GUIDE TO CYBERSECURITY

FOR LAW PRACTICES

30 MARCH 2020

The Law Society of Singapore

Published by:
The Law Society of Singapore
28 Maxwell Road, #01-03, Singapore 069120

Acknowledgements

This Guide was developed by the Law Society of Singapore's Cybersecurity and Data Protection Committee 2019-2020. The Committee members involved include:

Lim Kian Kim

Co-Chairperson of the Committee

Of Counsel, Head of Cybersecurity, Privacy and Data Protection, Eversheds Harry Elias LLP

Avinderjit Singh Rakhra

Lead Author and Committee Member

Senior Legal Counsel, Deutsche Bank AG Singapore

Lim Seng Siew

Council Representative to the Committee

Director, OTP Law Corporation

Tay Yew Choon

Committee Member

Senior Associate, CTLC Law Corporation

Darren Grayson Chng

Committee Member

Senior Legal Counsel

The Committee would like to thank the Law Society of Singapore's Secretariat for their support and Michelle Chua for her editorial assistance.

Preface

Dear Colleagues,

In an interconnected world, solicitors must practise in a secure environment that is as safe as it can be, both for themselves and their clients. This is because we are part of the national information security grid, members of an honourable profession and responsible residents of this country in a larger sense.

Solicitors and law practices have something that is valuable and potentially profitable to those who are out to cause us and our clients harm: confidential information. Hence, we owe it to our clients, and to ourselves as practising solicitors, to keep the information in our possession safe from cyber threats.

We hope that this Guide, put together by our Committee, will serve as the first step in fulfilling these duties.

This Guide has been designed to enable a law practice to take a risk-based approach in protecting its information. It prescribes recommended practices for a law practice to consider. In a risk-based approach, a law practice should decide on a level of security most appropriate for itself, based on, *inter alia,* its unique operations and size. Nonetheless, some of the basic security measures in this Guide will apply equally to all law practices.

Be safe!

KK Lim

Best Wishes,

Mr. Lim Kian Kim

Co-Chairperson

Cybersecurity and Data Protection Committee 2019-2020

The Law Society of Singapore

Executive Summary

Cybersecurity threats occur on a daily basis, placing the infocommunication technology systems of law practices at risk. This Guide enables law practices, regardless of size and degree of cybersecurity risk, to improve their cybersecurity resilience by applying the practices recommended.

This Guide adopts practices prescribed by the United States Department of Commerce's National Institute of Standards and Technology. References are also made to other cybersecurity standards and guidelines published by local and international regulatory bodies. This Guide seeks to contextualise the recommended measures found in these publications for solicitors and law practices.

Before explaining this Guide, it is helpful to consider the legal definition of cybersecurity in Singapore. Cybersecurity is defined in Singapore's Cybersecurity Act 2018 (No. 9 of 2018) as a state in which (*emphasis added*) a computer or computer system is protected from unauthorised access or attack, and because of that (*protected*) state, the computer or computer system is available and operational, its integrity is maintained and the integrity and confidentiality of the information stored in, processed by or transmitted through it is maintained. In essence, this definition covers both infocommunication technology systems themselves (i.e. hardware and software) as well as information (i.e. data) that is stored in, processed by or transmitted through these systems.

Because data can exist in many infocommunication technology services and components, such as in email, a database, the cloud, a computer network, on storage media and so on, the approach we took in writing this Guide was to provide a set of recommended practices for the key services and components that store, process or transmit the data of a law practice. If applied, these practices can improve the cybersecurity resilience of a law practice. Readers should note that this Guide is not intended to be an exhaustive guide on data protection, and may refer to the Personal Data Protection Commission of Singapore for resources on data protection.

This Guide first focuses on the governance aspects of a law practice in **Chapter 5**. Strong organisational and risk management processes are key foundations for a law practice in combatting cybersecurity issues. Potential measures include promoting staff awareness and ensuring that internal policies and processes thoroughly cover the operations of a law practice's infocommunication technology systems. Such measures also indirectly strengthen the incident response capabilities of a law practice.

People and processes aside, we focus on technology aspects in subsequent chapters. Given the amount of infocommunication technology software and hardware that can easily amass in a law practice, ensuring that these components are inventoried, kept up-to-date and monitored is imperative for a law practice's efficient functioning, as set out in **Chapter 6**. If, for example, software is not updated as regularly as recommended by the relevant software provider, it may not contain the latest cybersecurity updates and may therefore compromise a law practice's cybersecurity resilience.

In **Chapters 7 and 8**, we cover how to protect hardware devices and infrastructure typically used in a law practice, such as removable storage media, laptops and computer networks. Such

protection is akin to protecting the boundary of a law practice. If this defence is broken into, a cyber attack may be able to penetrate into the law practice.

Staff of a law practice must be able to access its infocommunication technology systems and information. However, the access mechanisms used by a law practice must be robust in order to prevent unauthorised access by third parties. Managing the security of data is equally important and potential measures include encrypting data to prevent unauthorised intervention, creating backups of data regularly and storing data for predefined retention periods. If these measures are applied, then in the situation of a cyber attack, a law practice could revert to an uncompromised backup copy of the relevant data. We cover these aspects of cybersecurity in **Chapters 9 and 10**.

Accessing data is necessary in performing routine tasks such as sending emails and accessing databases. On many occasions, these tasks are done via websites and web applications. Law practices should be aware that the performance of these tasks carries cybersecurity risk. For example, an email may contain a harmful virus that, if not screened and deleted by anti-malware software, could result in a cyber incident. The use of email, websites and databases is covered in **Chapters 11, 12 and 13**. Finally, we cover cloud computing in **Chapter 14**, given the prominence of this growing area.

This is not an exhaustive one-size-fits-all Guide. Law practices each have their own unique risks, and must take a risk-based approach by assessing their risks and then deciding which measures to apply.

Effective use of this Guide will enable a law practice that has not yet adopted some of the measures herein to achieve a minimum level of cybersecurity resilience. This Guide is a living document and will continue to be updated and improved as technology evolves and we receive feedback from our members.

Table of Contents

PART 1: OVERVIEW

1. Introduction

1.1 The status of this document is that of a Guide from the Law Society of Singapore. This Guide sets out measures that will improve a law practice's cybersecurity resilience, and suggests how law practices should handle personal and confidential data provided to them with respect to cybersecurity.

1.2 This Guide will be useful for:

- Solicitors in law practices;
- Persons who supervise or work as in-house information technology professionals in law practices; and
- Outsourced information technology vendors of law practices.

1.3 In applying this Guide, we propose that law practices take a risk-based approach in deciding the extent to which they wish to comply with its recommendations. This is because law practices can be extremely varied in terms of size, type and the nature and demands of their clients. In addition, global law practices may require that all their offshore practices, including those in Singapore, adopt their global security policies and procedures.

2. Scope and Qualifications

2.1 This Guide is not prescriptive and does not offer an exhaustive list of measures applicable to law practices. Each law practice needs to examine its operations in detail and decide on security measures that are most reasonable and appropriate for itself. Depending on the circumstances, minimum standards other than those recommended in this Guide may also be appropriate. Law practices may wish to seek professional advice and services regarding infocommunication technology ("**ICT**") cybersecurity, where necessary.

2.2 The collection, use and disclosure of personal data in Singapore is governed by the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**"). Generally, compliance with the PDPA is a requirement for all law practices in Singapore. A law practice's or solicitor's compliance with this Guide does not mean that the law practice or solicitor is compliant with the PDPA or related subsidiary legislation or guidelines issued by the Personal Data Protection Commission of Singapore.

2.3 This Guide does not in any way detract from a law practice's or solicitor's professional and ethical obligations, nor is it intended to create additional ethical obligations for a law practice or solicitor.

2.4 A law practice's or solicitor's compliance with this Guide does not mean that the law practice or solicitor is compliant with the terms or qualifying conditions of any cybersecurity, professional indemnity or other insurance policy negotiated for or recommended by the Law Society of Singapore.

3. Key Terms

3.1 There are key terms that a reader should be aware of when reading this Guide. These terms are set out in this section as well as in the accompanying Glossary to this Guide.

3.2 In parts of this Guide, we may use the term "ICT security", rather than "cybersecurity", because it is the security of information that we are primarily concerned with. In today's parlance, these terms are used interchangeably.

3.3 The term "domain" refers to the different broad areas that ICT security measures are classified under. An example of a domain is "governance", which refers to an organisation's internal ICT security policies and organisational processes. In this Guide, we examine various cybersecurity domains relevant to law practices, and in relation to each domain, offer a list of "controls", which are the specific recommendations on what to implement, i.e. the "how-to's". Controls are further divided into "good practices", which are basic practices for cybersecurity protection, and "enhanced practices", which are practices for achieving a higher standard of cybersecurity resilience.

3.4 Readers should note that any recommendations in this Guide concerning the protection of personal data can be applied to confidential information as well.

4. References to Existing Cybersecurity Standards and Guidelines

4.1 This Guide's recommendations are made with reference to local and international cybersecurity standards and guidelines used in the wider information technology sector. This is to ensure that this Guide is practical and implementable, and is not just another set of guidelines containing a plethora of principles without specific "how-to's".

4.2 In line with this, we respectfully make numerous references to publications issued by global technical bodies on information security and related regulatory bodies. We **acknowledge with gratitude** the use of the following materials produced by these bodies in our Guide:

A. The Personal Data Protection Commission of Singapore (2017). *Guide to Securing Personal Data in Electronic Medium*. Revised 20 January 2017. Available at: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Other-Guides (Accessed 28 March 2020) ("**PDPC SPD Guide**")

B. Cyber Security Agency of Singapore (2018). *Be Safe Online Handbook*. Available at: https://www.csa.gov.sg/gosafeonline/resources/be-safe-online-handbook (Accessed 28 March 2020) ("**CSA BSO Handbook**")

C. The United States Department of Commerce, National Institute of Standards and Technology (2013). *NIST Special Publication 800-53, Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations*. Updated 22 January 2015. Available at: http://dx.doi.org/10.6028/NIST.SP.800-53r4 (Accessed 28 March 2020) ("**NIST Special Publication 800-53**")

D. The International Bar Association (2018). *Cyber Security Guidelines*. Available at: https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx (Accessed 28 March 2020) ("**IBA Guidelines**")

E. Internet Engineering Task Force (2007). *Internet Security Glossary, Version 2*. Available at: https://tools.ietf.org/html/rfc4949 (Accessed 28 March 2020) ("**IETF Security Glossary**")

F. Committee on National Security Systems (2015). *Committee on National Security Systems (CNSS) Glossary. CNSS Instruction No. 4009*. Available at: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf (Accessed 28 March 2020) ("**CNSS Glossary**")

PART 2: DOMAIN SECURITY MEASURES

5. Governance

5.1 In order to mitigate the risk of cyber attacks, a law practice must implement strong organisational processes and good cybersecurity governance. For example, maintaining an audit trail can show unusual frequent access to a particular file at odd hours, and therefore alert a law practice to look into the situation further. The recommended controls are divided into four categories: a) Policies and Procedures; b) Awareness and Training; c) Audit and Accountability; and d) Operational Measures.

Table 1: Governance **a) Policies and Procedures**			
		Good Practice	**Enhanced Practice**
1.	Establish and enforce ICT security policies and procedures and keep such policies and procedures updated regularly.[1]	√	
b) Awareness and Training			
2.	Provide security awareness training to ICT users as part of initial training for new employees and conduct such training regularly to keep employees educated and abreast of cybersecurity threats and security measures.[2]	√	
3.	Evaluate and enforce legal and regulatory obligations.[3] This means understanding and implementing, where necessary, legal and regulatory obligations relating to cybersecurity that apply directly in Singapore.	√	
c) Audit and Accountability			
4.	Review and analyse ICT systems audit records and logs regularly for indication of inappropriate or unusual activity and report the findings to those responsible for managing such events.[4]		√

[1] NIST Special Publication 800-53, Controls AT-1 and AU-1; PDPC SPD Guide at Table 1
[2] NIST Special Publication 800-53, Control AT-2
[3] IBA Guidelines at page 16
[4] NIST Special Publication 800-53, Controls AU-3, AU-6 and AU-12. See also CSA BSO Handbook, Essential 5 at page 12

5.	Ensure that audit information is protected from unauthorised access, modification and deletion,[5] and is retained for administrative, regulatory or other operational purposes, until such time that these records are no longer required.[6]		√
d) Operational Measures			
6.	Conduct an assessment of risk, including the likelihood and severity of harm arising from unauthorised access, use, disclosure, disruption, modification or destruction of the law practice's ICT systems and the information that the law practice stores, processes and transmits.[7]	√	
7.	Conduct periodic scanning of the law practice's ICT systems to detect security vulnerabilities in the ICT systems and software applications that are used, for example, scanning for patch levels and ports that should not be accessible to users.[8]	√	
8.	Conduct periodic testing of cybersecurity incident response capabilities to test the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies.[9]		√
9.	Put in place adequate incident handling capabilities, for example, to stop attacks, misdirect attackers and to isolate components of systems, in order to limit the extent of damage from breaches or compromises.[10]		√
10.	Track, document and report ICT security incidents.[11]		√
11.	Ensure that the same personnel do not perform conflicting functions, for example, administrating security access controls as well as performing audit functions.[12] It is especially important that small law practices ensure there is clear separation of duties, adopting suitable methods that are practicable.	√	

[5] NIST Special Publication 800-53, Control AU-9
[6] NIST Special Publication 800-53, Control AU-11
[7] NIST Special Publication 800-53, Control RA-3
[8] NIST Special Publication 800-53, Control RA-5
[9] NIST Special Publication 800-53, Control IR-3
[10] NIST Special Publication 800-53, Control IR-4
[11] NIST Special Publication 800-53, Controls IR-5 and IR-6
[12] NIST Special Publication 800-53, Control AC-5

12.	Conduct regular backups of ICT systems, including backups of operating systems, application software, licences, ICT documentation and data.[13]	√	

6. Asset Management

6.1 The ICT infrastructure in a law practice will typically consist of various hardware and software components such as network equipment and server hardware. Irrespective of what these components are, certain common practices will apply to all of these assets, for example, monitoring and maintenance.

Table 2: Asset Management

		Good Practice	Enhanced Practice
1.	All hardware and software (software includes, for example, operating systems, middleware and organisation-defined applications) must be inventoried.[14]		√
2.	Ensure that hardware and software maintenance and upgrades of ICT systems are routinely scheduled and carried out by qualified professionals, and that impacted security controls are still functioning properly following maintenance or repair actions.[15]		√
3.	Enable and configure encryption: a. Enable network encryption protocols;[16] b. Encrypt passwords and other configuration settings;[17] and c. Encrypt storage.[18]	√	
4.	Make use of automated mechanisms that detect the presence of unauthorised user-installed software within		√

[13] NIST Special Publication 800-53, Control CP-9
[14] NIST Special Publication 800-53, Controls CM-8 and CM-11. See also CSA BSO Handbook, Essential 1 at page 4
[15] NIST Special Publication 800-53, Controls MA-2 and CM-5. See also CSA BSO Handbook, Essential 3 at page 8
[16] NIST Special Publication 800-53, Controls AC-18, SC-8 and SC-13
[17] NIST Special Publication 800-53, Controls IA-7, SC-8 and SC-13
[18] NIST Special Publication 800-53, Controls SC-13 and SC-28

	the ICT system and notify those responsible upon such detection.[19]		
5.	Regularly update operating systems, firmware, middleware and organisation-defined applications and ensure that security patches are applied in a timely manner as recommended by the supplier of the ICT product commensurate with the criticality of the ICT system, the type and confidentiality of the information residing on it and the criticality of the vulnerability.[20]	√	

7. Personal Computers, Removable Storage Media and Other Computing Devices

7.1 In addition to desktop personal computers ("**PCs**"), other fast maturing mobile devices ("**MDs**") can perform many of the functions of the PC. Examples of such devices include laptops, mobile phones and tablets. These devices enable access to a wide range of applications with the additional benefit of being mobile. Removable storage media such as USB drives are also commonly used.

7.2 MDs are more susceptible to being misplaced or stolen compared to PCs. Additional security measures should be taken to protect these devices and the data on these devices in order to reduce the likelihood of unauthorised access. For example, the application of sophisticated access controls and encryption can help reduce the likelihood of an attacker gaining direct access to sensitive information. These security measures should apply irrespective of whether the devices are issued by the law practice or owned by the employees.[21] In addition to security measures, law practices may consider implementing policies governing the use of MDs for work. Some common policies include Bring Your Own Device ("**BYOD**") and Company Owned and Personally Enabled ("**COPE**") policies.

7.3 Printers, scanners and fax machines can have many of the characteristics of computing devices. They may have storage, a computer processor and an operating system, and may be connected to the computer network system of a law practice. Law practices should thus take appropriate security measures in relation to these devices. For example, before exchanging an old printer for a new printer under your leasing scheme, information stored

[19] NIST Special Publication 800-53, Control CM-11(1). See also CSA BSO Handbook, Essential 2 at page 6
[20] NIST Special Publication 800-53, Control SI-7
[21] PDPC SPD Guide at paragraphs 11.2 and 11.3

on the old printer should be erased. Some printers and scanners are also connected to the internet and are consequently vulnerable to security threats from the internet. Many of the security measures covered in this Guide may be applicable to these devices.

Table 3: Personal Computers, Removable Storage Media and Other Computing Devices			
		Good Practice	**Enhanced Practice**
1.	Establish usage restrictions, configuration requirements, connection requirements and implementation guidance for organisational-controlled MDs such as COPE devices.[22]	√	
2.	Install software and/or implement sanitisation techniques that can remotely erase sensitive data and wipe out the contents of a PC or MD when it is lost or stolen, upon termination of employment or at any time necessary.[23]		√
3.	Implement a process that allows software to run (i.e. whitelist) or prevents software from running (i.e. blacklist).[24]		√
4.	Destroy or delete information from a PC or MD when the information is no longer needed.[25]	√	
5.	Configure a PC or MD such that it will lock automatically after an idle period.[26]	√	
6.	Disable access to a PC or MD when the relevant user leaves the law practice.[27] In a BYOD scenario, the business applications of the law practice and other related data must be backed up and then deleted from all relevant MDs.	√	
7.	Physically remove or disable connection ports and Input/Output devices (as appropriate) to prevent exfiltration of information from the law practice's ICT systems and to prevent the introduction of malicious code into the ICT systems from those ports or devices.[28]	√	

[22] NIST Special Publication 800-53, Control AC-19
[23] NIST Special Publication 800-53, Control MP-6(8)
[24] NIST Special Publication 800-53, Control CM-7(4 and 5)
[25] NIST Special Publication 800-53, Control MP-6. See also *NIST Special Publication 800-88, Revision 1. Guidelines for Media Sanitization*, listed at Annex B of this Guide
[26] NIST Special Publication 800-53, Control AC-11
[27] NIST Special Publication 800-53, Control AC-17(9)
[28] NIST Special Publication 800-53, Control SC-41

8.	Establish and implement configuration settings for security related parameters on the law practice's ICT systems, for example, security settings for functions, ports and remote connections.[29]		√

8. Computer Networks

8.1 A computer network allows devices connected to it to communicate with each other and to share computing resources. Such devices include computers, servers, printers, storage devices and so on. Computer networks can be established via various means, including copper, fibre optic or wireless radio waves. A computer network may also be connected to another network. For example, an internal corporate network may be connected to an external network, such as the internet.

8.2 Wireless local area networks (commonly referred to as "**WiFi networks**") are generally regarded as being more vulnerable, because a cyber attacker need not be physically connected to the relevant computer network in order to gain access.

8.3 It is important that the computer network in a law practice is secure and protects the usability and integrity of other devices connected to it and the data passing through it.

8.4 Defences that can be used to improve the security of computer networks include[30]:

- Intrusion prevention systems ("**IPS**") – devices or software applications that monitor networks or system activities and prevent malicious activities or policy violations;
- Intrusion detection systems ("**IDS**") – network security appliances that monitor network and system activities for malicious activities and which may raise alerts upon detecting unusual activities;
- Security devices that prevent the unauthorised transfer of data out of a computer network;
- Firewalls; and
- Web proxies, anti-virus software and anti-spyware software.

[29] NIST Special Publication 800-53, Control CM-6
[30] PDPC SPD Guide at paragraph 9.1

Table 4: Computer Networks			
		Good Practice	**Enhanced Practice**
1.	Equip networks with defence devices or software.[31]	√	
2.	Unless strictly necessary, disallow remote network administration.[32]	√	
3.	Design and implement the law practice's internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type and so on, and implementing boundary protection with external networks.[33]	√	
4.	Disable unused network ports.[34]		√
5.	Establish usage restrictions, configuration requirements, connection requirements, and implement guidelines for wireless access.[35]	√	
6.	Apply secure connection technologies or protocols[36] to protect the transmission of electronic data and to protect the authenticity of communications sessions between web clients and web servers.[37] Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking and the insertion of false information into sessions.	√	
7.	Restrict employee access to known malicious websites.[38]	√	
8.	Unless absolutely essential, ICT contractors and third-party suppliers should not be given administrator-level access to the law practice's ICT network[39] or any other ICT infrastructure.	√	
9.	Prohibit direct connection from a private network to an external network (such as the internet) without the use of	√	

[31] PDPC SPD Guide at Table 7; NIST Special Publication 800-53, Controls SI-4(1) and SI-4(14)
[32] PDPC SPD Guide at Table 7
[33] NIST Special Publication 800-53, Control SC-7; PDPC SPD Guide at Table 7
[34] NIST Special Publication 800-53, Control SC-41; PDPC SPD Guide at Table 7
[35] NIST Special Publication 800-53, Control AC-18
[36] Such as utilising the Transport Layer Security protocol to establish authenticated and encrypted links
[37] NIST Special Publication 800-53, Control SC-23(5); PDPC SPD Guide at Table 7
[38] NIST Special Publication 800-53, Control SC-7(8); PDPC SPD Guide at Table 7
[39] IBA Guidelines at Appendix H

	boundary protection devices such as routers and firewalls to mediate communications.[40]		

9. Authentication, Authorisation and Passwords

9.1 Law practices hold large volumes of confidential information. Such information includes the personal data of clients and employees, confidential information relating to client files and other commercially sensitive information such as a firm's own trade secrets and precedents. Law practices must therefore ensure that access to data is only granted to the relevant persons where appropriate. Common methods of controlling access to ICT systems include using usernames, passwords and multi-factor authentication.

Table 5: Authentication, Authorisation and Passwords

		Good Practice	Enhanced Practice
1. [41]	a. Determine a suitable authentication method (whether single-factor or multi-factor) for accessing personal data based on the risk of damage to the relevant individuals in the event of a data breach.	√	
	b. Determine a suitable maximum number of attempts to be allowed for a user to authenticate his or her identity, based on the type of data to be accessed.	√	
	c. Implement account lockout when the maximum number of attempts is reached, to prevent dictionary or brute-force attacks. These refer to methods of systematically checking all possible keys or passwords until the correct one is found.	√	
	d. Ensure that passwords used for authentication have a length of at least eight characters and contain at least one alphabetical character and one numeric character.	√	
	e. Ensure that when a password used for authentication is typed in, it is to be hidden under placeholder characters such as asterisks or dots.	√	

[40] NIST Special Publication 800-53, Control CA-3(1)
[41] PDPC SPD Guide at Table 4, a-h

	f. Ensure that passwords used for authentication are encrypted during transmission and also encrypted or hashed in storage. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.	√	
	g. Ensure that users are required to change their passwords regularly. The frequency should be based on the risk of damage to the relevant individuals if the data is compromised.	√	
	h. Ensure that users change default passwords to strong passwords at the earliest possible opportunity.	√	
	i. Assign unique and distinct user IDs to individual users.	√	
	j. Encourage users not to use passwords that can be easily deduced, such as their birth dates or names.	√	
	k. Ensure that users change system-generated passwords upon first login.	√	
	l. Discourage users from using the same password across different systems or applications.	√	
	m. Disallow users from using a password that was used within the last three password changes.	√	
	n. Ensure that passwords used include both lowercase and uppercase characters.	√	
	o. Ensure that passwords used include special characters such as '!', '&' and so on.	√	
2.	Inform users that passwords should not be recorded on paper (handwritten or otherwise) and attached to computers or other equipment, or shared between users. [42]	√	
3.	The access of an administrator or user to a law practice's email servers should be disabled upon that administrator or user leaving the law practice.[43]	√	
4.	Ensure authorised access at the ICT level and ensure access enforcement mechanisms are employed at all	√	

[42] IBA Guidelines at Appendix H
[43] NIST Special Publication 800-53, Controls AC-2 and AC-3

	levels of the ICT layer to increase information security, including controlling remote access where outside users connect into the law practice's ICT systems through external networks.[44]		

10. Data Management[45]

10.1 Law practices usually store electronic data on devices either within their premises or at an external location. Law practices may also choose to outsource the storage of electronic data, or to store electronic data in the cloud. In either case, security measures such as encryption and authentication must be implemented in order to protect the confidentiality and integrity of such data. Large and reputable cloud service providers would usually have the necessary security measures in place for their subscribers.

10.2 Unrecoverable loss or corruption of electronic data can cripple a law practice's business and result in significant reputational damage and economic loss. It is therefore essential for law practices to implement methods and processes that enable the restoration of lost or corrupted data. Backing up data regularly is a method of mitigating this risk. A law practice that is attacked by ransomware can restore uncorrupted data and applications if it had made backups regularly.

10.3 In deciding on a backup solution, law practices may wish to evaluate what data needs to be backed up, the size of that data, the appropriate backup frequency (for example, daily, weekly or monthly) and where the backups should be stored (whether onsite, at a secure offsite data storage location or in the cloud).

10.4 Law practices should note that the storage of backups onsite does not protect the data against fire, physical theft and other force majeure events. Backups can also be stored in the cloud, but law practices should take time to understand how cloud-based backup services work, the jurisdiction in which the backup is stored, and the policies and technical organisational measures that the service provider has in place in relation to protecting the data.[46]

[44] NIST Special Publication 800-53, Controls AC-3, AC-17 and IA-2

[45] See also the Law Society of Singapore's Guidance Note 3.12.1 on Storage of Documents in Electronic Form dated 1 June 2018

[46] See also the section in this Guide on Cloud Computing

10.5 It is generally not feasible to store data indefinitely. At some point, data will be erased either because the data retention period has ended, or because the data is no longer required. Statutory limitation periods, when applicable, must be considered when ascertaining the data retention period. Data under litigation hold must be conserved for at least the prescribed period.

10.6 The general information technology position is that while a file may have been deleted from a computer such that it is no longer visible, it may still exist on the hard drive or in the computer's memory and may thus be recoverable. Law practices must ensure that their data sanitisation techniques are robust enough such that once data is deleted, it cannot be retrieved or reconstructed. There are companies that specialise in hardware destruction and law practices should consider using these companies to physically dispose of unwanted ICT hardware such as computers and printers.

Table 6: Data Management **a) Data Storage**			
		Good Practice	**Enhanced Practice**
1.	Use cryptographic mechanisms to prevent unauthorised modification of data in storage. Sensitive files, as well as entire devices, can be encrypted.[47]	√	
2.	Use software mechanisms to detect and log unauthorised changes to data in storage, and which will trigger audit alerts when such events occur.[48]		√
3.	Where law practices wish to outsource electronic data storage or wish to store electronic data in the cloud, due diligence must be carried out on the service provider and there should be a written outsourcing agreement in place, covering amongst other obligations, liability for breaches of data protection and confidentiality.		√
b) Data Transmission			
4.	When data is transmitted, ensure that the law practice's ICT systems protect the confidentiality and integrity of the transmitted data, for example, by implementing cryptographic mechanisms.[49]	√	

[47] NIST Special Publication 800-53, Controls SC-28 and SI-7
[48] Ibid.
[49] NIST Special Publication 800-53, Control SC-8

c) Data Backup[50]			
5.	Create regular backups of electronic data based on the law practice's data management policies and test backups regularly to verify information integrity and media reliability.[51]	√	
d) Data Destruction			
6.	Until the data or the electronic media containing the data is sanitised, protect the electronic media by placing it in secure storage such as locked cabinets or a controlled media library.[52]	√	
7.	Use data sanitisation techniques with strength and integrity, which are commensurate with the type and confidentiality of the information residing on the media, in order to remove information from the media such that the information cannot be retrieved or reconstructed.[53]	√	

11. Email

11.1 Law practices, like other types of businesses, rely heavily on emails to carry out their business activities. Emails are susceptible to a wide range of threats and cyber attacks. Some of these attacks include Business Email Compromise ("**BEC**"), phishing and other forms of malicious software attacks.

Table 7: Email			
		Good Practice	**Enhanced Practice**
1.	Install anti-malware software on the law practice's email servers and PCs. Keep the software updated and perform scans regularly.[54]	√	
2.	Install anti-spam software on the law practice's email servers to prevent spam emails from being sent to end	√	

[50] See also the Law Society of Singapore's Guidance Note 3.12.1 on Storage of Documents in Electronic Form dated 1 June 2018
[51] NIST Special Publication 800-53, Control CP-9
[52] NIST Special Publication 800-53, Control MP-4
[53] NIST Special Publication 800-53, Control MP-6
[54] PDPC SPD Guide at Table 12

	users, or to reduce the number of spam emails being sent.[55]		
3.	Encrypt or password protect attachments containing personal data that have a higher risk of adversely affecting the relevant individuals should the data be compromised. The password should be communicated separately. For encryption, review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure. For password protection, ensure that a strong password is used.[56]	√	
4.	If an email appears suspicious, verify the identity of the sender and the legitimacy of the email contents through an out-of-band method. For example, by: (i) performing a verification via telephone; or (ii) checking the sender's actual email address or return email address. Do not merely rely on the displayed name of the email address. Do not click on, open or execute suspicious attachments.[57]	√	
5.	Do not click on unrecognised links. At first glance, a link may appear legitimate. You can verify the actual link when you hover your mouse over the link embedded in the body of an email. If the displayed link address and the actual link address are different, do not click on the link.[58]	√	
6.	Implement Sender Policy Framework ("**SPF**"), Domain Keys Identified Mail ("**DKIM**") and Domain-based Message Authentication, Reporting and Conformance ("**DMARC**") email authentication methods and protocols.	√ (SPF)	√ (DKIM, DMARC)

12. Websites and Web Applications

12.1 Websites and web applications are often used to communicate or provide services. A website is generally used to disseminate information while a web application tends to be more interactive and may allow users to perform transactions. Since websites and web

[55] NIST Special Publication 800-53, Control SI-8
[56] PDPC SPD Guide at Table 12; NIST Special Publication 800-53, Control AC-7
[57] The Law Society of Singapore's Cybersecurity Readiness and Response Advisory dated 21 August 2018
[58] Ibid.

applications ultimately connect into a database and the database may contain personal and confidential data, precautions must be taken by a law practice against common forms of malicious activities on websites and web applications. An attack against a law practice's website can lead to defacement and denial-of-service, thereby enabling hackers to take control of the website and its web applications.

Table 8: Websites and Web Applications[59]			
		Good Practice	**Enhanced Practice**
1.	Perform validation of user input.	√	
2.	Ensure that files containing personal data or confidential data are not made available through a web application or web server. Even if the web link to such files is not published, it is still possible to discover and access these files.	√	
3.	Perform cookie data validation and URL validation to correspond with the session in use.	√	
4.	Do not allow the bypassing of user authentication to access personal data or confidential data.	√	
5.	Perform web application scanning and source code analysis in order to detect web vulnerabilities.		√
6.	Configure web servers to disallow the browsing of file directories.		√

13. Databases

13.1 Databases are used to store information such that it can be easily accessed, managed and updated. Database software and management systems may have different security features. In selecting a database product, law practices should consider the types of data they will be storing in the database and how this data will be accessed by their employees and clients (if access is provided to clients). If personal data is stored in a database, law practices should consider the types of personal data to be stored and the risk of harm or adverse impact on the relevant individuals should their personal data be compromised in the event of a breach.

[59] PDPC SPD Guide at pages 20-22

Table 9: Databases[60]			
		Good Practice	Enhanced Practice
1.	Access to the database must be securely controlled.	√	
2.	Ensure that the database is placed in the most secure network zone and segregated from the internet.	√	
3.	Encrypt personal data stored in a database, in particular data which has a higher risk of harm to or which would adversely impact the relevant individuals in the event that it is compromised.	√	
4.	Log all unauthorised and anomalous database activities, so that these activities can be tracked and analysed.		√

14. Cloud Computing

14.1 Cloud computing allows users to access software and ICT resources from any physical location via a network, typically the internet. This allows law practices to "rent" ICT resources such as servers and application software from providers of cloud services, instead of investing in their own onsite ICT resources.

14.2 There are various cloud service models including:

- **Software as a Service** ("**SaaS**"): Where the service provider makes available end-user applications;[61]
- **Platform as a Service** ("**PaaS**"): Where the service provider provides computing platforms for developing software or deploying and hosting applications; and
- **Infrastructure as a Service** ("**IaaS**"): Where the service provider provides processing power and storage, meaning that instead of investing in their own servers and other infrastructure, a law practice may rent a third party's computing and storage infrastructure.

14.3 Depending on the cloud service model, organisations need to relinquish varying levels of control over the personal and confidential data held by them. It is generally regarded

[60] PDPC SPD Guide at pages 18-19

[61] For example, instead of installing a word processing software to run on each solicitor's computer, a law practice may use, amongst others, an online word processing service provided by a cloud service provider

that with SaaS, organisations have the least control, and the degree of control increases with PaaS and IaaS.[62]

14.4 There are also various cloud deployment models such as[63]:

- **Private cloud**: Infrastructure is usually managed by the service provider but sometimes managed by the customer (i.e. a law practice). Infrastructure is located either onsite at the premises of the law practice or, more typically, on the service provider's premises. Data and services are accessible exclusively by the particular law practice and are not co-mingled or "mixed" with other customers' data;
- **Community cloud**: Serves members of a community with similar computing needs or requirements;
- **Public cloud**: Infrastructure is owned and managed by the service provider and located off-premises from the law practice. Although data and services are protected from unauthorised access, the infrastructure is accessible by a variety of customers; and
- **Hybrid cloud**: A combination of two or more of private cloud, community cloud or public cloud.

14.5 Law practices that adopt cloud services should be aware of the security and compliance challenges that are unique to cloud services. Where possible, law practices should consider the recommendations in this Guide for controls which they are able to manage directly. Law practices should also ensure that there is adequate security protection for personal and confidential data, and that their ethical and professional obligations are maintained.[64] Where a cloud service provider is unable to customise a service for a law practice, the law practice must understand the risks and issues arising, and decide if the security measures put in place by the cloud service provider are reasonable. Many cloud service providers will publish a list of the security measures that they offer. This can be helpful in assisting law practices to make a decision on whether the level of protection offered is sufficient for the personal and confidential data being stored in the cloud.[65]

[62] PDPC SPD Guide at page 25
[63] The Law Society of Singapore's Guidance Note 3.4.1 on Cloud Computing dated 10 March 2017 at Annex A
[64] For example, obligations pursuant to Rule 35(4) of the Legal Profession (Professional Conduct) Rules 2015
[65] PDPA SPD Guide at page 26; the Law Society of Singapore's Guidance Note 3.4.1 on Cloud Computing dated 10 March 2017 at paragraph 5

14.6 Law practices may refer to existing standards and guidelines such as ISO/IEC 27001:2013[66], ISO/IEC 27017:2015[67], ISO/IEC 27018:2019[68] and the Law Society of Singapore's Guidance Note 3.4.1 on Cloud Computing for additional guidance.

Table 10: Cloud Computing			
		Good Practice	**Enhanced Practice**
1.	Ensure that the cloud service provider is ISO certified for the relevant standards as necessary. Relevant standards may include ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019 or other recognised international standards. Obtain a copy of the certification for your records if possible.	√	
2.	Be aware of the security measures that your cloud service provider deploys to protect your law practice's data on the cloud.[69] For example, the cloud service provider may perform their own penetration tests and may be willing to share the results with you if asked.	√	
3.	Be aware of which laws apply to any personal data stored in the cloud and the jurisdiction in which this data is stored.	√	
4.	Where possible, negotiate that your cloud service provider conducts on-going third party audits and provides you with reports on these audits.		√
5.	Where law practices wish to outsource electronic data storage, or to store electronic data in the cloud, due diligence should be carried out on the service provider and there should be a written outsourcing agreement in place.	√	

[66] ISO/IEC 27001:2013 specifies the requirements for establishing, maintaining and continually improving an information security management system within the context of an organisation. More information can be found at Annex B

[67] ISO/IEC 27017:2015 provides guidelines for information security controls applicable to the provision and use of cloud services. More information can be found at Annex B

[68] ISO/IEC 27018:2019 relates to the protection of personally identifiable information and provides guidance on ensuring that cloud service providers offer suitable information security controls to protect the privacy of client data. More information can be found at Annex B

[69] The Law Society of Singapore's Guidance Note 3.4.1 on Cloud Computing dated 10 March 2017 at paragraph 47

6.	Refer to the Law Society of Singapore's Guidance Note 3.4.1 on Cloud Computing for additional controls that you can implement.	√	

Annex A – Glossary

Unless the context requires otherwise, the following definitions apply in this Guide.

Besides terms used in this Guide, this glossary also includes commonly used terms in the cybersecurity field, for readers' information.

Term	Meaning
access	The ability and means to communicate with or otherwise interact with a system in order to use system resources, either to handle information or to gain knowledge of the information the system contains.[70]
access control	A process by which use of system resources is regulated according to a security policy and is permitted only by authorised entities (e.g. users, programs, processes or other systems) according to that policy.[71]
administrator	A person that is responsible for configuring, maintaining and administering the target of evaluation (defined below) in a correct manner for maximum security.[72]
advanced persistent threat ("APT")	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g. cyber, physical and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of an organisation for the purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organisation, or to place itself in a position to do so in the future. Moreover, the APT pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.[73]
attack	1. An intentional act by which an entity attempts to evade security services and violate the security policy of a system; or 2. An actual assault on system security that derives from an intelligent threat.[74]
attribute	Information of a particular type concerning an identifiable system, entity or object.[75]

[70] IETF Security Glossary
[71] Ibid.
[72] Ibid.
[73] CNSS Glossary
[74] IETF Security Glossary
[75] Ibid.

audit log	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading up to an operation, procedure or event in a security-relevant transaction, from inception to final results.[76]
authenticate	Verify (i.e. establish the truth of) an attribute value claimed by or for a system entity or system resource. (See: authentication.)[77]
authentication	The process of verifying a claim that a system entity or system resource has a certain attribute value. (See: attribute, authenticate.)[78]
authorisation	An approval that is granted to a system entity to access a system resource.[79]
backup	A copy of files and programs made to facilitate recovery if necessary.[80]
blacklist	A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity. Also known as a "dirty word list".[81]
boundary	The physical or logical perimeter of a system.[82]
boundary protection	Monitoring and control of communications at the external boundary of an information system in order to prevent and detect malicious and other unauthorised communications. This can be done through the use of boundary protection devices (e.g. gateways, routers, firewalls, guards, encrypted tunnels and so on).[83]
boundary protection device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g. controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.[84]

[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] *NIST Special Publication 800-34, Revision 1. Contingency Planning Guide for Federal Information Systems*, listed at Annex B of this Guide
[81] *NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS)*, listed at Annex B of this Guide
[82] CNSS Glossary
[83] NIST Special Publication 800-53
[84] NIST Special Publication 800-53

brute force	A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries a large number of possible solutions to a problem.[85]
cloud computing	Cloud computing is a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[86]
compromise	See: data compromise, security compromise.[87]
computer network	A collection of interconnected host computers together with the subnetwork or internetwork through which they can exchange data.[88]
corruption	A type of threat action that undesirably alters system operation by adversely modifying system functions or data.[89]
countermeasure	An action, device, procedure or technique that meets or opposes (i.e. counters) a threat, vulnerability or attack, either by eliminating or preventing it, minimising the harm that it can cause, or discovering and reporting it so that corrective action can be taken.[90]
data	Information in a specific representation, usually as a sequence of symbols that have meaning.[91]
data compromise	A security incident in which information is exposed to potential unauthorised access, such that unauthorised disclosure, alteration or use of information might have occurred. (Compare: security compromise, security incident.)[92]
dictionary attack	An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.[93]
encryption	Cryptographic transformation of data (called "plain text") into a different form (called "cipher text") that conceals the data's original meaning and prevents the

[85] IETF Security Glossary
[86] *NIST Special Publication 800-145. The NIST Definition of Cloud Computing*, listed at Annex B of this Guide
[87] IETF Security Glossary
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Ibid.

	original form from being used. The corresponding reverse process is "decryption", a transformation that restores encrypted data to its original form.[94]
evaluation	Assessment of an information system against defined security criteria.[95]
information system	An organised assembly of computing and communication resources and procedures (i.e. equipment and services, together with their supporting infrastructure, facilities and personnel) that create, collect, record, process, store, transport, retrieve, display, disseminate, control or dispose of information to accomplish a specified set of functions.[96]
logic bomb	Malicious logic that activates when specified conditions are met. Usually intended to cause denial-of-service or otherwise damage system resources.[97]
login	An act by which a system user has its identity authenticated by the system.[98]
malicious code	Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of an information system. It could be in the form of a virus, worm, Trojan horse or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.[99]
malicious logic	Hardware, firmware or software that is intentionally included or inserted in a system for a harmful purpose.[100]
malware	See: malicious code and malicious logic.[101]
man-in-the-middle attack ("MitM attack")	A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.[102]
mobile code	Software programs or parts of programs which are obtained from remote information systems, transmitted across a network and executed on a local information system without explicit installation or execution by the recipient.[103]

[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] NIST Special Publication 800-53
[100] IETF Security Glossary
[101] NIST Special Publication 800-53
[102] IETF Security Glossary
[103] Ibid.

	Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript and so on.[104]
mobile device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (for example by wirelessly transmitting or receiving information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (for example, photograph, video, record or determine the location of) information, and/or built-in features for synchronising local data with remote locations. Examples include smart phones and tablets.[105]
multi-factor authentication	Authentication using two or more factors to achieve authentication. Factors may include: (i) something you know (e.g. a password or personal identification number); (ii) something you have (e.g. cryptographic identification devices or tokens); or (iii) something you are (e.g. biometrics).[106]
network	An information system comprised of a collection of interconnected nodes. (See: computer network.)[107]
out-of-band	Information transfer using a channel or method that is outside (i.e. separate from or different from) the main channel or normal method.[108]
password	A secret data value, usually a character string, that is presented to a system by a user to authenticate the user's identity.[109]
penetration test	A system test, often part of system certification, in which evaluators attempt to circumvent the security features of a system.[110]
phishing	A technique for attempting to acquire sensitive data such as bank account numbers, through a fraudulent solicitation via email or on a web site, in which the

[104] NIST Special Publication 800-53
[105] Ibid.
[106] Ibid.
[107] IETF Security Glossary
[108] Ibid.
[109] Ibid.
[110] Ibid.

	perpetrator masquerades as a legitimate business or reputable person. (See: social engineering.)[111]
sanitise	To delete sensitive data from a file, device or system.[112]
security	A system condition that results from the establishment and maintenance of measures to protect the system.[113]
security audit	An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policies and procedures, detect breaches in security services and recommend any changes that are indicated for countermeasures.[114]
security compromise	A security violation in which a system resource is exposed, or is potentially exposed, to unauthorised access. (Compare: data compromise.)[115]
security event	An occurrence in a system that is relevant to the security of the system. (See: security incident.)[116]
security incident	A security event that involves a security violation.[117]
security policy	A defined goal, course or method of action to guide and determine present and future decisions concerning security in a system.[118]
security posture	The security status of an enterprise's networks, information and systems based on information assurance resources (e.g. people, hardware, software and/or policies) and capabilities in place to manage the defence of the enterprise and to react as the situation changes.[119]
security service	A processing or communication service that is provided by a system to give a specific kind of protection to system resources.[120]
security violation	An act or event that disobeys or otherwise breaches security policy. (See: compromise, security incident.)[121]

[111] Ibid.
[112] Ibid.
[113] Ibid.
[114] Ibid.
[115] Ibid.
[116] Ibid.
[117] Ibid.
[118] Ibid.
[119] CNSS Glossary
[120] IETF Security Glossary
[121] Ibid.

server	A system entity that provides a service in response to requests from other system entities called clients.[122]
social engineering	Euphemism for non-technical or low-technology methods, often involving trickery or fraud, that are used to attack information systems. Example: phishing.[123]
software	Computer programs (which are stored in and executed by computer hardware) and associated data (which is stored in the same hardware) that may be dynamically written or modified during execution.[124]
spam	Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.[125]
special characters	Any non-alphanumeric character that can be rendered on a standard American English keyboard. Use of a specific special character may be application dependent. The list of 7-bit American Standard Code for Information Interchange special characters is as follows: ` ~! @ # $ % ^ & * ( ) _ + | } { " : ? > < [ ] \ ; ' , . / - =[126]
spoofing	1. Faking the sending address of a transmission in order to gain illegal entry into a secure system; or 2. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking and mimicking are forms of spoofing.[127]
spyware	Software that an intruder has installed surreptitiously on a networked computer in order to gather data from that computer and to send the data through the network to the intruder or some other interested party. (See: malicious logic, Trojan horse.)[128]
supply chain attack	Attacks that allow the adversary to utilise implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information

[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] CNSS Glossary
[126] Ibid.
[127] Ibid.
[128] IETF Security Glossary

	technology hardware, software, operating systems, peripherals (i.e. information technology products) or services at any point during its operation.[129]
system	Any organised assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (See: information system.)[130]
system entity	An active part of a system (for example, a person, a group of persons, an organisation, an automated process or a set of processes) that has a specific set of capabilities.[131]
system resource	1. Data contained in an information system; 2. A service provided by a system; 3. A system capacity, such as processing power or communication bandwidth; 4. An item of system equipment (e.g. hardware, firmware, software or documentation); or 5. A facility that houses system operations and equipment.[132]
system user	A system entity that consumes a product or service provided by the system, or that accesses and employs system resources to produce a product or service of the system. (See: access.)[133]
threat	Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image or reputation), organisational assets, individuals, other organisations or the nation through an information system via unauthorised access, destruction, disclosure, modification of information and/or denial-of-service.[134]

[129] CNSS Glossary
[130] Ibid.
[131] IETF Security Glossary
[132] Ibid.
[133] Ibid.
[134] *NIST Special Publication 800-30, Revision 1. Guide for Conducting Risk Assessments,* listed at Annex B of this Guide

target of evaluation ("TOE")	An information technology product or system that is the subject of a security evaluation, together with the product's associated administrator and user documentation.[135]
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting the legitimate authorisations of a system entity that invokes the program. (See: malware, spyware. Compare: logic bomb, virus, worm.)[136]
user	See: system user.
USB	Universal Serial Bus.
validate	Establish the soundness or correctness of a construct.[137]
virus	A self-replicating and usually hidden section of computer software (usually malicious logic) that propagates by infecting (i.e. inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself. It requires its host program to be running in order to be active.[138]
watering hole attack	In a watering hole attack, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly.[139]
web bug	Malicious code, invisible to a user, placed on web sites in such a way as to allow third parties to track the use of web servers by and to collect information about users, including their internet protocol address, host name, browser type and version, operating system name and version and web browser cookies.[140]
whaling	A specific kind of phishing that targets high-ranking members of organisations.[141]
whitelist	A list of discrete entities, such as hosts or applications, that are known to be benign and are approved for use within an organisation and/or information system. Also known as a "clean word list".[142]

[135] IETF Security Glossary
[136] Ibid.
[137] Ibid.
[138] Ibid.
[139] CNSS Glossary
[140] Ibid.
[141] Ibid.
[142] *NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems*, listed at Annex B of this Guide

worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network and which may consume system resources destructively. (See: virus.)[143]
zero day attack	An attack that exploits a previously unknown hardware, firmware or software vulnerability.[144]

[143] IETF Security Glossary
[144] CNSS Glossary

Annex B – Additional Resources

In addition to the publications listed at page 9 of this Guide, we include a list of additional resources on cybersecurity for readers who are interested in finding out more. These links are for information only and are not published by the Law Society of Singapore.

Websites on Advisories and Alerts

A. National Security Agency (United States). *Cybersecurity Advisories & Technical Guidance*. Available at: https://www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/ (Accessed 28 March 2020)

B. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (United States). *Alerts*. Available at: https://www.us-cert.gov/ncas/alerts (Accessed 28 March 2020)

Other Publications

C. The United States Department of Commerce, National Institute of Standards and Technology (2007). *NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS)*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (Accessed 28 March 2020)

D. The United States Department of Commerce, National Institute of Standards and Technology (2010). *NIST Special Publication 800-34, Revision 1. Contingency Planning Guide for Federal Information Systems*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf (Accessed 28 March 2020)

E. The United States Department of Commerce, National Institute of Standards and Technology (2011). *NIST Special Publication 800-145. The NIST Definition of Cloud Computing*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (Accessed 28 March 2020)

F. The United States Department of Commerce, National Institute of Standards and Technology (2011). *NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf (Accessed 28 March 2020)

G. The United States Department of Commerce, National Institute of Standards and Technology (2012). *NIST Special Publication 800-30, Revision 1. Guide for Conducting Risk Assessments*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Accessed 28 March 2020)

H. The United States Department of Commerce, National Institute of Standards and Technology (2014). *NIST Special Publication 800-88, Revision 1. Guidelines for Media Sanitization*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (Accessed 28 March 2020)

I. The United States Department of Commerce, National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Available at: https://doi.org/10.6028/NIST.CSWP.04162018 (Accessed 28 March 2020)

Standards

J. International Organization for Standardization (2013). *ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements*. Available at: https://www.iso.org/standard/54534.html (Accessed 28 March 2020)

K. International Organization for Standardization (2015). *ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Available at: https://www.iso.org/standard/43757.html (Accessed 28 March 2020)

L. International Organization for Standardization (2019). *ISO/IEC 27018:2019, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. Available at: https://www.iso.org/standard/76559.html (Accessed 28 March 2020)