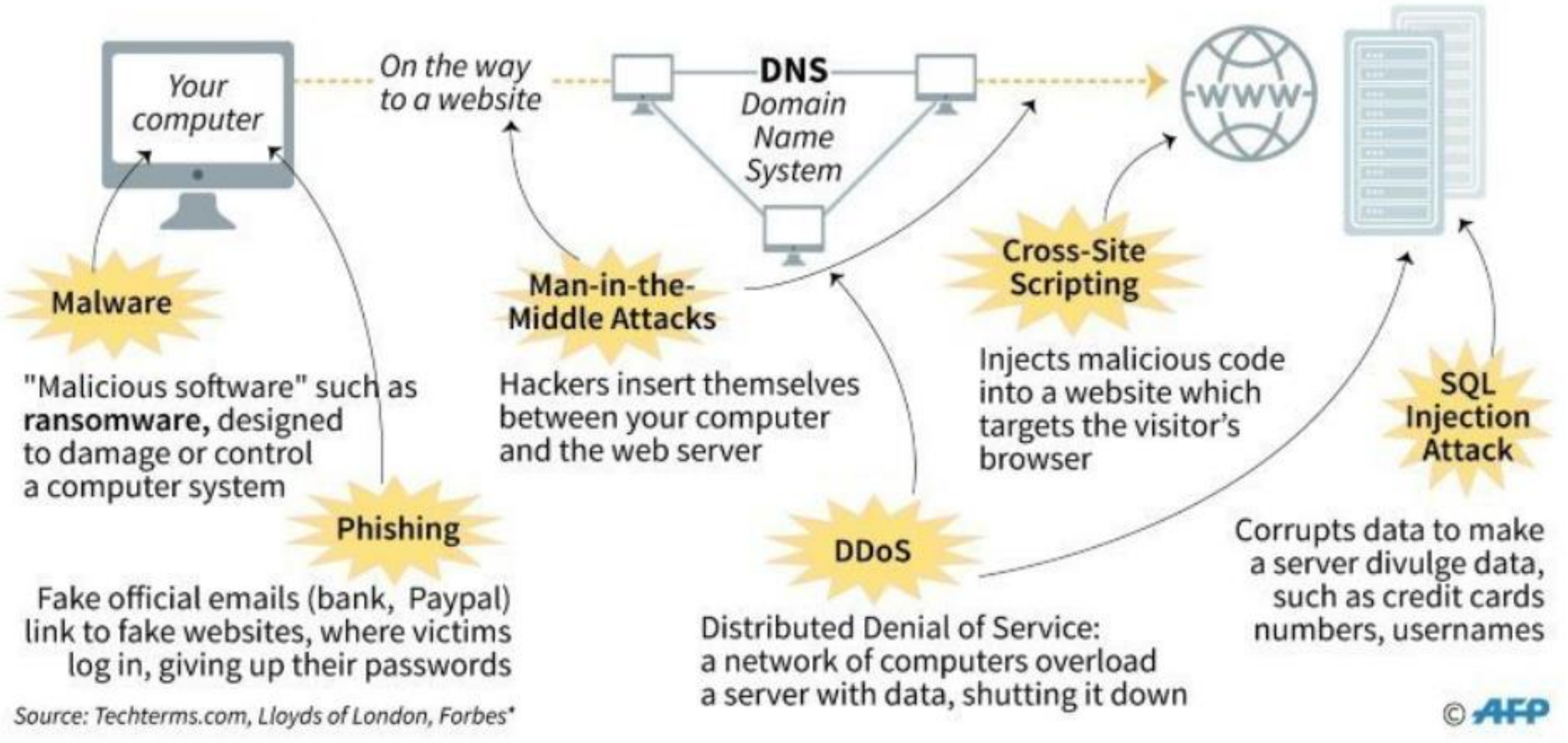
The Personal Data Protection Commission (PDPC) is responsible for the administration and enforcement of the PDPA and has issued general guides which, while not legally binding, provide greater clarity on the Protection Obligation and the types of ‘reasonable security arrangements’ that can be adopted in the protection of personal data that is in its possession or under its control. These general guides include:

- Guide to Data Protection by Design for ICT Systems (Design for ICT Systems Guide);
- Guide to Securing Personal Data in Electronic Medium (Securing Personal Data Guide); and
- Guide on Building Websites for SMEs;
- Guide to Managing Data Breaches 2.0 (Data Breach Guide).

Organisations in the telecoms, healthcare and financial sectors must also observe sector-specific codes of practice issued by the relevant regulatory body.

Understanding the Risks

Different Types of Cyber Attacks



Malware

"Malicious software" such as **ransomware,** designed to damage or control a computer system

Phishing

Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

Man-in-the-Middle Attacks

Hackers insert themselves between your computer and the web server

DDoS

Distributed Denial of Service: a network of computers overload a server with data, shutting it down

Cross-Site Scripting

Injects malicious code into a website which targets the visitor's browser

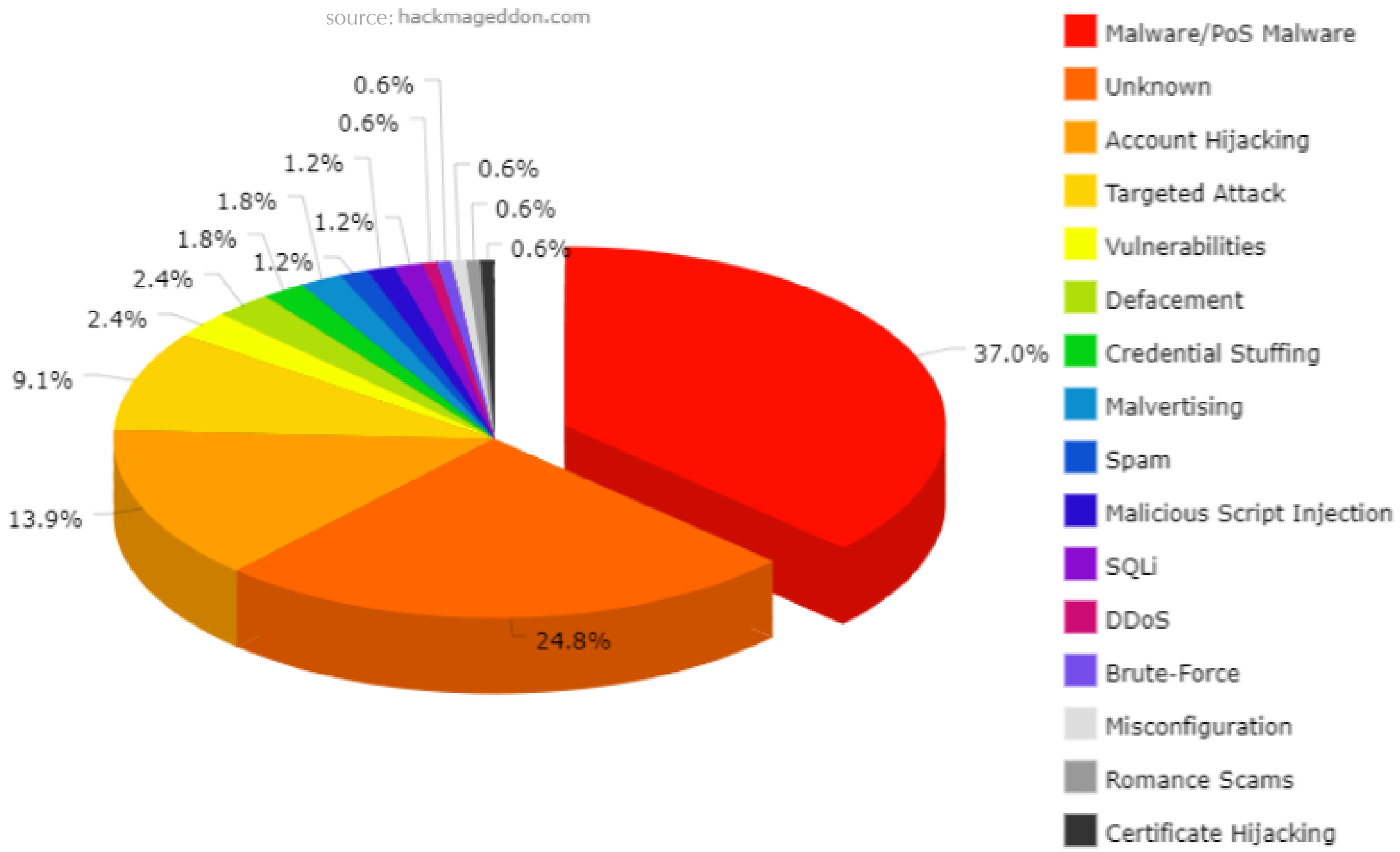
SQL Injection Attack

Corrupts data to make a server divulge data, such as credit cards numbers, usernames

*Source: Techterms.com, Lloyds of London, Forbes**

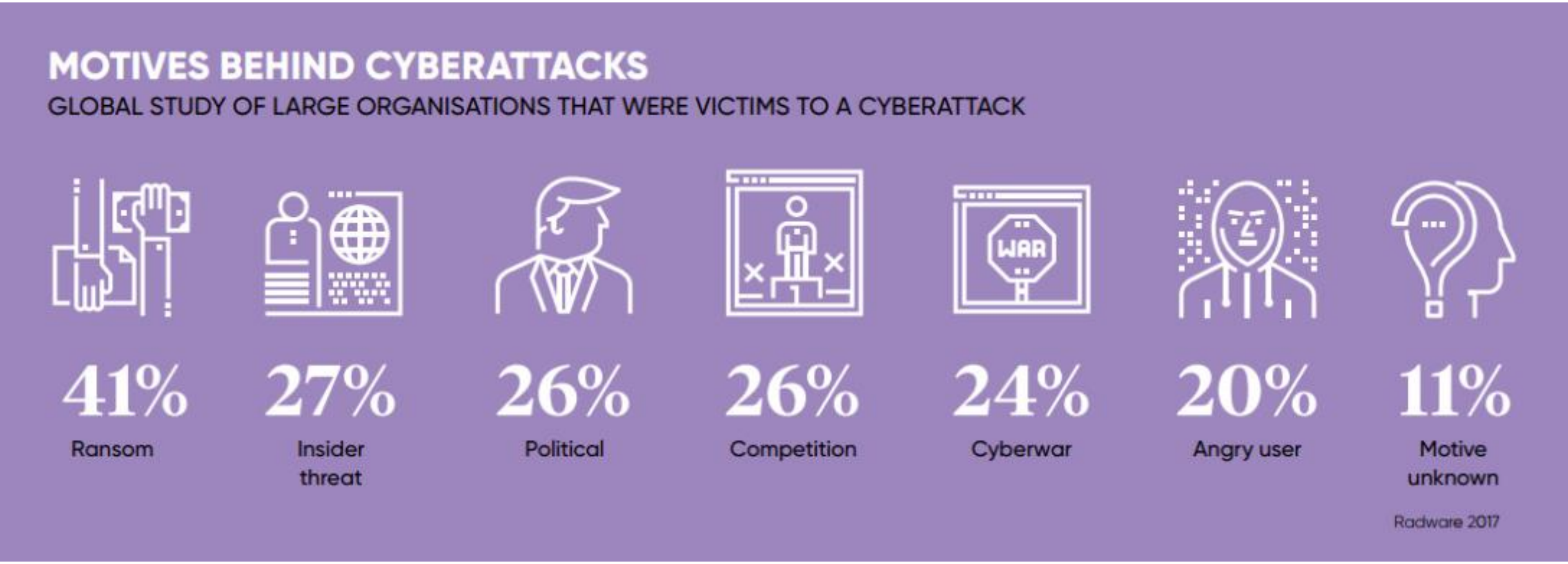
© AFP

Most Common Types of Cyber Attacks (2019)



source: hackmageddon.com

Main Motive for Cyber Attacks



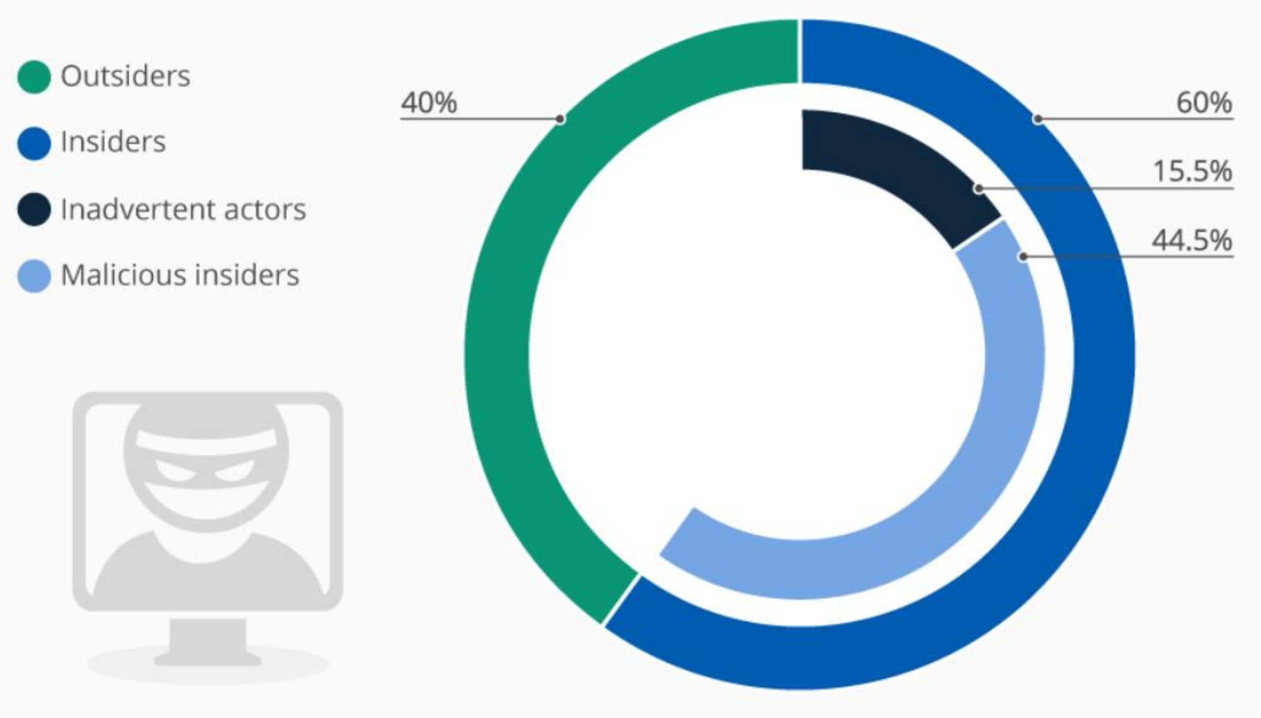
MOTIVES BEHIND CYBERATTACKS

GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK

41%	Ransom
27%	Insider threat
26%	Political
26%	Competition
24%	Cyberwar
20%	Angry user
11%	Motive unknown

Radware 2017

More than half are Inside Jobs



Malicious insiders

Intentionally use their access to sensitive data to harm the company

Careless insiders

Pose an unintentional threat due to human error or security policy violations

Compromised insiders

Insiders whose accounts are compromised and used by cyber criminals

Types of Insider Threats

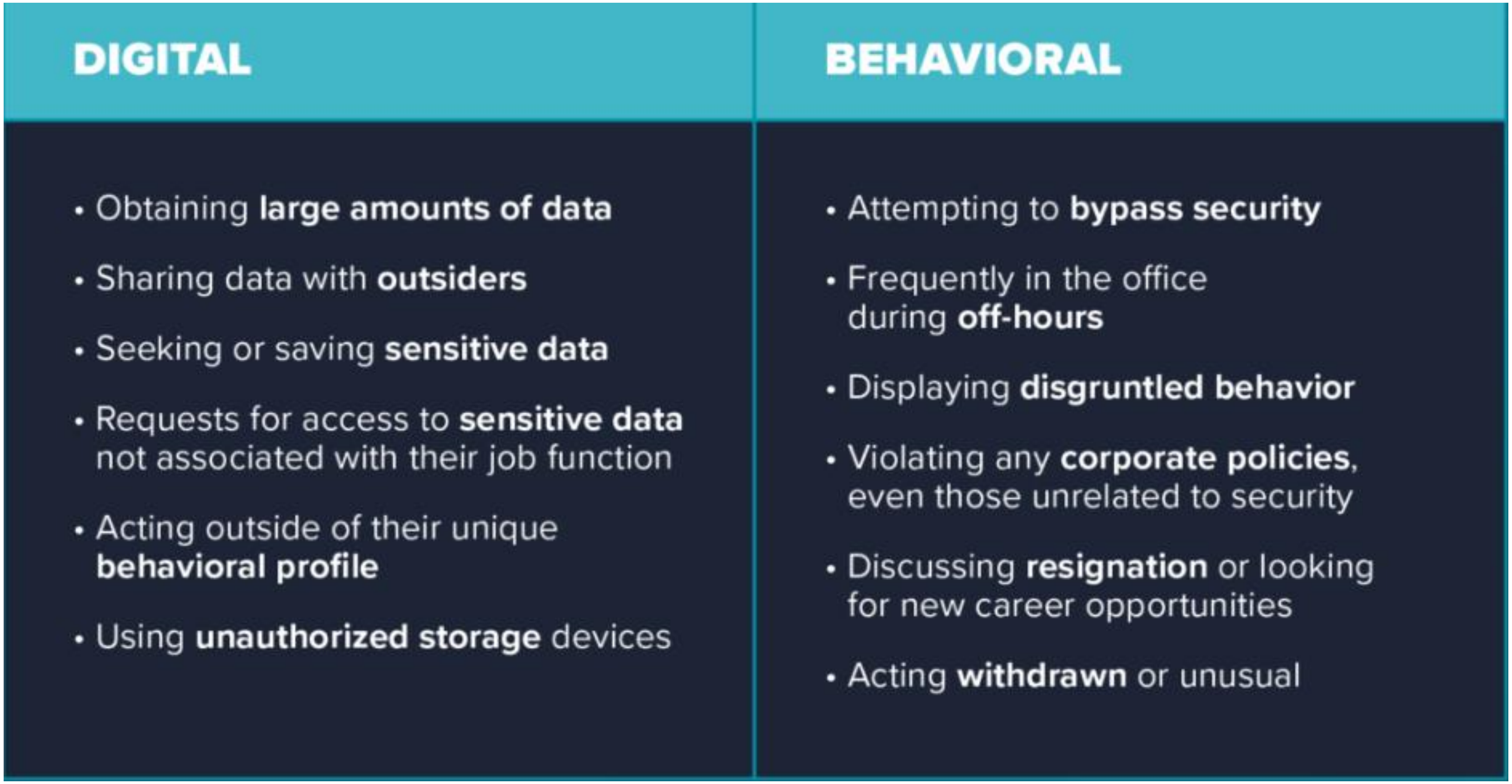
Malicious insider – also known as a Turncloak, someone who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives. For example, an individual who holds a grudge against a former employer, or an opportunistic employee who sells secret information to a competitor. Turncloaks have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

Careless insider – an innocent pawn who unknowingly exposes the system to outside threats. This is the most common type of insider threat, resulting from mistakes, such as leaving a device exposed or falling victim to a scam. For example, an employee who intends no harm may click on an insecure link, infecting the system with malware.

Compromised insider – an outsider who has managed to gain insider access to a privileged network through an employee or partner. This is someone from outside the organization who poses as an employee or partner.

What do you need to do?

How to detect Insider Threats



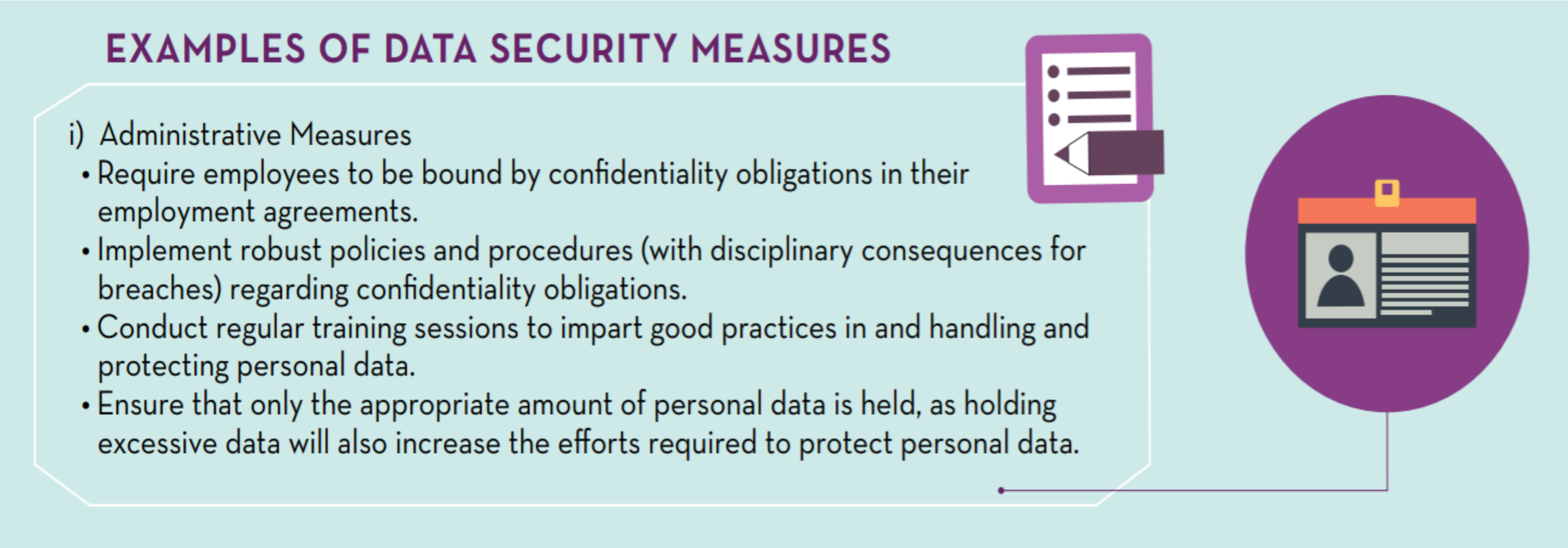
DIGITAL	BEHAVIORAL
• Obtaining **large amounts of data**	• Attempting to **bypass security**
• Sharing data with **outsiders**	• Frequently in the office during **off-hours**
• Seeking or saving **sensitive data**	• Displaying **disgruntled behavior**
• Requests for access to **sensitive data** not associated with their job function	• Violating any **corporate policies**, even those unrelated to security
• Acting outside of their unique **behavioral profile**	• Discussing **resignation** or looking for new career opportunities
• Using **unauthorized storage** devices	• Acting **withdrawn** or unusual

source: www.varonis.com

How to detect an Insider Threat

- Identify those who need to access sensitive data as part of their job.
- Monitor behavior of these staff as they go about performing their duties.
- Ask: “Does this staff regularly access this data? Is the staff exhibiting any other abnormal behaviors? Is he uploading large quantities of data to email?”
- Another strategy is to install cybersecurity solutions to analyze user behaviors and help identify normal or abnormal activities.

Reasonable Security Arrangements



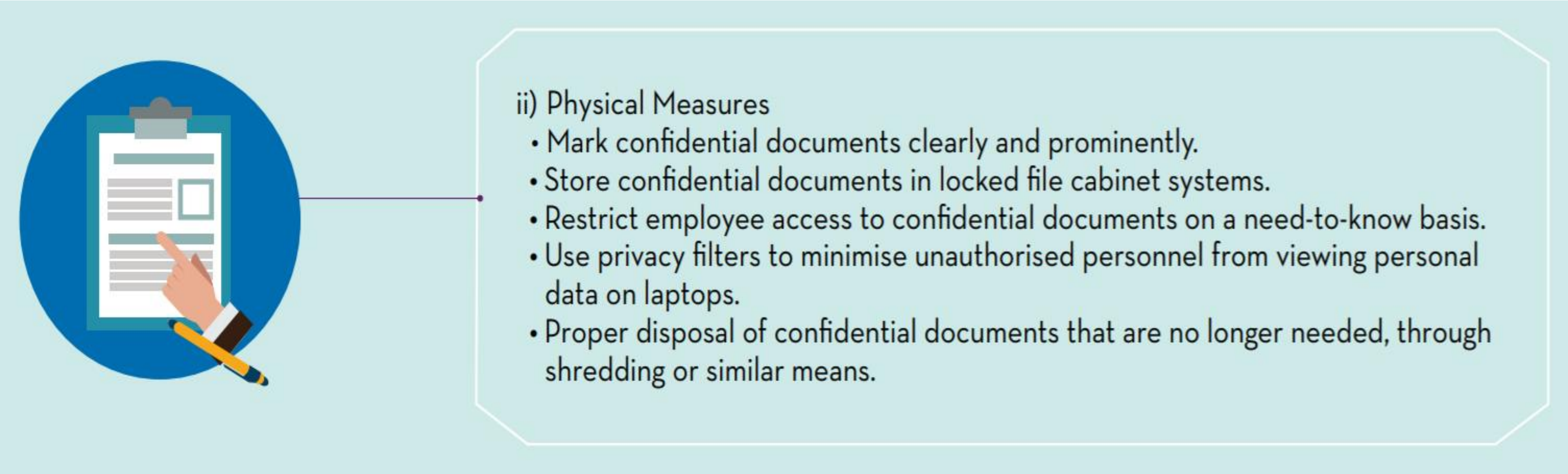
EXAMPLES OF DATA SECURITY MEASURES

i) Administrative Measures

- Require employees to be bound by confidentiality obligations in their employment agreements.
- Implement robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations.
- Conduct regular training sessions to impart good practices in and handling and protecting personal data.
- Ensure that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data.

source: www.pdpc.gov.sg

Reasonable Security Arrangements

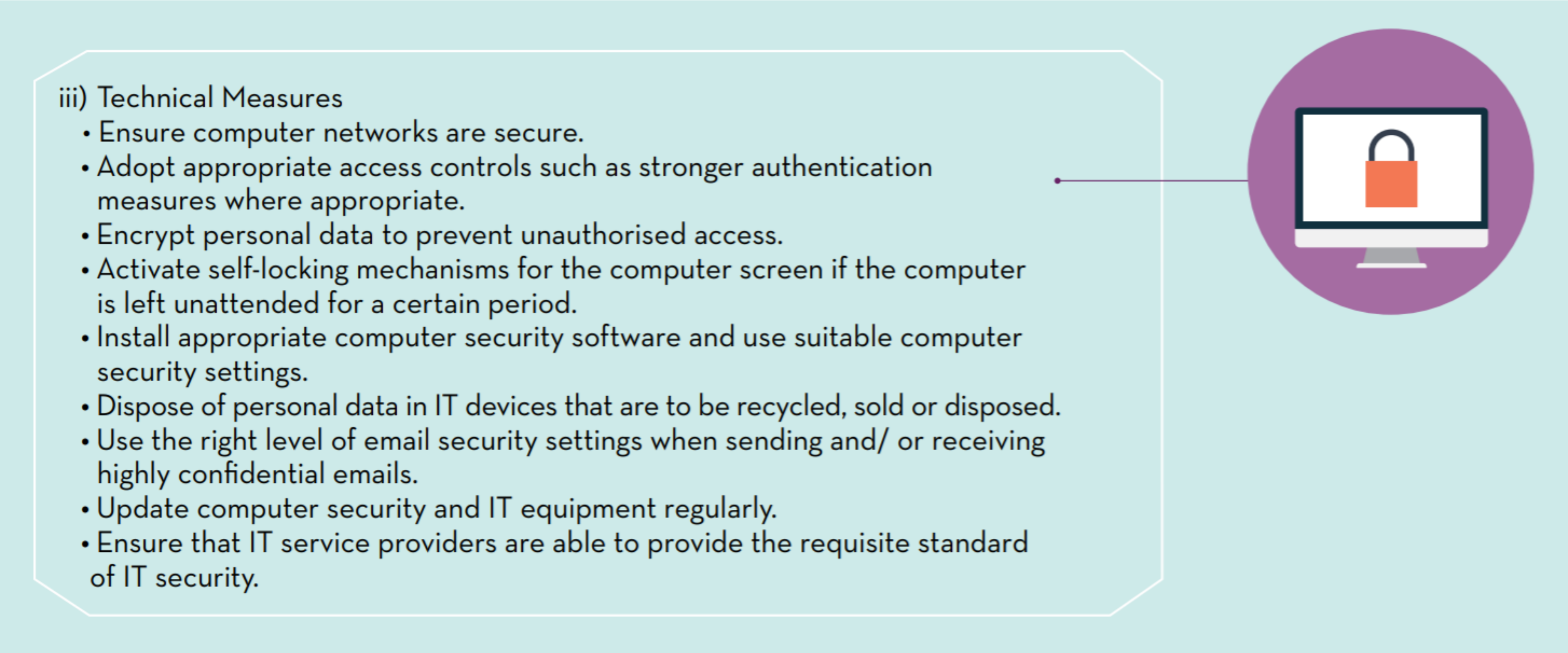


ii) Physical Measures

- Mark confidential documents clearly and prominently.
- Store confidential documents in locked file cabinet systems.
- Restrict employee access to confidential documents on a need-to-know basis.
- Use privacy filters to minimise unauthorised personnel from viewing personal data on laptops.
- Proper disposal of confidential documents that are no longer needed, through shredding or similar means.

source: www.pdpc.gov.sg

Reasonable Security Arrangements

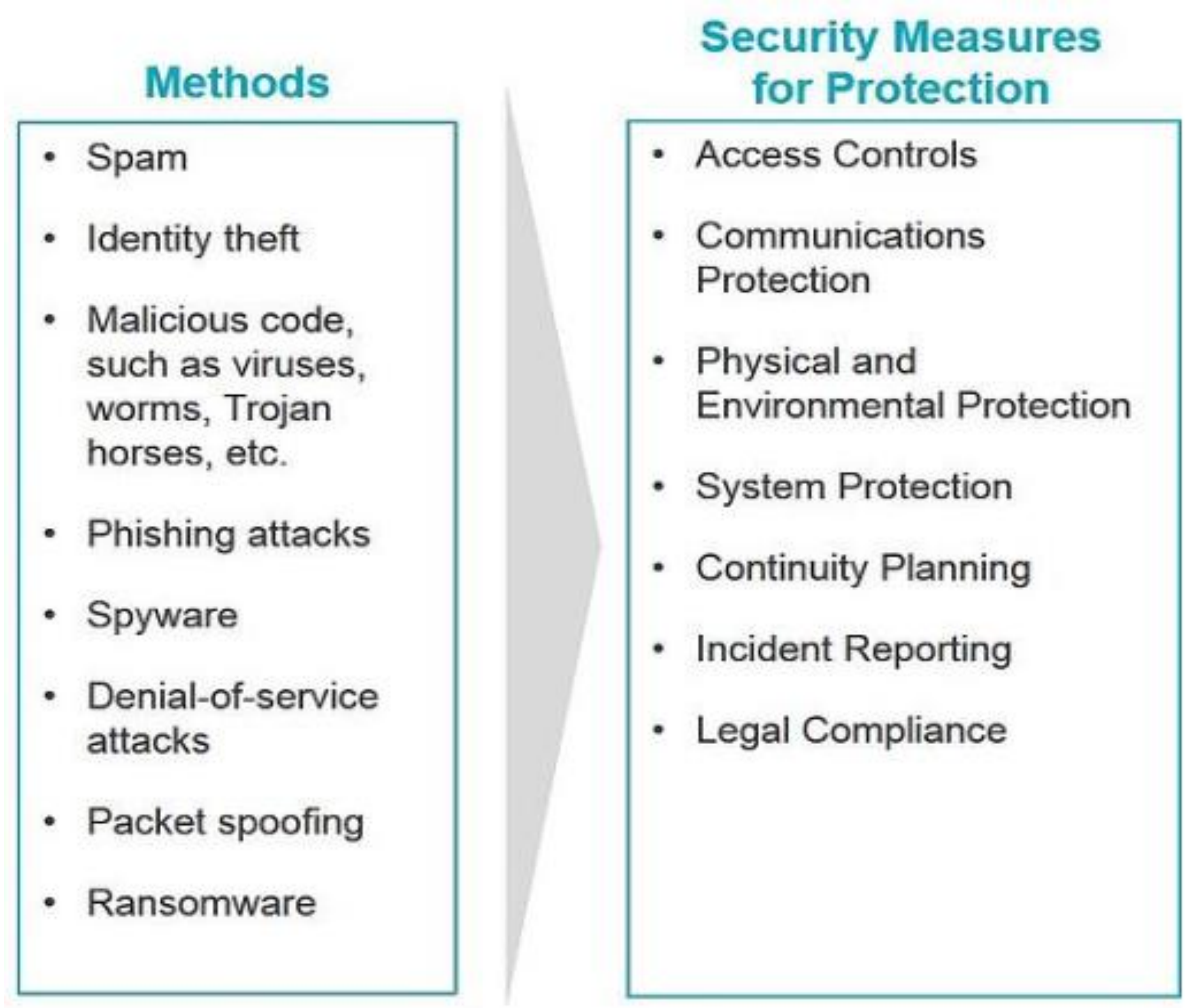


iii) Technical Measures

- Ensure computer networks are secure.
- Adopt appropriate access controls such as stronger authentication measures where appropriate.
- Encrypt personal data to prevent unauthorised access.
- Activate self-locking mechanisms for the computer screen if the computer is left unattended for a certain period.
- Install appropriate computer security software and use suitable computer security settings.
- Dispose of personal data in IT devices that are to be recycled, sold or disposed.
- Use the right level of email security settings when sending and/ or receiving highly confidential emails.
- Update computer security and IT equipment regularly.
- Ensure that IT service providers are able to provide the requisite standard of IT security.

source: www.pdpc.gov.sg

Security Measures against Cyber Threats



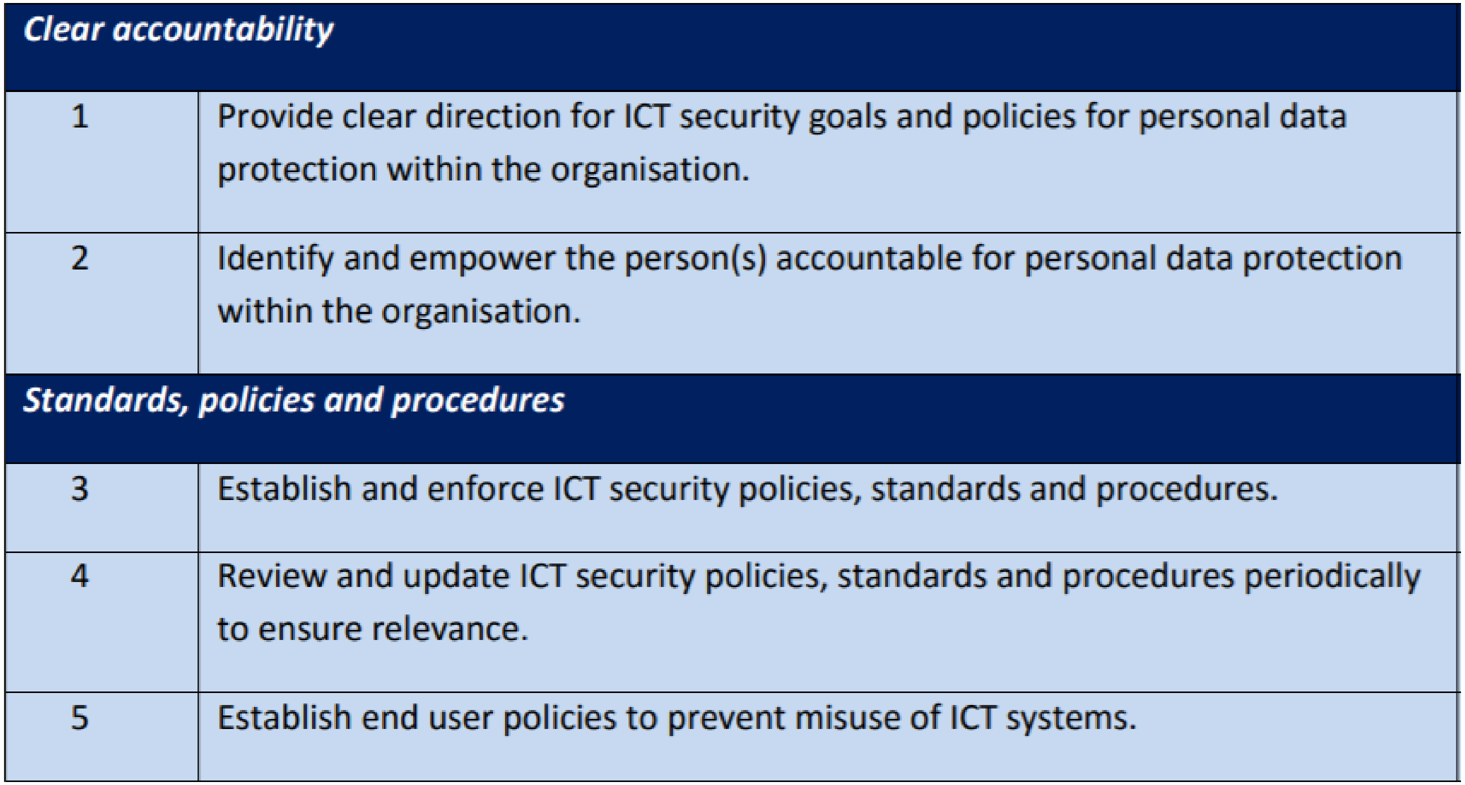
Methods

- Spam
- Identity theft
- Malicious code, such as viruses, worms, Trojan horses, etc.
- Phishing attacks
- Spyware
- Denial-of-service attacks
- Packet spoofing
- Ransomware

Security Measures for Protection

- Access Controls
- Communications Protection
- Physical and Environmental Protection
- System Protection
- Continuity Planning
- Incident Reporting
- Legal Compliance

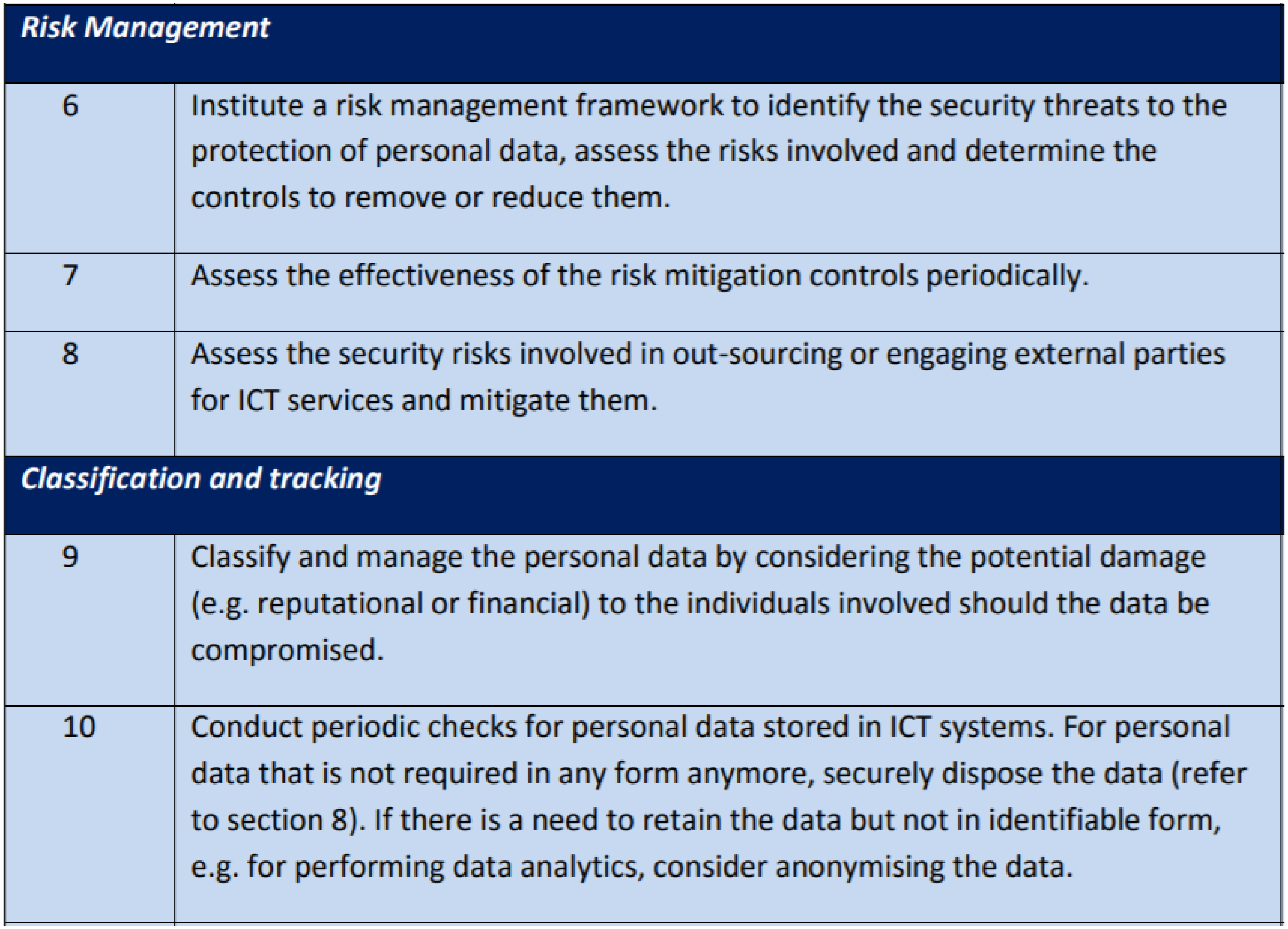
Sample list of Good Practices in Securing Personal Data in Electronic Medium



Clear accountability	
1	Provide clear direction for ICT security goals and policies for personal data protection within the organisation.
2	Identify and empower the person(s) accountable for personal data protection within the organisation.
Standards, policies and procedures	
3	Establish and enforce ICT security policies, standards and procedures.
4	Review and update ICT security policies, standards and procedures periodically to ensure relevance.
5	Establish end user policies to prevent misuse of ICT systems.

source: www.pdpc.gov.sg

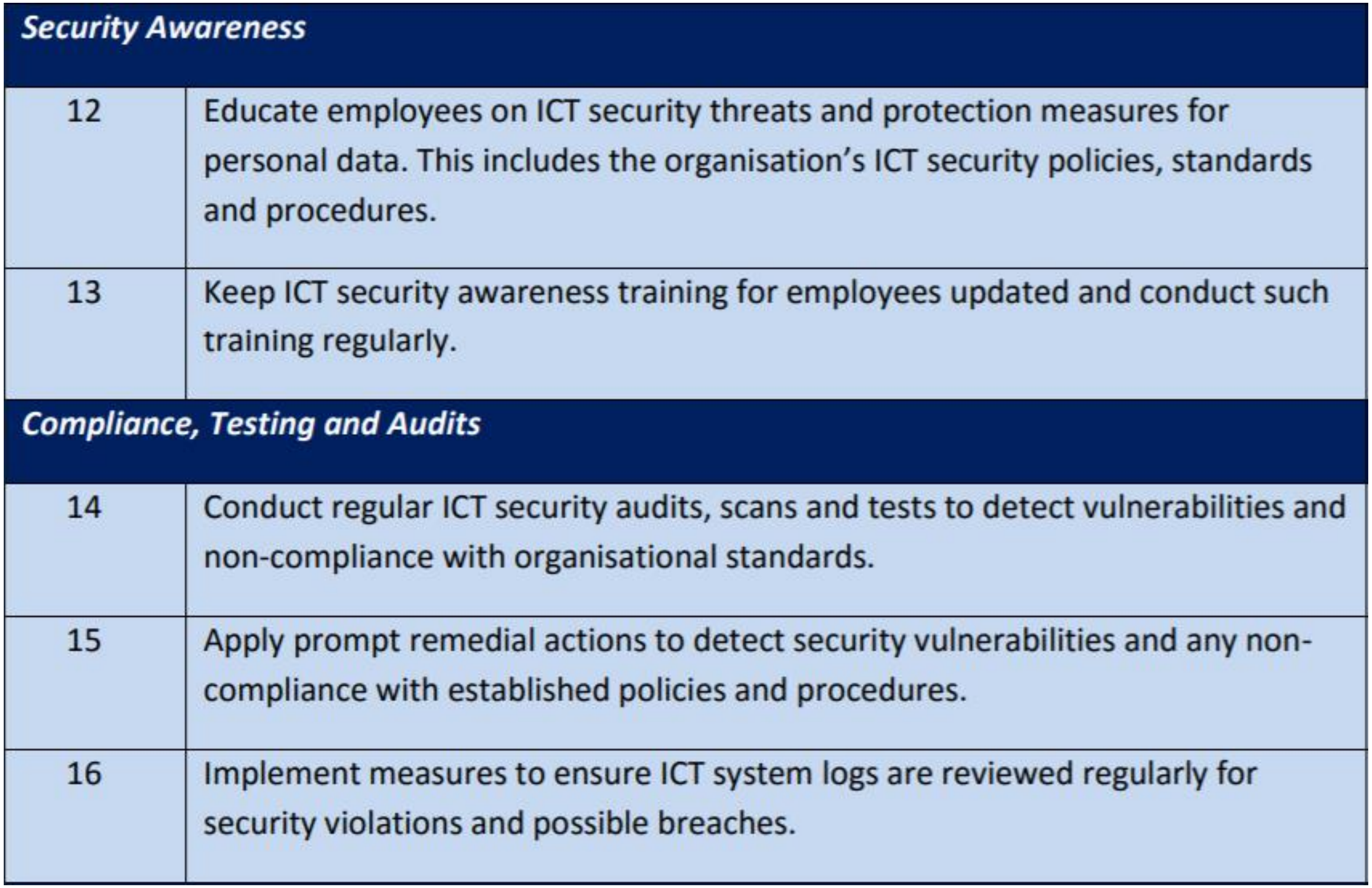
Sample list of Good Practices in Securing Personal Data in Electronic Medium



Risk Management	
6	Institute a risk management framework to identify the security threats to the protection of personal data, assess the risks involved and determine the controls to remove or reduce them.
7	Assess the effectiveness of the risk mitigation controls periodically.
8	Assess the security risks involved in out-sourcing or engaging external parties for ICT services and mitigate them.
Classification and tracking	
9	Classify and manage the personal data by considering the potential damage (e.g. reputational or financial) to the individuals involved should the data be compromised.
10	Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose the data (refer to section 8). If there is a need to retain the data but not in identifiable form, e.g. for performing data analytics, consider anonymising the data.

source: www.pdpc.gov.sg

Sample list of Good Practices in Securing Personal Data in Electronic Medium



Security Awareness	
12	Educate employees on ICT security threats and protection measures for personal data. This includes the organisation’s ICT security policies, standards and procedures.
13	Keep ICT security awareness training for employees updated and conduct such training regularly.
Compliance, Testing and Audits	
14	Conduct regular ICT security audits, scans and tests to detect vulnerabilities and non-compliance with organisational standards.
15	Apply prompt remedial actions to detect security vulnerabilities and any non-compliance with established policies and procedures.
16	Implement measures to ensure ICT system logs are reviewed regularly for security violations and possible breaches.

source: www.pdpc.gov.sg

Questions to ask …..

- Have we implemented ICT security SOPs and policies?
- Have we conducted risk assessments of IT system?
- Have we maintained a certain level of awareness among staff on data protection and cyber risks?
- Do we regularly train our staff on data protection and cyber risks?
- Do we have a procedure for reporting and managing a cyber breach?

Take Aways …..

- There is no ‘one size fits all’ solution for all organisations. Each organisation has to adopt ICT security measures that are reasonable and appropriate for their circumstances.
- Familiarise yourself with latest developments on ICT security and protection of personal data stored in electronic medium.
- Establish good practices to protect electronic personal data.
- Where necessary, engage professional advice and services regarding ICT security.

Jonathan Kok
Partner | Singapore
Intellectual Property & Technology

t: +65 6238 3032
e: jon.kok@witherskhattarwong.com

Withers KhattarWong LLP is a Singapore law practice with Registration No. T12LL0001E with Singapore qualified lawyers and foreign registered lawyers. Only Singapore law qualified lawyers of Withers KhattarWong LLP are allowed to provide Singapore law advice and represent clients in the Singapore courts under the Legal Profession Act. We are regulated by the Law Society of Singapore and the Legal Services Regulatory Authority.

'Withers' and 'Withersworldwide' are the names under which Withers LLP, Withers Bergman LLP and their affiliated partnerships, offices, undertakings and affiliates and alliances, including Withers Australia, Withers BVI, Withers 衛達仕, Studio Legale Associato con Withers LLP, Withers KhattarWong LLP, Withers Japan and Zeirishi Houjin (each of which is its own legal entity), are authorised to provide legal or other client services.