COUNTERING THE ESCALATION OF CYBERCRIME

Cybercrime is an ever-present danger in a world that is increasingly dependent on information and communication technology (ICT). Cybercrime affects us all. From individuals to governments, and boutique asset managers to global financial institutions, there is no target too big or small for cyber criminals.

In recent years the focus of cyber security has shifted. As attacks on governments and the institutions that enable our society to operate proliferate, lawmakers increasingly speak of cyber security not just in terms of an extension of managing operational risk, but rather as an active defence against domestic and foreign aggressors. As a result of this paradigm shift, these lawmakers have introduced regulations that specifically require firms to have cyber security plans in place.

On top of this, the unprecedented rise in remote work due to the Covid-19 pandemic and the subsequent lockdowns has resulted in a rising tide of cyber attacks on businesses and individuals as cyber criminals sought to take advantage of hastily implemented business continuity plans, unfamiliar processes and a lack of individual cyber security savvy and operational security.

With this background in mind, we look at some of the regulations in place and those in development, that attempt to help firms mitigate against the risks associated with the implementation of ICT, and the resultant threats this increased digitisation poses, due to enterprising bad actors.[1]

Global coordination

To begin with we'll look at the work undertaken by the Financial Stability Board (FSB), as well as three prominent and internationally-accepted cyber frameworks that the International Organization of Securities Commissions (IOSCO) refers to as the 'core standards'.[2]

International coordination by the FSB

At an international level, the FSB coordinates the work of national financial authorities and international standard-setting bodies, and develops and promotes the implementation of effective regulatory, supervisory and other financial sector policies in the interest of financial stability. Its cyber security remit is to support financial institutions and international standards organisations in addressing financial sector cyber resilience.

Following a public consultation in October 2020, the FSB published a toolkit of effective practices for financial institutions' cyber incident response and recovery.[3] The toolkit includes 49 practices for effective cyber incident response and recovery across seven components:

(i) Governance;
(ii) Planning and preparation;
(iii) Analysis;
(iv) Mitigation;
(v) Restoration and recovery;
(vi) Coordination and communication; and
(vii) Improvement.

The FSB's aim is to provide firms with the tools needed to ensure that their 'respond function' executes the appropriate activities in reaction to a detected or reported cyber incident, while their 'recover function' enables organisations to carry out the appropriate activities to restore any systems, capabilities, services, or operations that were impaired due to the cyber incident.

The toolkit publication is the latest in a series of papers issued by the FSB which are designed to promote cross-border cooperation[4], starting with the 2017 Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices.[5] This was followed in 2018 by the FSB's Cyber Lexicon which comprises a set of approximately 50 core terms related to cyber security and cyber resilience in the financial sector.

The Cyber Lexicon defines a cyber incident as "a cyber event that jeopardises the cyber security of an information system or the information the system processes, stores or transmits, or violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not."[6]

IOSCO's 'core standards'

1. NIST Cybersecurity Framework

First published in 2014 and intended for critical infrastructure operators, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) is a voluntary, risk-based framework of industry standards and best practices designed to help organisations manage cyber security risks.[7]

Although primarily a U.S. initiative (NIST is part of the U.S. Department of Commerce), the NIST Cybersecurity Framework has been adopted globally and enables organisations (irrespective of size, degree of cyber security risk or cyber security sophistication) to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

The NIST Cybersecurity Framework consists of three main components: the Core, Implementation Tiers, and Profiles.

The Core component provides a set of desired cyber security activities and outcomes using common language that is easy to understand. The Core guides organisations in managing and reducing their cyber security risks in a way that complements their existing cyber security and risk management processes.

The Implementation Tiers assist organisations by providing context on how they should view cyber security risk management. These tiers enable organisations to apply the appropriate level of rigor for their cyber security programme and are often used as a communication tool to discuss risk appetite, mission priority and budget.

The Profiles component refers to how organisations should align their organisational requirements and objectives, risk appetite, and resources against the desired outcomes of the Core component. Organisations use NIST Profiles in order to identify and prioritise opportunities for improving cyber security within an organisation.

2. CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures

Published in 2016, the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO Guidance)[8] was developed for financial market infrastructures (FMIs) to enhance their cyber resilience. The CPMI-IOSCO Guidance is principles-based, and outlines five primary risk management categories and three overarching components for organisations to address across their cyber resilience framework.

The five primary risk management categories are:

1. Governance;
2. Identification;
3. Protection;
4. Detection; and
5. Response and recovery.

The three overarching components cover:

- Testing;
- Situational awareness; and
- Learning and evolving.

The aim of the CPMI-IOSCO Guidance is to aid FMIs in pre-empting cyber attacks and, if the attacks are successful, responding rapidly and effectively to them, and achieving faster and safer target recovery objectives.

In addition, this framework aims to ensure a degree of uniformity in organisations' efforts to build resilience are similar from one country to another. As a result, the CPMI-IOSCO Guidance provides authorities with a set of internationally agreed-upon guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber risk.

3. ISO and IEC standards

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27000 family of information security management standards is a series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best-practice information security management.[9]

First published in the early 2000's, they have been developed to help organisations keep secure information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties.

The ISO/IEC 27000 family of standards can be applied to organisations of all sizes and in all sectors. They are purposefully not static, in order to ensure that as technology evolves, new standards are in turn developed to address the changing requirements of information security in different industries and environments.

A firm that has implemented one or more of the standards can be certified (or registered) as compliant if it successfully completes an audit carried out by a certification body that has been accredited by ISO. Certification demonstrates a firm's compliance with ISO/IEC standards to customers.

Relevant ISO/IEC cyber security standards include ISO/IEC 27001, which lays out the framework for creating a comprehensive IT security programme, and ISO/IEC 27002, which contains "best practices" for constructing such a programme.

Regional Approaches

Global initiatives such as the core standards described above, have their limitations in terms of universal applicability. As such, jurisdictions have developed, or are developing, local regulations and guidance to help organisations mange the risks that inevitably arise from ICT deployment.

The European collective resilience approach

On 20 December 2020, the European Commission (Commission) launched the EU Cybersecurity Strategy[10] (EU Strategy). The aim of the EU Strategy is to bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

Existing EU-level measures aimed at protecting key services and infrastructures from both cyber and physical risks are to be updated.

Building upon past EU achievements, the EU Strategy contains proposals for regulatory, investment and policy initiatives, in three areas:

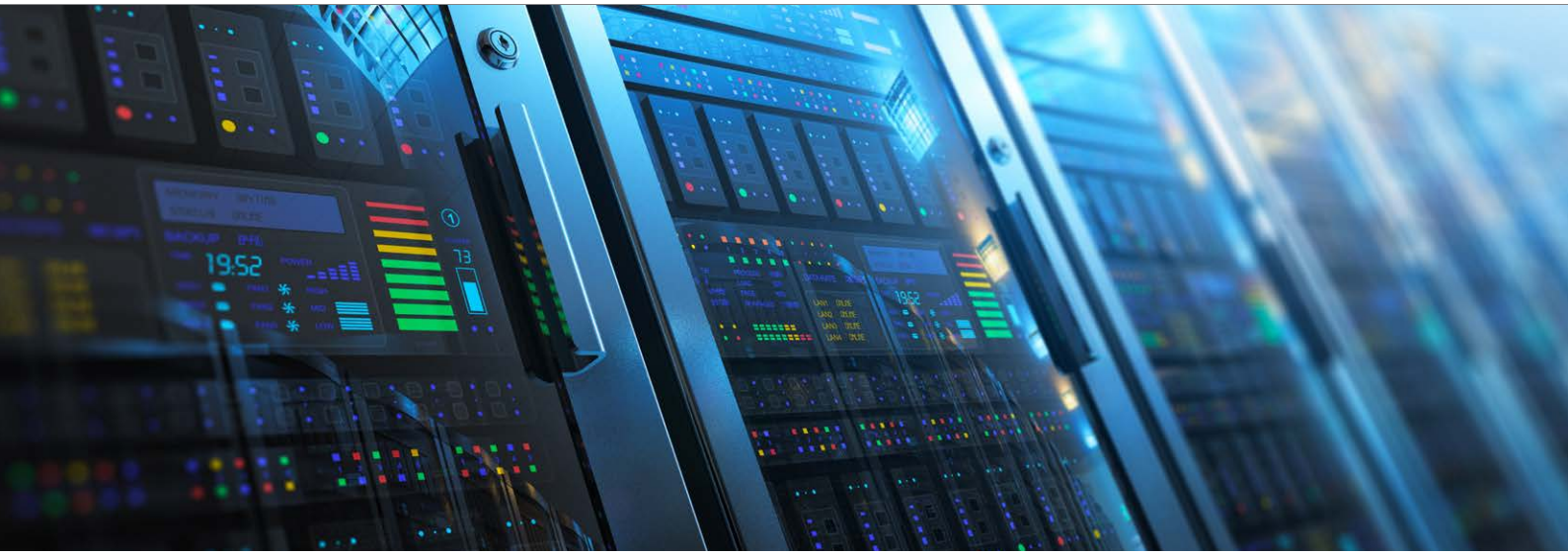
1. **Resilience, technological sovereignty and leadership**
   - » The Commission proposes to reform the rules on network and information systems security, under a Directive which lays out measures meant to ensure a high common level of cybersecurity across the Union (NIS 2), in order to increase the level of cyber resilience in both the public and private sectors. In order to respond to the expanding cyber threats as a result of increased digitalisation and interconnectedness NIS 2 will cover medium and large entities from more sectors than were covered by the first NIS Directive, based on their economic and societal criticality.
   - » Its aim is to strengthen security requirements for companies, address supply chain security, streamline reporting obligations, introduce more stringent supervisory measures for national authorities, impose stricter enforcement requirements and harmonise sanctions regimes across Member States.
   - » In addition, NIS 2 will expand information sharing and cooperation on cyber crisis management at both the national and EU level.
   - » The Commission also proposes to launch a network of Security Operations Centres (SOC) across the EU, powered by artificial intelligence (AI), which will constitute a real 'cyber security shield' for the EU. This SOC network would enable EU member states to better detect signs of a cyber attack early enough to enable proactive action, before damage occurs. Additional measures will include providing dedicated support to small and medium-sized enterprises (SMEs), under Digital Innovation Hubs, as well as increased efforts to upskill the workforce, attract and retain the best cybersecurity talent, and invest in research and innovation that is open, competitive and based on excellence.
2. **Building operational capacity to prevent, deter and respond**
   - » The Commission is preparing a new Joint Cyber Unit through a collaborative process with EU Member States, which is intended to strengthen cooperation between EU bodies and Member State authorities responsible for preventing, deterring and responding to cyber attacks, including civilian, law enforcement, diplomatic and cyber defence communities. The EU will also aim to further enhance cyber defence cooperation and develop state-of-the-art cyber defence capabilities, building on the work of the European Defence Agency and encouraging Member States to make full use of the Permanent Structured Cooperation and the European Defence Fund.
3. **Advancing a global and open cyberspace through increased cooperation**
   - » The EU will expand work with international partners to strengthen the rules-based global order, promote international security and stability in cyberspace, and protect human rights and fundamental freedoms online. It will advance international norms and standards that reflect these EU core values, by working with international partners in the United Nations and other relevant fora. The EU will further strengthen its EU Cyber Diplomacy Toolbox, and increase cyber capacity-building efforts to third countries by developing an EU External Cyber Capacity Building Agenda. Cyber dialogues with third countries, regional and international organisations, as well as the multi-stakeholder community will all be intensified. The EU will also form an EU Cyber Diplomacy Network around the world to promote its vision of cyberspace.

U.S. has its own way

Unlike the EU, the U.S. does not usually legislate holistically, with over a dozen regulatory bodies and federal agencies that either oversee or shape policies, leaving individual agencies to regulate their own sectors. This is unlikely to change despite increased federal government oversight following an advanced persistent threat alert issued by the Cybersecurity & Infrastructure Security Agency in December 2020.[11] That's not to say that the U.S. has no level of national cyber security coordination, however.

The FSSCC

In 2002, U.S. financial institutions established the Financial Services Sector Coordinating Council (FSSCC) to work collaboratively with key government agencies while coordinating critical infrastructure and security activities within the financial services industry.



In October 2018, the FSSCC published its Cybersecurity Profile (the Profile).[12] This document details a framework that integrates widely-used standards and supervisory expectations to help guide financial institutions in developing and maintaining cyber security risk management programmes.

Currently maintained by the Cyber Risk Institute[13], the Profile is billed as "the benchmark for cyber risk assessment" and offers a unified approach for assessing cyber security risk, by consolidating 2,300 plus regulations into 277 diagnostic statements. The Profile is based on common ISO/IEC and NIST categories (identify, protect, detect, respond, and recover) and adds two categories specific to the financial industry (governance and dependency management).

The Profile uses a series of questions to determine a firm's systemic impact, places them in one of four tiers, and tailors the resulting questionnaire accordingly with Tier 1 firms with a national or super-national impact subject to all 277 statements, while Tier 4 firms (deemed to have only a localised impact) are subject to only 137 of these diagnostic statements.

The CFTC and SEC approaches

In July 2020, the Commodity Futures Trading Commission (CFTC) named the Profile as one of several standardised approaches for assessing and improving cyber security preparedness that firms regulated by the CFTC may consider using. The CFTC believes firms that adopt a standardised approach to cyber risk assessment are better able to track their progress over time and to share information and best practices with their peers and regulators. However, the CFTC stresses that reliance on tools such as the Profile does not replace its examination programmes and its risk based approach to cyber security oversight.

The basis for the Securities and Exchange Commission (SEC) oversight of cyber security in asset management is guidance paper 2015-02, issued in April 2015, which shoehorns cyber security into pre-existing principles.[14] For example, Regulation S-P requires registered broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." Guidance paper 2015-02 states that SEC Staff will view any theft of customer data as a result of a failure in cyber security as a breach of that Regulation.

The information securities rule package

In May 2019, the North American Securities Administrators Association (NASAA) adopted an information security model rule package. This information security model rule package has three components:

1. A requirement that investment advisers adopt specific policies and procedures regarding information security (both physical security and cyber security), and that these advisors deliver their firm's privacy policy annually to clients[15];
2. An amendment to the existing investment adviser NASAA model recordkeeping requirements rule to require that investment advisers maintain these records[16]; and
3. Amendments to the existing investment adviser NASAA Unethical Business Practices of Investment Advisers, Investment Adviser Representatives, and Federal Covered Advisers[17] and NASAA Prohibited Conduct of Investment Advisers, Investment Adviser Representatives and Federal Covered Investment Advisers Model Rule USA 2002 502(b)[18] model rules to include failing to establish, maintain, and enforce a required policy or procedure to the list of unethical business practices/prohibited conduct.

US Department of Labor

On 14 April 2021, the US Department of Labor announced new guidance for retirement plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cyber security, including tips on how to protect the retirement benefits of American workers. This guidance is directed at plan sponsors and fiduciaries who are regulated by the Employee Retirement Income Security Act (ERISA), as well as plan participants and beneficiaries.

The guidance comes in three forms:

- Tips for Hiring a Service Provider[19]: Helps plan sponsors and fiduciaries prudently select a service provider with strong cyber security practices and monitor their activities, as ERISA requires.

- Cybersecurity Program Best Practices[20]: Assists plan fiduciaries and record-keepers in their responsibilities to manage cyber security risks.

- Online Security Tips[21]: Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

The guidance complements the Employee Benefits Security Administration's regulations on electronic records and disclosures to plan participants and beneficiaries. These regulations include provisions on ensuring that electronic recordkeeping systems have reasonable controls, that adequate records management practices are in place, and that electronic disclosure systems include measures intended to protect Personally Identifiable Information.

The winds of change blow from the east

It would be a mistake to assume progress in cyber security regulation is being driven primarily from the EU or the US. In Asia, a region that is so often first to adopt new technologies, regulators are also trying to ensure organisations have the processes in place to minimise cyber risks.

Hong Kong

In November 2020, the Hong Kong Monetary Authority (HKMA) announced the launch of an upgraded Cybersecurity Fortification Initiative (CFI) 2.0.[22]

The HKMA originally introduced the CFI in 2016, with the aim of raising the cyber resilience of Hong Kong's banking system. The initiative is underpinned by three pillars:

- **The Cyber Resilience Assessment Framework (C-RAF)** – a risk based framework for authorised institutions to assess their own risk profiles and benchmark the level of defence and resilience that would be required to accord appropriate protection against cyber attacks;
- **The Professional Development Programme (PDP)** – a localised certification scheme and training programme for cyber security professionals developed by the HKMA in collaboration with the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute. The PDP is an integrated and well-structured programme to train and nurture cybersecurity practitioners in the banking and information technology industries, and to enhance their cybersecurity awareness and technical capabilities of conducting cyber resilience assessments and simulation testing; and
- **The Cyber Intelligence Sharing Platform (CISP)** – this provides an effective infrastructure for sharing intelligence on cyber attacks. The timeliness of receiving alerts or warnings from a commonly shared intelligence platform can help the banking sector as a whole to prepare for possible cyber attacks. The platform was launched by the HKMA in collaboration with the Applied Science and Technology Research Institute and the Hong Kong Association of Banks.

To cope with the fast-changing cybersecurity landscape, the HKMA has recently completed a review of the CFI through market studies, interviews, and surveys, followed by extensive industry consultation.

The results of the review showed that the banking industry is strongly supportive of the CFI. Over 90% of banks found the C-RAF useful, especially for identifying previously unrecognised gaps. All of the banks surveyed found the Intelligence-led Cyber Attack Simulation Testing (iCAST) helpful in preparing for cyber attacks.

Taking into account the financial industry's feedback during the review, the CFI has been enhanced with a view to streamlining the cyber resilience assessment process while maintaining effective control standards that are commensurate with the latest technology trends. The CFI 2.0 came into effect on 1 January 2021 and will be phased in between September 2021 and December 2022.

Singapore

In January 2021, the Monetary Authority of Singapore (MAS) issued revised Technology Risk Management Guidelines (MAS Guidelines) to keep pace with emerging technologies and shifts in the cyber threat landscape.[23]

The MAS Guidelines are a set of best practices that provide financial institutions (FIs) with guidance on the oversight of technology risk management, practices and controls to address technology and cyber risks. MAS expects FIs to observe the guidelines as this will be considered in MAS' risk assessment of the FIs. They are designed to complement the Notice on Technology Risk Management and Notice on Cyber Hygiene.

The MAS Guidelines focus on addressing technology and cyber risks in an environment in which FIs are increasingly adopting cloud technologies, application programming interfaces and rapid software development. The MAS Guidelines reinforce the importance of incorporating security controls as part of FIs' technology development and delivery lifecycle, as well as in the deployment of emerging technologies.

The MAS Guidelines set out the following enhanced risk mitigation strategies for FIs:

- To establish a robust process for the timely analysis and sharing of cyber threat intelligence within the financial ecosystem; and
- To conduct cyber exercises to allow FIs to stress test their cyber defences by simulating the attack tactics, techniques and procedures used by real-world attackers.

In light of FIs' growing reliance on third party service providers, the MAS Guidelines set out the expectation that FIs exercise strong oversight of arrangements with third party service providers, to ensure system resilience as well as maintain data confidentiality and integrity.

The revised MAS Guidelines provide additional guidance for firms on the roles and responsibilities of the board of directors and senior management:

- The board and senior management should ensure that a Chief Information Officer and a Chief Information Security Officer, with the requisite experience and expertise, are appointed and accountable for managing technology and cyber risks; and
- The board should include members with the relevant knowledge to provide effective oversight of technology and cyber risks.

UK – the journey to come – 2021 and beyond

The UK is now looking at developing its own regulations and standards, now that it is no longer part of the European Union.

Bank of England and the Prudential Regulation Authority

In the UK, regulators have taken an active approach to establishing whether firms have tried and tested cyber defences in place.

Working with CREST, the international not-for-profit accreditation and certification body that represents and supports the technical information security market, the Bank of England (BoE) developed CBEST, a framework to deliver controlled, bespoke, intelligence-led cyber security tests that replicate the behaviours of threat actors.

In addition to developing CBEST, the BoE has indicated that it will conduct regular cyber stress tests to see how firms perform against severe but plausible scenarios. Such is the importance of the cyber stress tests to the stability of financial markets that temporary changes to the BoE's approach in May 2020 were not publicly announced as it was felt this would inadvertently increase the risk of cyber attacks during a period of heightened cyber risk in the Covid-19 environment. The BoE eventually publicised the changes in March 2021 after reintroducing the full stress test regime.

In a recent BoE speech[24] Lyndon Nelson, Deputy CEO, discussed what he referred to as 'basic cyber hygiene'. Examples of some of the cyber hygiene issues Mr Nelson mentioned during his speech included:

- Shortcomings in vulnerability management and information storage;
- Poor configuration of IT infrastructure; and
- Poor user account and password management.

Key takeaways

The message from global regulators as discussed in this piece reveal some important realities: Cyber risks are growing and an organisation's approach to the likelihood of a cyber attack should not be 'if' but 'when' it will happen.

Wherever in the world your firm is based, it is advisable to have a comprehensive cyber security process. This includes knowing your cyber risks and having the tools in place to mitigate against them. The existing and proposed regulations and guidance coming from regulators around the world will help organisations develop more secure systems and will aid in the dissemination of information, solutions and best practice between jurisdictions.

However, ultimately it will be down to individual firms to ensure their ICT systems, and those of their suppliers, are secure. Your operational resilience plans must take into account the ever-evolving sophistication of cyber attacks and how to recover from them.

Finally, your people, from the top down, must be aware of their role in protecting themselves and your firm from threat actors.

1. For more on bad actors please see our webpage Who Are The Threat Actors at www.citibank.com.
2. IOSCO 'core standards' consist of: the NIST Cybersecurity Framework, the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures and the ISO/IEC 27000 family of information security management standards.
3. See Effective Practices for Cyber Incident Response and Recovery Final Report at www.fsb.org.
4. See Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices at www.fsb.org.
5. See Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices at www.fsb.org.
6. See Cyber Lexicon at www.fsb.org.
7. See NIST Cybersecurity Framework at www.nist.gov.
8. See Guidance on cyber resilience for financial market infrastructures at www.iosco.org.
9. For more information on the ISO 27000 family see www.iso.org.
10. See New EU Cybersecurity Strategy at ec.europa.eu.
11. See Alert (AA20-352A) at us-cert.cisa.gov.
12. See the Profile at cyberriskinstitute.org.
13. A coalition of financial institutions and trade associations.
14. See guidance update 2015-02 at www.sec.gov.
15. See investment adviser information security and privacy rule at www.nasaa.org.
16. See NASAA recordkeeping requirements for investment advisers model rule 203(a)-2 (amended May 2019) at www.nasaa.org.
17. See NASAA Unethical Business Practices Of Investment Advisers, Investment Adviser Representatives, And Federal Covered Advisers Model Rule 102(a)(4)-1 (amended May 2019) at www.nasaa.org.
18. See NASAA Prohibited Conduct of Investment Advisers, Investment Adviser Representatives and Federal Covered Investment Advisers Model Rule USA 2002 502(b) (amended May 2019) at www.nasaa.org.
19. See Tips for Hiring a Service Provider with Strong Cybersecurity Practices at www.dol.gov.
20. See Cybersecurity Program Best Practices at www.dol.gov.
21. See Online Security Tips at www.dol.gov.
22. See Cybersecurity Fortification Initiative (CFI) at www.hkma.gov.hk.
23. See Technology Risk Management Guidelines at www.mas.gov.sg.
24. Cyber Risk: 2015 to 2027 and the Penrose steps – speech by Lyndon Nelson | Bank of England.

Please contact for further details:

David Morrison
Global Head of Trustee and Fiduciary Services
david.m.morrison@citi.com
+44 (0) 20 7500 8021

Ann-Marie Roddie
Head of Product Development Fiduciary Services
annmarie.roddie@citi.com
+44 (1534) 60-8201

Amanda Hale
Head of Regulatory Services
amanda.jayne.hale@citi.com
+44 (0)20 7508 0178

Caroline Chan
APAC Head of Fiduciary Business
caroline.mary.chan@citi.com
+852 2868 7973

Shane Baily
EMEA Head of Trustee and Fiduciary Services
UK, Ireland and Luxembourg
shane.baily@citi.com
+353 (1) 622 6297

Jan-Olov Nord
EMEA Head of Fiduciary Services
Netherlands and Sweden
janolov.nord@citi.com
+31 20 651 4313

www.citibank.com/mss

GRA34778 08/21