University of New South Wales Law Research Series

CYBERSECURITY REGULATION IN SINGAPORE'S FINANCIAL SECTOR: PROTECTING FINTECH 'ANTS' IN A JUNGLE FULL OF 'ELEPHANTS'

ANTON DIDENKO

[2020] *UNSWLRS* 45

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Cybersecurity regulation in Singapore's financial sector: protecting FinTech 'ants' in a jungle full of 'elephants'

Anton N Didenko[*]

Abstract

The financial services sector is a prime target for cyber attackers: for four years in a row, it has been the single most attacked industry globally. It is thus only logical that Singapore's regulators have identified cybersecurity as the 'first priority' on the way towards a Smart Financial Centre and developed bespoke cybersecurity rules. This paper analyses the implications of Singapore's cybersecurity regulation for domestic FinTech firms and the impact of prospective international legal harmonisation in cyberspace. It argues that the increasing complexity and interconnectedness of the financial services ecosystem increases the risks of contagion and creates new entry points for cyber-attackers. This calls for additional measures to ensure cybersecurity of smaller and less sophisticated parties – FinTech innovators that may lack the resources and expertise to competently implement the 'default' cybersecurity rules and fend off advanced cyber-attacks. Internationally, Singapore is in an excellent spot to lead by example in the Asia-Pacific region, through developing and implementing novel regulatory approaches to cybersecurity – but true international harmonisation in this area remains only a distant possibility.

Keywords: cybersecurity, finance, FinTech, harmonisation, international, resilience Singapore.

I. Introduction

Technological innovation underpins Singapore's ambition to create a 'Smart Nation' – a 'leading economy powered by digital innovation' ("Transforming Singapore Through Technology," n.d.). The concept of Smart Nation is premised on the understanding that Singapore 'must embrace digitalisation and the benefits it brings' ("Smart Nation: The Way Forward," 2018). It is only natural for a country in which 98% of households have Internet access ("Infocomm Usage – Households and Individuals," 2020), almost 100% adults have a bank account (Demirguc-Kunt A. et al., 2018, p. 125) and mobile phone penetration rate exceeds 159% ("InfoComm and Media," n.d.).

Since digitalisation underpins all of Singapore's Strategic National Projects ("Transforming Singapore Through Technology," n.d.), it is no wonder that cybersecurity has become a national strategic priority. To illustrate this point: the five Asia-Pacific economies most dependent on internet use known as the 'Cyber Five' – South Korea, Australia, New Zealand, Japan and *Singapore* – were found, as a group, to be nine times more vulnerable to cyberattack compared to other economies in the region (Deloitte, 2016). Unsurprisingly, David Koh (2019), Chief Executive of the Cyber Security Agency of Singapore (CSA), has characterised cybersecurity as nothing less than 'an existential threat for Singapore'.

Singapore has a solid international reputation in the area of cybersecurity. It has been recognised by the International Telecommunication Union (ITU) as one of the leading jurisdictions in terms of cybersecurity engagement, as evidenced by the ITU Global Cybersecurity Index (GCI): Singapore topped the GCI ranking in 2017 (p. 59) and ranked 6th twice, in 2015 (p. 2) and 2018 (p. 62). This recognition is based on a range of regulatory and organisational initiatives, such as establishment of the CSA in 2015, adoption of the

[*] Research Fellow and Member, Centre for Law, Markets and Regulation, UNSW Sydney.

Cybersecurity Act in 2018, periodic nationwide cyber crisis management tests (such as Exercise Cyber Star), establishment of the first cybersecurity start-up hub ("ICE71," n.d.) in the region or the annual Singapore International Cyber Week.

Yet, despite these efforts, major cyber incidents cannot be eliminated, as illustrated by the data breach of SingHealth records that exposed personal data of over 1.5 million healthcare patients in 2018, leading to record-breaking financial penalties for failing to protect personal data (Yu, 2019). This recent wake-up call has demonstrated well that cybersecurity risk cannot be underestimated and left unchecked. As I wrote elsewhere, the main reasons for this lie in the very different nature of cyber threats, which are persistent, dynamic, intelligent, and adaptive (Didenko, 2020, p. 128).

A. Cybersecurity in the Smart Financial Centre

The financial sector is one of the key pillars of Singapore's Smart Nation initiative. This means that (quoting Ravi Menon (2015), the Managing Director of the Monetary Authority of Singapore (MAS)), '[a] Smart Nation needs a Smart Financial Centre'. However, the concept of a Smart Financial Centre is built entirely around digital infrastructure – one that can be vulnerable to cyber-attacks. Furthermore, the COVID-19 pandemic has further promoted the transition to digital payment methods, following the recommendation of the MAS (2020) to all individuals and businesses 'to use digital financial services and e-payments, and minimise visits to the premises of financial institutions' to support the elevated safe distancing measures announced by the Ministry of Health.

At the same time, financial institutions remain lucrative targets for cyber attackers all over the world. According to IBM (2019, pp. 16-17; 2020, p. 30), the finance and insurance sector has now been the single most attacked industry globally for four years in a row (with 19 per cent of all recorded attacks in 2018 and 17 percent of all attacks in the top 10 attacked industries in 2019). In this context, it is no surprise that cybersecurity is seen as the '*first priority* on [the] journey towards a Smart Financial Centre' (Menon, 2015). Furthermore, given Singapore's status as a major regional and global financial centre, there is little doubt that ripples from any potential disruption of Singapore's financial sector would be felt not only domestically, but also in many other parts of the world.

One of the biggest challenges in regulating cybersecurity in the financial sector is the increasing complexity and interconnectedness of the financial ecosystem, which is based on the interdependent operational network of a broad range of actors (banks, financial market infrastructures, and various service providers). This interconnectedness increases the risks of contagion and creates new entry points for attackers, thus calling for greater overall cybersecurity within the entire sector (and not just the largest institutions).

The same is of course true for Singapore. On the one hand, large financial institutions remain the dominant players in the financial sector. On the other hand, Singapore is one of the biggest FinTech hubs in the world: it is home to more than 1,000 FinTech firms, according to the MAS ("FinTech and Innovation," n.d.). In the constantly evolving financing landscape, incumbents and start-ups become connected on many levels. As a result, a successful cyberattack on a smaller firm could have a disproportionate effect on the entire financial system. In this context, cybersecurity becomes a priority not just for the larger financial institutions, but even for FinTech start-ups – or, using the analogy in the title, for both the 'elephants' and the 'ants'. The latter are understandably less likely to be fully equipped to fend off sophisticated cyber attackers compared to large financial institutions.

B. Paper structure

This paper discusses the implications of Singapore's cybersecurity regulation for domestic FinTech firms and the impact of prospective international legal harmonisation in cyberspace. It proceeds as follows.

Part II outlines the key existing rules governing cybersecurity in Singapore's financial sector. Part III analyses the recurring challenges in cybersecurity regulation in finance and their relevance for Singapore. Part IV outlines the specific cybersecurity challenges faced by FinTech firms in the context of the rules discussed in Part II. Part V focuses on the cross-border implications of cybersecurity regulation and the prospects of international harmonisation of rules governing cybersecurity in the financial sector. Part VI summarises the conclusions.

II. Singapore's key elements of cybersecurity regulatory framework in finance

Singapore's regulatory framework for cybersecurity in the financial sector consists of two layers: (i) general (cross-sector) regulation and (ii) cybersecurity rules specific to the financial sector.

A. General cybersecurity regulation

Singapore's overall vision, goals and priorities for cybersecurity are reflected in the 2016 Cybersecurity Strategy, which is built on four key pillars: (i) strengthening the resilience of critical information infrastructure, (ii) mobilising businesses and the community to improve the safety of cyberspace, (iii) development of a vibrant cybersecurity ecosystem comprising a skilled workforce, technologically-advanced companies and strong research collaborations and (iv) strong international partnerships.

The *Cybersecurity Act 2018* (s 24; Second Schedule) is the principal legislative instrument in the area of cybersecurity in Singapore and is one of the earliest statutes globally to focus entirely on the regulation of cybersecurity and to establish a mandatory licensing regime for two types of cybersecurity services in Singapore: (i) managed security operations centre monitoring and (i) penetration testing. The act (ss 4-5) created the office of Commissioner of Cybersecurity ('Commissioner') tasked with a broad range of functions, from overseeing and promoting the cybersecurity of computers and computer systems, to cyber threat monitoring, responding to cyber incidents, establishing cybersecurity standards and facilitating cyber awareness within Singapore generally. In addition, the Commissioner holds a broad range of powers to investigate and prevent cybersecurity incidents (*Cybersecurity Act 2018* Part 4).

One of the key powers of the Commissioner is the authority to classify computer systems as 'critical information infrastructure' (CII) – where the relevant computer systems are necessary for the continuous delivery of essential services and 'the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore' (*Cybersecurity Act 2018* s 7(1)). The list of the essential services includes 46 categories broken down into 11 groups: energy, info-communications, water, healthcare, banking and finance, security and emergency, aviation, land transport, maritime, government functioning and media. Importantly, the essential services in the financial sector are not limited to just banking or payments but include, among other things, securities- and derivatives-related services (such as trading, clearing and settlement) (*Cybersecurity Act 2018* First Schedule). While the list of CII and CII owners is kept secret for national security reasons ("Cybersecurity Act Frequently Asked Questions," n.d., p. 4), CII owners are subject to additional oversight, including binding directions issued by the Commissioner, obligations to report cyber incidents and periodic reviews (comprising annual cybersecurity risk

assessments and biennial cybersecurity audits) (*Cybersecurity Act 2018* ss 12, 14, 15). In addition, the Commissioner may organise mandatory cybersecurity exercises to test the state of readiness of CII owners for responding to cyber incidents (*Cybersecurity Act 2018* s 16).

The general provisions of the *Cybersecurity Act 2018* relating to the supervision of CII owners have been supplemented by the more detailed provisions of the *Cybersecurity (Critical Information Infrastructure) Regulations 2018* ('CII Regulations') and the *Cybersecurity Code of Practice for Critical Information Infrastructure 2018* ('Code of Practice'). The CII Regulations clarify the obligations of the Cybersecurity Act (such as deadlines for incident reporting and prescribed forms and channels of communication), while the Code of Practice (cl 1.3) sets out the minimum cybersecurity protection policies that must be implemented by owners of CII. Furthermore, the Code of Practice (cl 3.4.1) implements a 'comply or explain' approach to security by design: CII owners must adopt the *Security-by-Design Framework 2017* developed by the CSA or explain how and why certain parts of the framework are not applicable to the relevant CII. The *Security-by-Design Framework 2017* (ss 1.1-1.5) defines 'security-by-design' as 'an approach to software and hardware development that seeks to minimise systems vulnerabilities and reduce the attack surface through designing and building security in every phase of the [Systems Development Lifecycle]'. This approach – which is specific to cybersecurity – is contrasted with systems development that only applies security at a certain (eg commissioning) stage.

Other relevant legislation does not target cybersecurity per se but should nevertheless be considered as part of Singapore's broader cybersecurity framework. One such example is the *Personal Data Protection Act 2012* (s 24), which requires organisations to make 'reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks'. Another example is the *Computer Misuse Act 1993*, which criminalises various cyber offences, such as unauthorised access to, or modification of, computer material or unauthorised use of computer service and disclosure of access code (ss 3, 5, 6, 8).

B. Sector-specific cybersecurity regulation

The MAS, Singapore's financial regulator, plays the key role in regulating cybersecurity in the financial sector. The relevant regulatory framework includes a range of regulatory tools, including notices, guidelines, and circulars.

Since 2013, the MAS has issued a total of 11 Notices on Technology Risk Management (TRM) targeting different types of financial firms: banks (*MAS Notice 644*), merchant banks (*MAS Notice 1114*), credit card and charge card licensees (*MAS Notice 644A*), finance companies (*MAS Notice 830*), approved money brokers (*MAS Notice 912*), capital markets entities (eg exchanges, trade repositories and clearing houses) (*MAS Notice CMG-N02*), financial advisers (*MAS Notice FAA-N18*), insurers (other than captive insurers and marine mutual insurers) (*MAS Notice MAS 127*), registered insurance brokers (*MAS Notice MAS 506*), licensed trust companies (*MAS Notice TCA-N05*) and designated payment systems (*MAS Notice PSN05*). Although the TRM notices are separate instruments (as they are addressed to different entities), their content and structure is substantially similar. Each notice requires the regulated entity to identify its critical IT systems, minimise downtime of such systems (which should not exceed 4 hours over a period of 12 months) and protect customer information from unauthorised access or disclosure. If disruption cannot be prevented, the relevant firms should aim to recover each critical system within 4 hours but must first notify the MAS within 1 hour of discovery of the relevant incident and then provide a detailed root cause and impact analysis report within 14 days.

While the scope of the TRM Notices is quite narrow, more detailed guidance for financial institutions has been provided in the *Technology Risk Management Guidelines*. These Guidelines were issued by the MAS in 2013, but remain relevant today due to the in-built flexibility. Unlike the TRM Notices, the TRM Guidelines (cl 1.0.5, 2.0.1) are not legally binding and serve as a regulator-approved set of industry best practices that can be adjusted by the regulated entities as appropriate.

Strictly speaking, the scope of the TRM Notices and TRM Guidelines covers the whole range of technology-related risks. For example, the TRM Notices (eg *MAS Notice 644* cl 2) require reporting of any material 'system malfunction' (defined as any failure of a critical system, regardless of its origin), while the TRM Guidelines cover the entire IT risk management framework, including matters such as safeguarding information system assets (part 3), managing development of information systems (part 6) and protection of equipment from physical threats, such as fire (cl 10.3.3). At the same time, a number of provisions specifically target *cybersecurity* risks. For example, the TRM Notices explicitly require reporting of 'IT security incidents' (defined as events involving a 'security breach', such as hacking, intrusion or denial of service attacks). Similarly, the TRM Guidelines (cl 9.0.1) emphasise the need to combat 'cyber attacks' (including so-called middleman attacks – see cl 12.1.9) and propose bespoke measures to achieve this objective, such as two-factor authentication for all types of online financial systems and transaction-signing (cl 12.1.7).

Although cybersecurity risks possess a number of unique characteristics distinguishing them from other forms of technology risks and requiring different regulatory tools to address them (Didenko, 2020, p. 128), the above TRM Notices and Guidelines view cybersecurity issues through the lens of the broader 'technology risk' category – rather than as a standalone type of risk. Until recently, these instruments formed the core of the financial sector-specific cybersecurity regulation in Singapore, offering a harmonised but flexible guidance to the regulated entities and at the same time designating the MAS as the focal point for the sector-wide cyber incident data collection.

Over time, cybersecurity has been elevated to a standalone regulatory objective – as evidenced by the gradual decoupling of cybersecurity rules from the general operational risk management provisions. This change was reflected in a new trend – adoption of new financial sector regulations focusing specifically on cybersecurity. In 2015, the MAS issued a circular requiring all financial institutions to implement 'a comprehensive technology risk and cybersecurity training programme' for the board of directors (*MAS Circular SRD TR 03/2015*). Crucially, in this document cybersecurity matters were no longer considered as a mere sub-category of technology risks: throughout the document the two categories are treated as separate. Another 2015 circular focused entirely on cybersecurity – in particular, early detection and prompt investigation of cyber-attacks on financial institutions (*MAS Circular SRD TR 01/2015*).

This trend continued in 2019 with the adoption by the MAS of a set of bespoke cybersecurity regulations known as Notices on Cyber Hygiene (NCH). The new Notices (11 in total) came into force on 6 August 2020 and target a wide range of financial institutions in Singapore – with several exceptions, the list of covered financial institutions mirrors the TRM Notices. The main difference of the NCH from the earlier TRM Notices and Guidelines is that the NCH put *cybersecurity* front and centre and establish a set of mandatory requirements that financial institutions must put in place to manage cyber threats. In contrast, the TRM Notices put emphasis on reporting incidents and maintaining 'a high level of availability and recoverability in their critical systems, protect customer information from unauthorised access or disclosure, and to report relevant incidents to MAS' (MAS, 2019, p. 6).

The new requirements in the NCH are harmonised across the financial services sector and include six key obligations:

- protection of administrative accounts from unauthorised access;
- timely installation of security patches;
- maintaining and enforcing security standards for every system;
- restriction of all unauthorised network traffic within the entity's network perimeter;
- implementation of malware protection measures; and
- implementation of multi-factor authentication for certain accounts.

Although the cybersecurity practices listed in the NCH are mandatory, they remain quite flexible. First, they are specific as to the end-result only (in that they set out the desired outcome, leaving it up to the financial institutions themselves to determine the best course of action to achieve the objectives). For example, while the NCH require multi-factor authentication for administrative accounts, the Notices do not prescribe the 'best' combination of authentication tools (eg a password, a hardware-generated one-time access token or biometric data) or the appropriate number of such tools (while technically two would be enough, more can be used to satisfy the requirement). Similarly, the Notices require installation of security patches but do not prescribe the mandatory timeframe (only stating that such timeframe must be 'commensurate with the risks posed by each vulnerability') (eg, *MAS Notice MAS 655* para 4.2(a)). Second, the NCH offer alternative methods of compliance with certain provisions. For example, although each computer system must conform to a corresponding set of security standards, failure to comply with such standards is permissible so long as compensating controls have been put in place. Third, a financial institution is permitted to deviate from the requirements of the NCH so long as it is unable to exercise effective control over the computer system in question and it is 'unreasonable' to procure an alternative system provider allowing the financial institution to exercise such control (eg, *MAS Notice MAS 655* para 3.1).

Overall, the level of specificity of cybersecurity rules applicable to a financial institution in Singapore largely depends on whether such institution owns computer systems designated as CII under the *Cybersecurity Act 2018*. Unlike the sector-specific rules and guidelines issued by the MAS, which can be described as light touch and principles-based, the provisions applicable to CII are substantially more detailed. The underlying reasons and associated challenges are analysed in Part III.

III. Recurring challenges of cybersecurity regulation

The decoupling of cybersecurity rules from the general operational and technology risk management provisions and the increasing sophistication of the relevant regulatory regimes is an international trend that can be observed in a number of jurisdictions (such as the European Union, Hong Kong, Russia, and the USA). This means that both the MAS and the regulated financial institutions are facing challenges that are in no way unique to Singapore. These common challenges are examined in this Part III.

A. Need for legal certainty

Although cybersecurity is becoming formally separated from the other types of risk management, the corresponding rules often remain broad and obscure. In a number of cases, this separation has ended up being merely textual, without impacting the scope of the relevant rules. For example, in the EU, *Directive (EU) 2015/2366* refers to 'operational and security risks' throughout Article 95 but the difference between the two risk types is not clearly explained. Similarly, the *MAS Circular SRD TR 03/2015* focuses on 'the oversight of

technology risks *and cyber security*' (emphasis added) but does not elaborate on the relationship between the two concepts.

Another common obstacle towards greater legal certainty stems from the design of cybersecurity provisions, which largely remain principles based. As a result, the relevant regulations often contain abstract high-level requirements that lack specificity and cannot be readily applied without additional research or guidance. Examples of such provisions can be found in various EU instruments (such as *Regulation (EU) No 910/2014* (art 19(1)), *Directive (EU) 2016/1148* (arts 14(1), 16(1)) or *Regulation (EU) 2016/679* (art 32(1))), which include obligations to take *appropriate* technical and organisational *measures* to manage cyber risks, and obligations to achieve a *level* of security *appropriate* to the risks – without specifying what is considered 'appropriate' in each case. In Singapore, the 2019 Notices on Cyber Hygiene follow a similar approach. They impose only high-level obligations (eg to secure administrative accounts, to restrict unauthorised network traffic, to implement malware protection measures) but do not offer more specific guidance (eg, *MAS Notice MAS 655* paras 4.1, 4.4, 4.5). Likewise, security patches must be installed 'within a timeframe that is commensurate with the risks posed by each vulnerability' (eg, *MAS Notice MAS 655* para 4.2(a)).

There is, of course, a good reason why regulators may prefer high-level non-specific cybersecurity provisions. I explored the issue elsewhere (Didenko, 2020, pp. 138-139):

> The implication of a principles-based approach is clear: fear of over-regulation and inflexibility of setting out in advance the 'final destination' of a cybersecurity regime that may shift unexpectedly for reasons such as advances in technology. On the one hand, a set of overly prescriptive rules can backfire by providing potential attackers with information about cybersecurity controls implemented across the industry, effectively informing attackers on what must be done to circumvent those controls. On the other hand, regulated firms are very different in terms of their size, systemic importance, and technology applied, which demands a certain level of regulatory flexibility. These factors create a major challenge for regulators.

While a very high level cybersecurity requirements may help curb the risk of overregulation, the resulting uncertainty may be problematic for some financial firms: after all, the same general provisions can be interpreted broadly and narrowly at the same time, creating a standard of compliance that is not easily verifiable *ex ante*. To help address this issue, the MAS has published responses to certain frequently asked questions relating to its new Notices on Cyber Hygiene ("Frequently Asked Questions: Notice on Cyber Hygiene," n.d.). These responses provide some additional guidance but overall the NCH provisions may remain a source of uncertainty for financial institutions that will invite the regulated entities to proactively engage with the MAS to verify whether the relevant measures are in compliance with the NCH.

B. Limited reach of organisational measures

Since fear of overregulation limits the level of specificity of cybersecurity provisions, regulators commonly focus their attention on organisational matters, namely cyber governance. Cyber governance is a critical part of modern cybersecurity regimes in finance that includes five key components: (i) cybersecurity strategy, (ii) management roles and responsibilities, (iii) cyber risk awareness culture, (iv) architecture and standards, and (v) cybersecurity workforce (Basel Committee on Banking Supervision, 2018, p. 11). This means that building an effective cyber governance framework is a complex endeavour that goes beyond simple allocation of responsibility for cybersecurity within a regulated entity – the

key objective of cyber governance is to establish a forward-looking proactive approach to cybersecurity.

Today, cyber governance has become a core element of international cybersecurity guidelines issued by the G7 (2016) or the CPMI and IOSCO (2016, pp. 9-10) and has been integrated in a number of national regulatory regimes, particularly in the financial sector. Examples include the *Cybersecurity Requirements for Financial Services Companies* adopted by the New York State Department of Financial Services, which require regulated entities to maintain a 'cybersecurity *program*' (s 500.02) and a 'cybersecurity *policy*' (s 500.03), and the EU *Cyber Resilience Oversight Expectations*, which require each relevant financial market infrastructure, as a minimum, (i) to 'document its cyber resilience strategy', (ii) to have a 'cyber resilience framework' setting out cyber resilience objectives, risk tolerance and risk management practices, and (iii) appropriate board-level expertise, responsibility and accountability for cybersecurity (European Central Bank, 2018, ss 2.1.2.1(2), 2.1.2.1(6), 2.1.2.2).

Singapore's approach to cyber governance in the financial sector is aligned with the leading international practices: cyber governance requirements can be found in a range of instruments. The Notices on Cyber Hygiene require financial institutions to 'ensure that there is a written set of security standards for every system' (eg, *MAS Notice MAS 655* para 4.3(a)). The *MAS Circular SRD TR 03/2015* outlines the key responsibilities of the board of directors of a financial institutions in the area of cybersecurity:

> The FI's board of directors ("the Board") and senior management are responsible for the oversight of technology risks and cyber security. In particular, the Board needs to endorse the organisation's IT strategy and risk tolerance, and ensure that management focus, expertise and resources are brought to bear on this important topic. The Board also needs to ensure an appropriate accountability structure and organisational risk culture is in place to support effective implementation of the organisation's cyber resilience programme.

Cyber governance requirements become more complex if a financial institution is the owner of computer systems designated as 'critical information infrastructure' under the *Cybersecurity Act 2018* – the corresponding Code of Practice sets out a broad range of organisational requirements on CII owners, including obligations to (i) specify the organisational structure for the management of the CII's cybersecurity (cl 3.1.1), (ii) establish in writing a 'cybersecurity risk management framework' (cl 3.2.1), (iii) maintain a cybersecurity risk register in respect of the CII (cl 3.2.2), (iv) develop and review 'policies, standards and guidelines for managing cybersecurity risks and protecting CII against cybersecurity threats' (cl 3.3.1) and (v) adopt the CSA's Security by Design Framework (cl 3.4.1).

Some of the more recent cybersecurity frameworks overseas include a requirement to appoint a senior executive (often referred to as 'chief information security officer', or 'CISO') to facilitate effective implementation of cybersecurity programs. However, there is no uniformity in approaching this matter across jurisdictions. For instance, under the EU *Cyber Resilience Oversight Expectations* (p. 62) the CISO must be appointed in-house or on a group-wide basis, whereas the New York regulators allow financial services firms to use a CISO employed by a third-party service provider (*Cybersecurity Requirements for Financial Services Companies* s 500.04(a)). In Singapore, a somewhat similar requirement applies to owners of CII. Although the Code of Practice (cl 3.1.1) suggests that various cybersecurity functions may be split among different officers of the CII owner, the documentation allocating responsibility for cybersecurity matters must specify which person is 'ultimately

responsible' for compliance with the *Cybersecurity Act 2018* and any subsidiary legislation, codes of practice or standards issued pursuant to that Act.

The main challenge associated with cyber governance is control over its effective implementation: there may be a large gap between an organisation's cybersecurity program on paper and in practice. After all, existence of a robust formalised framework and allocation of corresponding responsibilities among staff may conceal substantial practical deficiencies, such as lack of resources to implement the documented measures or inadequate understanding of the relevant risks. Ultimately, cybersecurity in a financial institution is, to an extent, everyone's job.

C. Balancing flexibility and specificity of cyber defences

In contrast to cyber governance, which is quickly becoming the standard element of cybersecurity regulation, approaches to cyber defences (ie measures aimed at improving logical and physical security of a computer system) differ substantially across jurisdictions. At the EU level, specific (especially technology-related) requirements remain rare – and where specific cyber defences are listed, they are often given merely as examples, rather than mandatory requirements. The *Cyber Resilience Oversight Expectations* contain a detailed list of possible cyber defences, but almost all of them are listed for illustrative purposes: (i) tools to establish network boundary (s 2.3.2.1(10)), (ii) secure network protocols (cl 2.3.2.1(14)), (iii) intrusion detection or prevention systems, end point security solutions (cl 2.3.2.1(16)) or (iv) measures (such as network access control) to prevent unauthorised devices from connecting to the network (cl 2.3.2.1(24)). In contrast, the Bank of Russia has developed more detailed requirements concerning cyber defences, such as mandatory local certification of cryptographic modules and cryptographic information protection facilities, as well as minimal requirements to the standard of encryption (*CBR Instruction 3342-U*, *CBR Regulation 382-P*, *CBR Regulation 672-P*).

Singapore's current financial services framework does not prescribe specific cyber defences but provides certain examples. For example, the *MAS Circular SRD TR 01/2015* suggests that financial institutions 'could put in place decoys, sensors and/or other appropriate capabilities to detect anomalous traffic across systems within the internal networks'. The NCH (eg, *MAS Notice MAS 655* paras 4.4, 4.5, 4.6) require implementation of 'controls' restricting unauthorised network traffic, 'measures' to protect against malware and multi-factor authentication – leaving it up to the financial institutions to choose the appropriate 'controls', 'measures' and authentication modes. In its clarifications, the MAS has opted not to provide more specific guidance:

> MAS does not prescribe the types of device that FIs can implement at its network perimeter and to meet the Notice requirement. The types of device to be used would depend on the systems used, the IT operating environment and the associated risks. ("Frequently Asked Questions: Notice on Cyber Hygiene," n.d., p. 4)

As with cyber governance, additional guidance applies to owners of CII: the Code of Practice sets out limitations on accessing CII's physical interfaces (cl 5.1.4), requires establishment of security baseline configuration standards (cl 5.2.1), protection of remote connection channels (cl 5.3) and restriction of access to removable storage media (such as disabling external connection ports) (cl 5.4). Despite a large number of additional provisions, the requirements themselves remain largely principles-based and do not prescribe specific protections. For example, the Code of Practice merely lists in cl 5.2.2 the seven *principles* of security baseline configuration standards (leaving it up to the CII owner to develop the standards accordingly) and requires in cl 5.3.2(b) implementation of 'strong authentication techniques, transmission security, and message integrity' (but does not specify the types of authentication themselves).

The main underlying challenge in designing cybersecurity rules in the context of cyber defences lies in achieving the right balance between specificity (to avoid turning regulations into abstract declarations) and flexibility (to ensure that the rules do not need to be revised every time the relevant technology changes). This explains why many of the requirements only specify the desirable method of protection – leaving selection of the relevant tools in the hands of the regulated entity. This approach makes the relevant provisions both explicit (as to the method) and non-specific (as to the particular defences to be used) at the same time.

D. Effectiveness of cyber recovery

The accepted paradigm in cybersecurity is characterised by the 'assume breach' approach: businesses should assume that at some point a cyber-attack will inevitably penetrate the defences and succeed. Since not every breach can be prevented, regulators emphasise the importance of recovery measures by establishing data backup requirements. The relevant provisions can be vague and abstract (such as an obligation to 'at least provide for the establishment of backup facilities' in *Regulation (EU) No 648/2012*, art 79(2)) or, on the contrary, more specific about the measures taken and the time required to resume operations after breakdown (for example, article 15.5 of the *Regulation of The European Central Bank (EU) No 795/2014* requires (i) 'the use of a secondary site', (ii) resumption of critical system operations within two hours, (iii) capacity to settle all payments due by the end of the business day of disruption and (iv) annual testing and review of the continuity plan).

Singapore's MAS accepts in its *Circular SRD TR 01/2015* that 'not all successful attacks can be prevented' and stresses the importance of 'the speed at which [a financial institution] detects and responds to an intrusion'. In the same document, the regulator stresses the importance of a recovery strategy (known as a 'cyber breach response plan'):

> The presence of a well-thought-out and tested cyber breach response plan will assist [financial institutions] in coordinating effective response and recovery actions across the entire organisation and ensure that there is timely communication of key cyber breach details and findings to relevant stakeholders.

It is perhaps unsurprising that owners of CII are subject to more stringent requirements, which include the establishment of two backup plans: (i) a Cybersecurity Incident Response Plan ('CIRP') and (ii) a Crisis Communication Plan ('CCP') (Code of Practice, cl 7.1-7.2). The CIRP is designed to ensure business continuity, limit the effects of cyber incidents and transition to prompt recovery. The main objective of the CCP is to ensure coordinated and consistent communication between the CII owner (and its spokespersons and experts) and various third parties, including the media. Both plans must establish special response groups (known, respectively, as the Cyber Incident Response Team and the 'crisis communication team'). Furthermore, the Code of Practice requires continuous updating of the two backup plans: the CIRP must be reviewed at least every 24 months (cl 7.1.3), while the CCP needs to be tested once every 12 months (cl 7.2.4).

The recurring challenge in designing incident response plans – which is rarely adequately resolved in the cybersecurity regulations – is the need to ensure not just adequate functionality of backup systems, but also their *cyber resilience*. Indeed, a simple backup copy of an existing system may replicate its cyber vulnerabilities – thus making it easy for cyber attackers to take down the backup system as well. Cyber-attacks are different from natural disasters and other forms of operational disruption in that cyber threats are intelligent and may be prepared to target any backup system too. For this reason, regulations that focus purely on operational continuity, without considering the specific character of cyber threats, are likely to be of limited usefulness.

E. Pitfalls of cyber enforcement

While it is clear from the above discussion that designing cybersecurity rules is a difficult task, enforcement of such rules constitutes a separate challenge. Some of the underlying problems may depend on the regulatory structure: for example, the multiplicity of cybersecurity regulations in the EU makes possible coexistence of different enforcement regimes targeting essentially the same violations and creates unnecessary overlaps and possibility of simultaneous enforcement under different instruments for the same cyber incident.

Furthermore, selection and application of appropriate sanctions for violation of cybersecurity regulations remains a universal challenge, in the light of the unique features of cyber threats. It should be noted that one's ability to prevent a cyber-attack is not always the deciding factor in determining whether the attack will succeed. Some attackers (such as nation states) may possess resources vastly superior to the capability of their target, including cybersecurity intelligence and knowledge of undocumented features of cyber defences of the target. But if that is true, application of strict liability provisions may not always be justified. Another challenge stems from the earlier conclusion that cybersecurity regulations tend to be principles-based, which gives regulators substantial discretion in 'translating' the relevant principles into concrete enforcement action. Regardless of the quality of such enforcement, such *status quo* creates a standard of compliance that is not easily verifiable *ex ante*.

The recurring challenges discussed above are complex and have no easy solutions. Although the specific issues raised in this Part III are more significant in some jurisdictions compared to others, each of these five groups of regulatory challenges will remain relevant for Singapore's financial sector in the near future. However, the financial sector is not uniform: it is not limited to 'elephants' (large regulated financial institutions) and includes much smaller 'ants' (unregulated FinTech firms that disrupt the sector through technological innovation). The next Part IV argues that these 'ants' experience additional challenges when navigating cybersecurity regulations.

IV. Cybersecurity and FinTech disruptors

Let us now consider Singapore's existing cybersecurity framework from the perspective of smaller FinTech firms and identify the specific challenges particularly relevant for such 'ants'.

A. Relevance of cybersecurity regulation for FinTechs

The level of complexity of the financial ecosystem has been increasing rapidly in recent years. The financial sector of a developed economy like Singapore is an interdependent operational network of a broad range of actors (including banks, financial market infrastructures and various service providers). However, the interconnectedness of all of these actors multiplies the risks of contagion and creates additional entry points for attackers, thus calling for greater overall cybersecurity within the *entire financial sector* (and not just the largest institutions).

As an illustration, let us consider two major FinTech disruptors in Singapore at the time of writing: digital-only banks and the open banking initiative.

In January 2020, the MAS announced that it had received 21 applications for digital bank licences and planned to announce the successful applicants in June 2020. The COVID-19 pandemic prompted the regulator to extend the assessment period until the second half of 2020 (MAS, 2020). The launch of fully digital banks, which aims to further liberalise

banking, is particularly important from the cybersecurity perspective, given that the new banks are expected to carry out all of their operations in digital form.

Open banking is yet another initiative capable of multiplying cybersecurity risks. It is defined as 'the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities' (Basel Committee on Banking Supervision, 2019, p. 19). The objective of open banking is increased competition for financial services – but this competition is expected to result from sharing customer data among a broader number of entities, including FinTechs. In other words, open banking 'presents an opportunity for Fintechs to work with incumbent data organisations to create new data use cases' (EPA Asia, n.d., p. 3). However, this also means that each of the recipients of banking data can become a source of new cybersecurity risks:

> Data sharing brings many benefits, but also results in a bigger surface area for cyber attacks. Data collected by third parties, whether via screen scraping, reverse engineering or tokenised authentication methods through APIs, can be stolen or compromised. Furthermore, as more data is shared and with more parties, the possibility of a data breach increases and therefore effective data management has become more crucial. (Basel Committee on Banking Supervision, 2019, p. 6)

Open banking is already being implemented in a number of jurisdictions, including Australia, Brazil, Canada, China, Japan, Malaysia, Mexico, New Zealand, South Korea, United Kingdom and the USA – yet the mode of implementation of open banking differs from country to country. Singapore's approach to open banking has been described as 'organic': unlike jurisdictions with bespoke open banking legal frameworks (such as Australia or the United Kingdom), Singaporean regulators facilitate information sharing via APIs (application programming interfaces) – see "Finance-as-a-Service: API Playbook" (n.d.). At the same time, the use of APIs for the sharing of data is associated with multiple cybersecurity risks, as noted by the Basel Committee:

> Committee members have identified a variety of potential operational and cyber security issues related to the use of APIs, including data breaches, misuse, falsification, denial of service attacks and un-encrypted login. Other types of identified risks include infrastructure malfunction, speed of execution and operations, man-in-the-middle attack, token compromise and IP address spoofing. An API gateway could also be a single point of failure if not designed to be resilient. (Basel Committee on Banking Supervision, 2019, p. 18)

B. FinTech-related challenges of cybersecurity regulation

FinTech firms, whose business model is typically based on novel computer technologies or novel application of existing computer technologies, need to be resilient to cyber threats, to protect their know how and valuable customer data, as well as to prevent contagion in the increasingly interconnected financial sector. Smaller FinTech, especially start-ups, are particularly vulnerable for a number of reasons.

First, as discussed in Part III above, cybersecurity regulations tend to include abstract high-level requirements that lack specificity. In Singapore, this is especially true for cybersecurity regulations issued by the MAS, which, for example, require each covered financial institution to 'implement controls at its network perimeter to restrict all unauthorised network traffic' (eg, *MAS Notice MAS 655* para 4.4) but does not prescribe the types of network security devices that ensure compliance. The regulator clarifies that '[t]he types of device to be used

would depend on the systems used, the IT operating environment and the associated risks' ("Frequently Asked Questions: Notice on Cyber Hygiene," n.d., p. 4). Understanding what kinds of cyber defences are most appropriate in each case requires specialist expertise and resources – neither of which small FinTechs may possess. In other words, while the reasons for choosing high-level abstract cybersecurity requirements may be justified, FinTech 'ants' may struggle with deciphering such requirements, as well as with navigating and implementing the relevant technical standards (should they be prescribed by the regulations).

Second, it is worth noting that the existence of abstract cybersecurity requirements can be largely mitigated through regular contact with the regulator, which might assist with clarifying certain parameters. However, while such practice may be quite common among incumbents (such as banks), it may seem counterintuitive for FinTechs, which are not used to being in regular contact with supervisory authorities and often exhibit 'under-the-radar' attitude.

Third, many FinTech firms (particularly start-ups) have a very quick development cycle prior entering the market – which calls for greater alignment between the speed of growth and the level of cyber resilience. Since clear cybersecurity requirements may greatly assist with achieving this objective, a realignment of regulatory priorities may be useful. Under the current regulatory regime, owners of critical information infrastructure (which are likely to be major incumbents) are subject to detailed cybersecurity requirements found in the *Cybersecurity Act 2018*, the underlying CII Regulations and the Code of Practice – which is logical, given the strategic importance of safeguarding CII. On the other hand, other financial institutions follow more abstract rules, such as those found in the NCH. At the same time, despite their brevity, the requirements found in the NCH establish high cybersecurity standards (for example, on a literal reading, the obligation to 'ensure that every administrative account … is secured to prevent any unauthorised access to or use of such account' suggests that any unauthorised access constitutes a violation, despite the fact that prevention of certain targeted sophisticated attacks, eg those assisted by nation-states, may be unrealistic). Yet, despite these high standards, financial firms (including FinTechs) are not given more detailed guidance resembling the rules targeting CII owners. This raises the question of desirability of developing additional tools to improve cybersecurity among the less sophisticated FinTechs and thereby achieve a certain minimum level of cybersecurity expectations within the interconnected financial sector.

For many FinTechs such outsourcing is likely to be not only a source of convenience and cost-saving, but also a source of specialist knowledge they may lack inhouse. Smaller firms may not have the resources to analyse the programming code for vulnerabilities, or negotiate appropriate contractual terms with software vendors or developers, and are generally more prone to implementing 'black box' software that contains vulnerabilities and undocumented features. This may lead to information asymmetry between FinTechs and cybersecurity service providers engaged by them, as well as lack of effective control over the operations of such service providers.

Different solutions have been considered to address this issue. One involves the development of common cybersecurity resources to assist businesses with lower levels of cyber-preparedness. These may include setting up a purpose-built outsourcing entity controlled by the regulator – an initiative considered in February 2019 by the Russian authorities. The initiative was driven by two considerations. On the one hand, the regulators were concerned that engagement of major outsourcing cybersecurity companies may be too costly for smaller firms, which could get captured in specific digital architecture and be subjected to high tariffs (Goryacheva, Zhukova and Soldatskikh, 2019). On the other hand, it was unlikely that

financial institutions would entrust cybersecurity to specialised firms established or controlled by competitors (and so a regulator-driven approach seemed more attractive).

Singapore's *Cybersecurity Act 2018* (Part 5) offers an alternative response: mandatory licensing of cybersecurity service providers. Although the licensing regime is limited to just two forms of cybersecurity services (managed security operations centre monitoring service and penetration testing service) and it remains to be seen how the licensing framework will be implemented in practice, regulatory oversight may help alleviate some of the concerns of FinTechs engaging cybersecurity service providers. In addition, it is expected that the new licensing framework 'will be complemented by CSA's partnerships with the industry and professional association partners to establish voluntary accreditation regimes for cybersecurity professionals' ("Cybersecurity Act Frequently Asked Questions," n.d., p. 8). There is little doubt the above-mentioned concerns will remain important factors in determining the attractiveness of such partnerships for FinTechs.

V. Singapore and international harmonisation of cybersecurity frameworks

The Basel Committee on Banking Supervision (2018, p. 9) has argued that '[b]anks and supervisory authorities may benefit from harmonisation and standardisation'. The desirability of international harmonisation of cybersecurity rules can be explained by several factors. First, multiplicity of regulatory frameworks (as seen in the EU) can cause overlaps, whereby the same relationship is governed by more than one instrument – whether as a result of using inconsistent terminology or overlapping provisions found in sectoral and cross-sector (as well as local and federal) regulations. Second, the cross-border nature of cyber threats suggests that isolated, local measures to promote cybersecurity are unlikely to be efficient. Third, the scope and mode of harmonisation of cybersecurity rules adopted by major economies and leading financial centres can be implemented in other countries to improve the overall level cybersecurity at the global level – potentially opening a pathway towards adopting binding international instruments in the area.

Let us now briefly consider the relevance of these three factors for Singapore.

A. Regulatory overlaps

Regulatory overlaps in the cybersecurity context can take three main forms: (i) conflicts between domestic and international rules, (ii) multiple (national) regulatory regimes binding a single financial institution operating in more than one jurisdiction and (iii) overlapping domestic regulatory requirements. In the short term, the first category is less relevant, given the absence of binding international cybersecurity rules outside the EU. The second category is relevant for any financial institutions in Singapore operating on a cross-border basis and is unlikely to be resolved in the absence of harmonised international rules.

The third type of regulatory overlaps is most relevant for those jurisdictions where bespoke cross-sector cybersecurity rules have been adopted in addition to, but not as a replacement of, pre-existing sector-specific regulations. In Singapore, the recent *Cybersecurity Act 2018* has not replaced sectoral rules issued by the MAS – consequently, it is possible for a financial institution designated as a CII owner to be subject to overlapping sectoral and cross-sector requirements. While the corresponding clarifications have explained that sectoral regulators can set 'more stringent cybersecurity requirements' that would take precedence of the corresponding provisions of the *Cybersecurity Act 2018* ("Cybersecurity Act Frequently Asked Questions," n.d., p. 4), implementation of this approach may be challenging. For example, if both the sectoral and cross-sector regulations impose abstract principles-based requirements or cannot be easily compared for another reason, which one should be

considered 'more stringent'? One example of such challenge relates to reporting obligations. The CII Regulations (reg 5) require CII owners to notify the Commissioner within 2 hours after becoming aware of the occurrence of a cybersecurity incident. At the same time, the TRM Notices (eg *MAS Notice 644* cl 7) require financial institutions to notify the MAS within 1 hour following discovery of a cyber incident. On the one hand, the MAS requirements appear to be more stringent (since they give the relevant entity less time to report the breach). On the other hand, the two instruments use different language to describe reportable incidents and require the reporting entities to provide different sets of information. This raises the question whether, in the light of the above clarification, the requirements in the TRM Notices should replace the reporting obligations under the *Cybersecurity Act 2018* if the relevant financial institution has been designated as a CII owner.

B. Inefficiency of isolated measures

The cross-border nature of cyber threats suggests that isolated, local measures to promote cybersecurity are unlikely to be efficient. Singapore's status of a major international financial centre makes it a prime target for cyber attackers but also one of the main beneficiaries of international harmonisation of cybersecurity rules. At the time of writing, emergence of firm international rules to govern cybersecurity – whether general or sectoral – remains a distant possibility. Whereas a lot of exploratory work has taken place under the auspices of numerous international organisations – including the G7, the BCBS, OECD, FSB, IAIS, World Bank Group, IMF, CPMI and IOSCO (for more details, see Didenko, 2020, pp. 148-149) – there is an understandable gap between recommendations and so-called 'soft law' instruments and binding rules of international law. As a result, different jurisdictions are trying to solve the cybersecurity regulatory puzzle individually or as part of a regional bloc (as we have seen in the EU – see Didenko, 2020). These individual attempts to design cybersecurity regimes frequently rely on existing technical standards as a basis for cybersecurity rules and frameworks (FSB, 2017, p. 44). Different technical cybersecurity standards developed by the ISO and IEC, NIST, ISACA, CIS, ISF and FFIEC have been used by regulators as a basis for domestic regulatory standards and as a source of terminology (Didenko, 2020, pp. 149-150). In Singapore, the MAS has not mandated the use of any such standards, although the regulator does mention the CIS and NIST as sources of 'internationally recognised industry best practices' in its guidance ("Frequently Asked Questions: Notice on Cyber Hygiene," n.d., p. 3).

C. Leading by example

Over the years, through numerous initiatives, from the launch of the National Cybersecurity R&D Programme and establishment of the first cybersecurity start-up hub (ICE71) to conduct nationwide cyber crisis management tests, Singapore has earned the reputation of one of the leading jurisdictions in the area of cybersecurity engagement, as reflected in Singapore's consistently high ranking in ITU's Global Cybersecurity Index. As an early adopter of legislation focusing specifically on cybersecurity, Singapore is now in a perfect position to influence the development of cybersecurity rules in the region and possibly start the harmonisation process.

'We have a saying in Asia: when the elephants fight, the ants get trampled.' These words of David Koh (2019) aptly describe Singapore's pragmatic approach to international harmonisation of rules governing cyberspace. While the analogy with an 'ant' may be plausible from a geographical perspective, Singapore's role does not have to be reduced to that of an 'ant' in the development of a harmonised multilateral legal framework on

cybersecurity. By developing and implementing cutting edge cybersecurity rules, Singapore can lead by example.

Although proper international harmonisation of cybersecurity frameworks remains a distant possibility, the early steps in that direction have already been made. In September 2018, participants of the 3rd ASEAN Ministerial Conference on Cybersecurity in Singapore agreed to subscribe in-principle to the 11 recommendations for 'voluntary, non-binding norms, rules or principles of responsible behaviour of States' in cyber space listed in the United Nations Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. These early steps are certainly encouraging, but a lot more needs to be done before an international rules-based order in cyberspace can become a reality.

VI. Concluding remarks

The importance of a safe and secure financial sector for Singapore is hard to overestimate. On the one hand, it is a key component of the Smart Nation initiative. On the other hand, it remains the preferred target among cyber attackers. Singapore's recent regulatory reform aims to enhance the level of cyber resilience across the entire financial services sector, which remains a particularly challenging task, given the many underlying difficulties discussed in this paper.

This paper has also shown that ever-increasing complexity and interconnectedness of the financial services ecosystem increases the risks of contagion and creates new entry points for cyber-attackers. This calls for additional measures to ensure cybersecurity of smaller and less sophisticated parties – FinTech innovators that may lack the resources and expertise to competently implement the 'default' cybersecurity rules and fend off advanced cyber-attacks.

Finally, Singapore's commitment to the establishment of a rules-based order in cyberspace can be particularly useful for the local financial services sector, by reducing regulatory overlaps. Singapore is in an excellent spot to lead by example in the Asia-Pacific region, through developing and implementing novel regulatory approaches to cybersecurity – but true international harmonisation remains only a distant possibility.

References

"ICE71". (n.d.). Retrieved from https://ice71.sg/

Basel Committee on Banking Supervision. (2018). Cyber-Resilience: Range of Practices. Retrieved from https://www.bis.org/bcbs/publ/d454.pdf

Basel Committee on Banking Supervision. (2019). Report on open banking and application programming interfaces. Retrieved from https://www.bis.org/bcbs/publ/d486.pdf

CBR Instruction 3342-U. (2014)

CBR Regulation 382-P. (2012)

CBR Regulation 672-P. (2019)

Computer Misuse Act 1993. Retrieved from https://sso.agc.gov.sg/Act/CMA1993

CPMI and IOSCO. (2016). Guidance on Cyber Resilience for Financial Market Infrastructures. Retrieved from https://www.bis.org/cpmi/publ/d146.pdf

Cybersecurity Act 2018. Retrieved from https://sso.agc.gov.sg/Acts-Supp/9-2018/

Cybersecurity Act Frequently Asked Questions. (n.d.). Retrieved from https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/cybersecurity_act_faq.pdf

Cybersecurity Code of Practice for Critical Information Infrastructure. (2018). Retrieved from https://www.csa.gov.sg/-/media/csa/documents/legislation_cop/cybersecurity-code-of-practice-cii-dec-2019.pdf

Cybersecurity Requirements for Financial Services Companies. (2017). Retrieved from https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

Deloitte. (2016). Asia-Pacific Defense Outlook 2016: Defense in Four Domains. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-ap-defense-outlook-2016-160216.pdf

Demirguc-Kunt Asli, Klapper Leora, Singer Dorothe, Ansar Saniya, Hess Jake. (2018). The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Retrieved from http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf

Didenko Anton. (2020). Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond. *Uniform Law Review*. 25(1), 125-167. doi:10.1093/ulr/unaa006

Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337/35).

Directive (EU) 2016/1148 of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (OJ L 194/1).

EPA Asia. (n.d.) 'OpenBanking APAC – New world collaboration for payments'. Retrieved from https://www.emergingpaymentsasia.org/oba-report/

European Central Bank. (2018). Cyber Resilience Oversight Expectations for Financial Market Infrastructures. Retrieved from https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

Finance-as-a-Service: API Playbook. (n.d.). Retrieved from https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/API/ABSMASAPIPlaybook.pdf

FinTech and Innovation. (n.d.). Retrieved from https://www.mas.gov.sg/development/fintech

Frequently Asked Questions: Notice on Cyber Hygiene. (n.d.). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/FAQ---Notice-on-Cyber-Hygiene.pdf?la=en&hash=57A6DF29D6F73F30CF871883A95C99083241F67F

FSB. (2017). Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices. Retrieved from https://www.fsb.org/wp-content/uploads/P131017-2.pdf

G7. (2016). G7 Fundamental Elements of Cybersecurity for the Financial Sector'. Retrieved from https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

Goryacheva V, Zhukova K and Soldatskikh V. (2019, February 19). Кибербезопасность ушла на базу (Cybersecurity Has Gone to the Base). Retrieved from https://www.kommersant.ru/doc/3888889

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). Retrieved from https://undocs.org/A/70/174

IBM. (2019). X-Force Threat Intelligence Index 2019. Retrieved from https://www.ibm.com/downloads/cas/ZGB3ERYD

IBM. (2020). X-Force Threat Intelligence Index 2020. Retrieved from https://www.ibm.com/downloads/cas/DEDOLR3W

InfoComm and Media. (n.d.). Retrieved from https://www.singstat.gov.sg/find-data/search-by-theme/industry/infocomm-and-media/latest-data

Infocomm Usage – Households and Individuals. (2020). Retrieved from https://www.imda.gov.sg/infocomm-media-landscape/research-and-statistics/infocomm-usage-households-and-individuals

International Telecommunication Union. (2015). Global Cybersecurity Index & Cyberwellness Profiles. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

International Telecommunication Union. (2017). Global Cybersecurity Index 2017. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

International Telecommunication Union. (2019). Global Cybersecurity Index 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Koh David (2019, April 23). Keynote Speech at the International Conference on Cyber Engagement.

MAS Circular SRD TR 01/2015 'Early Detection of Cyber Intrusions'. (2015, August 24). Retrieved from https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRS-Circulars/SRD-TR-0115--Early-detection-of-cyber-intrusions.pdf

MAS Circular SRD TR 03/2015 'Technology Risk and Cyber Security Training for Board'. (2015, October 9). Retrieved from https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRS-Circulars/Circular-TR03-2015--Technology-Risk-and-Cyber-Security-Training-For-Boa.pdf

MAS Notice 1114. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-1114.pdf

MAS Notice 644. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-644.pdf

MAS Notice 644A (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-644A.pdf

MAS Notice 830 (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-830.pdf

MAS Notice 912. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-912.pdf

MAS Notice CMG-N02. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Securities-Futures-and-Fund-Management/Regulations-Guidance-and-Licensing/Notices/Notice-on-Technology-Risk-Management-CMGN02.pdf

MAS Notice FAA-N18. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-FAAN18.pdf

MAS Notice MAS 127. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-127.pdf

MAS Notice MAS 506. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-MAS-506.pdf

MAS Notice MAS 655 (2019, August 6). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/MAS-Notice-655.pdf

MAS Notice PSN05. (2019, December 5). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/PSN05-Notice-on-Technology-Risk-Management.pdf

MAS Notice TCA-N05. (2013, June 21). Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Notice-TCAN05.pdf

MAS. (2019, August 6). Draft Notice on Cyber Hygiene: Response to Feedback Received. Retrieved from https://www.mas.gov.sg/-/media/MAS/Notices/PDF/Responses-to-Feedback-Received-to-Draft-Notice-on-Cyber-Hygiene---6-August.pdf?la=en&hash=A1C7973B311BDDE11712B6FC64CB23BD284AA7E8

Menon Ravi. (2015, June 29). Keynote Speech 'A Smart Financial Centre'. Retrieved from https://www.mas.gov.sg/news/speeches/2015/a-smart-financial-centre

Menon Ravi. (2015, June 29). Keynote Speech 'A Smart Financial Centre'. Retrieved from https://www.mas.gov.sg/news/speeches/2015/a-smart-financial-centre

Monetary Authority of Singapore. (2020, April 09). MAS Extends Digital Bank Assessment Period in view of COVID-19 Pandemic. Retrieved from https://www.mas.gov.sg/news/media-releases/2020/mas-extends-digital-bank-assessment-period-in-view-of-covid-19-pandemic

Monetary Authority of Singapore. (2020, April 9). MAS Urges Use of Digital Finance and E-Payments to Support COVID-19 Safe Distancing Measures. Retrieved from https://www.mas.gov.sg/news/media-releases/2020/mas-urges-use-of-digital-finance-and-e-payments-to-support-covid-19-safe-distancing-measures

Personal Data Protection Act 2012. Retrieved from https://sso.agc.gov.sg/Act/PDPA2012

Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) No 648/2012 of 4 July 2012 on OTC Derivatives, Central Counterparties and Trade Repositories (OJ L 201/1).

Regulation (EU) No 910/2014 of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (OJ L 257/73).

Regulation of The European Central Bank (EU) No 795/2014 of 3 July 2014 on Oversight Requirements for Systemically Important Payment Systems (OJ L 217/16).

Security-by-Design Framework. (2017). Retrieved from https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf

Singapore's Cybersecurity Strategy. (2016). Retrieved from https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

Smart Nation: The Way Forward. (2018). Retrieved from https://www.smartnation.gov.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf?sfvrsn=3f5c2af8_2

Technology Risk Management Guidelines. (2013). Retrieved from https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines--21-June-2013.pdf

Transforming Singapore Through Technology. (n.d.). Retrieved from https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore

Transforming Singapore Through Technology. (n.d.). Retrieved from https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore

Yu Eileen. (2019, March 6). Hacker Group Behind SingHealth Data Breach Identified, Targeted Mainly Singapore Firms. Retrieved from https://www.zdnet.com/article/hacker-group-behind-singhealth-data-breach-identified-targeted-mainly-singapore-firms/