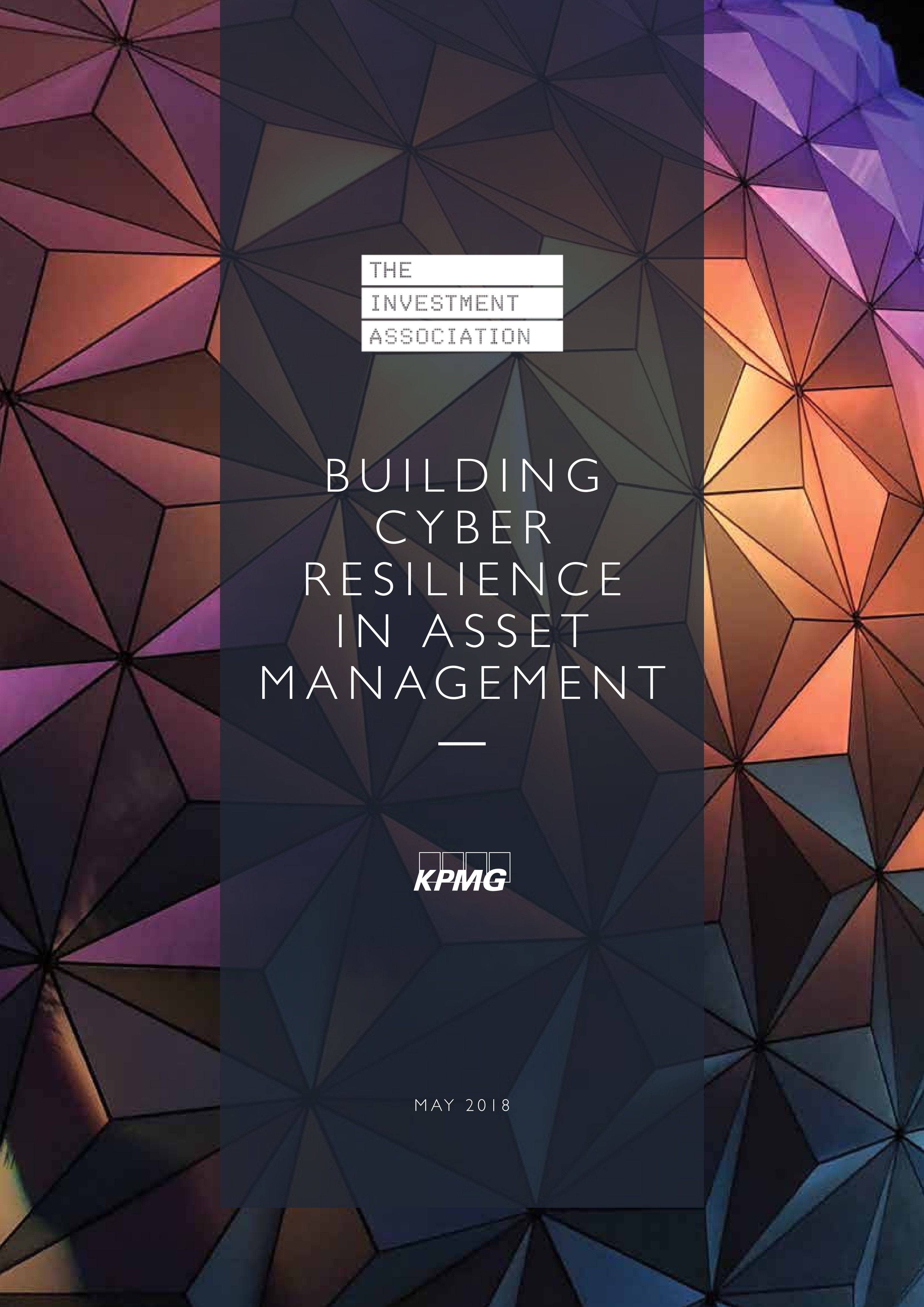


THE
INVESTMENT
ASSOCIATION

BUILDING CYBER RESILIENCE IN ASSET MANAGEMENT

KPMG

MAY 2018

CONTENTS

FOREWORD

Cyber crime is a growing global industry now estimated to make criminals over $400 billion a year[1]. Cyber attackers are becoming more determined and more skilled than ever. Highly professional and highly motivated, they are continually developing new techniques and seeking new targets to attack. With just 39% of asset management CEOs consulted in KPMG's 2017 CEO survey saying they are fully prepared for a cyber event[2], now is the time for the industry to act decisively to protect their clients' data and their own reputations.

Technology is transforming the asset management industry at a speed and scale never seen before. The global regulatory environment for cyber security and privacy is becoming more complex and fragmented. This combined with the regular cases of high profile breaches being reported in the media, creates an issue that requires attention in the Board room.

The Investment Association and KPMG have jointly written this paper to provide an overview of the key cyber security risks facing the industry, offer guidance on the steps organisations can take to protect their business from cyber-attack, share thoughts on the power of an industry wide response and present cyber security risks around future disruptive technologies.

There are two key drivers behind publishing this paper:

Firstly, as we have seen, cyber attacks are real and are happening to a growing number of businesses regardless of their industry. The asset management sector's cousins in banking and insurance can vouch for this, and are generally far ahead in configuring their defences, in part because of the greater threat they have faced to date. However, asset management firms are not immune to a cyber-attack and are likely to be an increasing target given the significant value of assets under management.

Secondly, regulators and authorities are increasing their focus on cyber security as an issue and looking for assurances that businesses are taking the necessary steps to prevent breaches. The UK government strongly supports the Investment Association's development of an Asset Management Cyber Security Strategy[3]. It called on stakeholders to "participate in this work and engage with industry to provide a new level of protection for asset management and FinTech firms."

A 2017 review of cyber security commissioned by the US Securities and Exchange Commission found that asset management firms had generally improved their cyber security standing. The review found that while most firms had now implemented cyber security policies, many did not enforce them properly[4].

Now is the time for asset managers, as individual firms and as a community, to get serious about cyber security. This paper should help you consider cyber security risks and the practical steps you can take to protect your business. After all, your customers are putting their trust in you to safeguard their investments and their data.

EXECUTIVE SUMMARY

The key messages in this report are:

Cyber Security Threat Landscape: cyber-attacks are most likely to come from organised crime groups or from a malicious insider. Malicious data disclosure, CEO fraud / business email compromise and ransomware are particular threats. Risks can materialise across the entire value chain of an asset manager, with particular risks around the theft of client data as well as payment fraud. There are also risks to client data processed by third party administrators and custodian banks, while the use of cloud service providers needs to be carefully managed. Criminals are becoming more creative in how they attack systems including using increasingly automated methods to attack large numbers of organisations using customised malware.

Building a Cyber Resilient Business: there are key actions which help build an effective cyber security capability. The Board must be fully engaged and have an understanding of cyber security issues, and establish clear accountability for action. It is vital to map the cyber security risks facing the business, check whether the current cyber security capabilities deal with those risks and agree the organisation's cyber security risk appetite and tolerance levels. There should be the technical ability and processes to detect, respond and recover from incidents; and cyber security risks should be managed effectively across the supply chain. But most importantly of all, employees should be educated around cyber security risks and good behaviours.

Collaborative Action: the sector needs to work more collaboratively as a community and benefit from the economies of scale and pooling of expertise across the industry. By sharing threat intelligence, collaborating to create solutions and working together on response and recovery best practices, we can help everyone improve.

Future Technology Disruptors: the speed at which technology is transforming the asset management industry adds an interesting new dimension to the cyber security risk landscape. Digital channels, the cloud, artificial intelligence and robotics, blockchain – the industry is becoming increasingly dependent on technology at the core of its business. This creates fantastic ways for asset managers to differentiate their business, grow revenues and increase profits but also creates opportunities for cyber criminals. The potential cyber security risks need to be understood, managed and mitigated – in some cases this will require new and innovative approaches to security controls.

1: CYBER SECURITY THREAT LANDSCAPE

The first section in this paper highlights the broad and growing array of cyber security risks confronting the asset management industry and the business drivers for managing these effectively.

We have produced a cyber security risk radar showing the current threats, identified the ways in which these threats could potentially impact the asset management value chain and highlighted examples of cyber security incidents that have occurred. The section concludes with a view on the future direction of cyber threats.

BUSINESS DRIVERS

There are a number of compelling business drivers for proactively understanding and managing cyber security risks.

Cyber security is, perhaps more than anything else, an issue of brand and reputation. Organisations that have secure systems and manage customer data effectively will uphold their perception in the market as trusted players. By contrast, organisations that have fallen foul of a cyber-attack have often suffered significant reputational damage. This is especially the case for businesses that have not managed the fall-out well. Poor handling of communications can further damage customer confidence that has already been dented by the breach occurring in the first place.

Cyber security incidents can also disrupt business operations for a significant period of time beyond the initial incident itself. We only need to look at the WannaCry ransomware episode where some businesses were offline for days and weeks afterwards[5].

This causes further frustration, anger and loss of customer confidence, which can be hard to win back. Organisations have to be able to show that they have sustainable operations.

Looking at other sectors such as banking, some organisations have taken a proactive approach to increase customer confidence and engagement, such as by offering or promoting awareness of anti-virus software products. This extension into end-consumer territory enhances their own standing as cyber aware organisations and shifts their cyber security strategy from brand protecting to brand enhancing.

In today's digital and interconnected world, businesses rely on each other across partnerships and supply chains. It is essential that everyone in the chain can rely on each other and there is a vested interest for all parties to be safe and secure.

Moreover, the penalties from regulators for falling short are only set to rise. The General Data Protection Regulation (GDPR), for example, could see fines of up to 4% of global turnover for lax privacy protection[6].

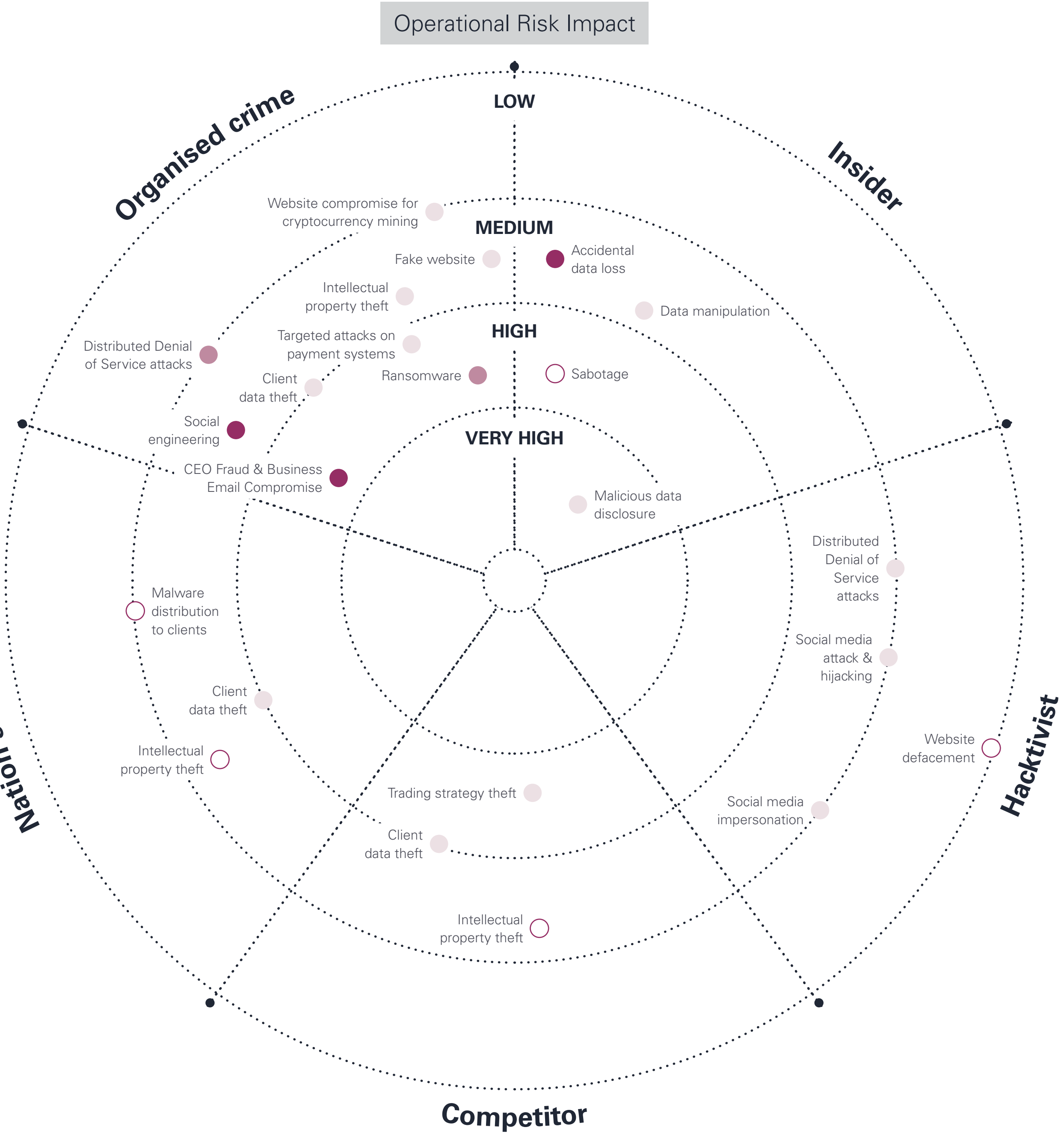
Organisations that have suffered cyber security breaches may face significant fines from authorities, compounded by a hit to their share price. Compliance with standards is a licence to do business, not a choice. This can be challenging, especially in the heavily regulated financial services sector – but the best organisations will rise to that challenge.

Quite simply, managing cyber security effectively can turn a threat into an operational and strategic strength and drive a competitive advantage.

CYBER SECURITY RISK RADAR

Based on KPMG's experience and analysis of publicly available incidents we have produced a cyber security risk radar. Figure 1 shows the cyber security risks posed from five threat actors to the asset management industry. The main cyber security risks originate from attacks by organised criminals or from people within an organisation (e.g. employees, contractors or third parties). Very high operational impact could materialise from a malicious data disclosure, with other high profile impacts coming from CEO fraud / business email compromise and ransomware.

Figure 1: Cyber security risk radar



Operational Risk Impact
LOW
MEDIUM
HIGH
VERY HIGH
Organised crime
Insider
Hacktivist
Competitor
Nation state
Website compromise for cryptocurrency mining
Fake website
Accidental data loss
Intellectual property theft
Data manipulation
Distributed Denial of Service attacks
Targeted attacks on payment systems
Ransomware
Sabotage
Client data theft
Social engineering
CEO Fraud & Business Email Compromise
Malicious data disclosure
Distributed Denial of Service attacks
Malware distribution to clients
Social media attack & hijacking
Client data theft
Intellectual property theft
Website defacement
Trading strategy theft
Social media impersonation
Client data theft
Intellectual property theft

Source KPMG International

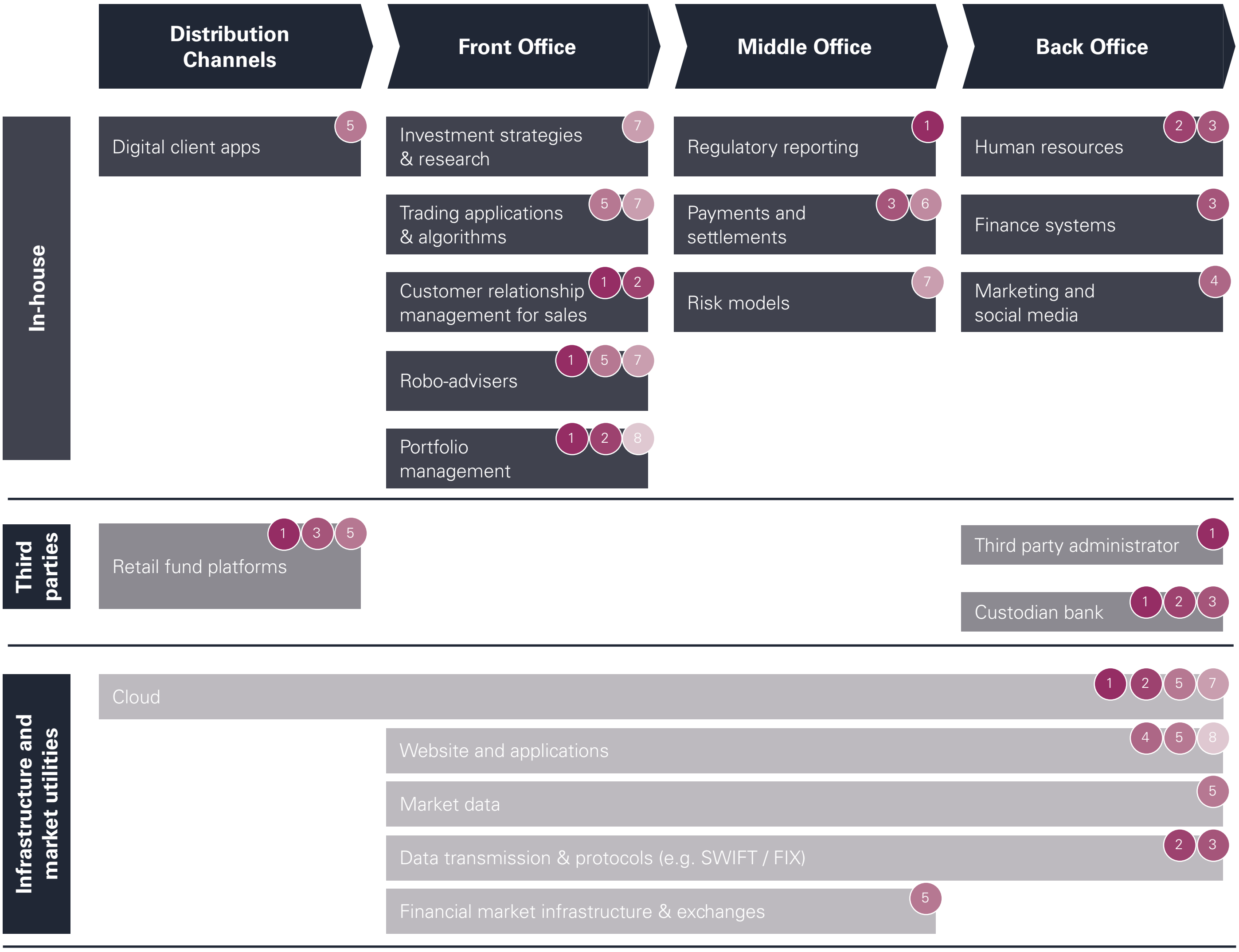
Probability key

● Very likely
● Likely
● Possible
○ Remote

CYBER SECURITY THREATS TO THE ASSET MANAGEMENT SECTOR

This section presents a view on how cyber security threats could potentially impact the asset management value chain. Figure 2 below presents an end-to-end example of an asset management firm's value chain, with the key cyber security threats overlaid.

Figure 2: Cyber security risks to the asset management value chain



Distribution Channels

Front Office

Middle Office

Back Office

In-house

Digital client apps 5

Investment strategies & research 7

Trading applications & algorithms 5 7

Customer relationship management for sales 1 2

Robo-advisers 1 5 7

Portfolio management 1 2 8

Regulatory reporting 1

Payments and settlements 3 6

Risk models 7

Human resources 2 3

Finance systems 3

Marketing and social media 4

Third parties

Retail fund platforms 1 3 5

Third party administrator 1

Custodian bank 1 2 3

Infrastructure and market utilities

Cloud 1 2 5 7

Website and applications 4 5 8

Market data 5

Data transmission & protocols (e.g. SWIFT / FIX) 2 3

Financial market infrastructure & exchanges 5

Key

1 Client data theft

2 Data loss

3 Payment fraud

4 Website or social media attack

5 DDoS attack

6 CEO fraud

7 IP theft

8 Ransomware

Source KPMG International

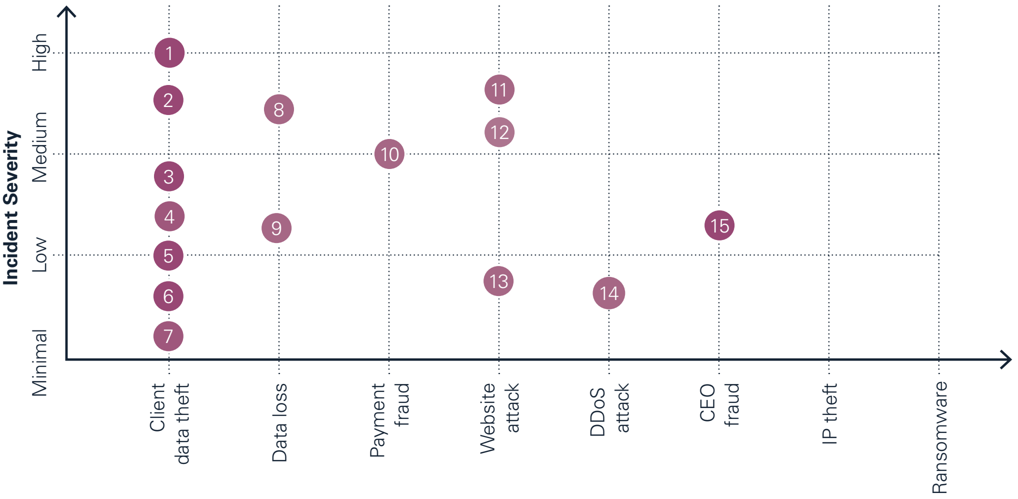
Some of the key observations from Figure 2 are:

- Cyber security risks can materialise across the entire value chain and in particular there are risks around the theft of client data and intellectual property as well as payment fraud.
- Given the significant use of third parties and the complex web of providers, there are risks to client data as this is processed by third party administrators and custodian banks.
- There is an increased use of, and dependency on, infrastructure and market utilities. In particular, there are multiple cyber security risks associated with the use of cloud service providers to support across the entire value chain that should be managed.

EXAMPLES OF CYBER SECURITY INCIDENTS

Figure 3 depicts a selection of publicly reported cyber security incidents based on KPMG's research of online sources. It shows incidents suffered by asset management firms or other closely related industries, and highlights that the overwhelming majority of incidents suffered have involved client data theft or data loss more generally.

Figure 3: Cyber security incidents in the asset management and related industries



Source KPMG International

A summary of the medium to high severity incidents is provided below:

(1) **Online Brokerage**: hackers accessed 4.6 million clients' personal information including their contact details

(2) **Global Bank – Wealth Management Division:** forced to pay $1 million fine after an employee stole data about approximately 730,000 customer accounts

(8) **Wealth Manager:** details about thousands of the firm's clients were leaked, not stolen, to investigative journalists resulting in high-profile news stories

(10) **Investment Firm:** an employee sent $495,000 to a bank account in Hong Kong after being tricked by a spear-phishing email claiming to be from a company executive

See Figure 3 references in the appendix

(11) **Investment Managers:** criminals copied names, logos, addresses and created look-alike websites of multiple high-profile asset management firms. 95 dubious website appeared on the Financial Conduct Authority's warning page for clones in the first nine months of 2017

(12) **Online Brokers:** a hacker broke into at least four different brokerage firms to make fraudulent trades aimed at manipulating share prices so they could benefit from this. The attack caused $1 million in losses for the victims

FUTURE CYBER SECURITY THREATS

At KPMG we expect the cyber threat of the future to evolve, become more sophisticated and use innovative new attack techniques. We have set out below some of the potential threats for the future:

Criminals are becoming more creative in how they attack financial systems - we can expect more attempts to initiate fraudulent payment transactions typically with a social engineering element[7], as well as growing interest in core financial infrastructure including payment and trading platform gateways. Growing demands are being placed on fraud control and anti-money-laundering systems to block these transactions, while customers demand instantaneous financial transfers. If these controls fail, there could be many more $100 million pay-outs from cyber-attacks.

Cyber-attacks will become increasingly automated, allowing criminals to target large numbers of organisations both for extortion and fraud purposes, using malware and attack methods which are increasingly tailored to the organisation being targeted.

This will place growing demands on cyber security teams to quickly respond to the changing threat, and place a premium on good threat intelligence and cyber security operations. The KPMG 'Clarity on Cyber Security' survey of Swiss organisations found that only 4% of respondents declared that they use artificial intelligence (AI) to protect themselves from cyber threats, whilst 40% expect that attackers will begin to use AI to enhance their attack capability in the future[8].

The shadow of state activity will lengthen - as countries invest to develop their cyber espionage and offensive capabilities, we will see more signs of their activities. Disclosures of high end techniques used by nations will continue, fuelling the opportunistic re-purposing of these vulnerabilities by less sophisticated states and organised crime groups.

2: BUILDING A CYBER RESILIENT BUSINESS

In this section we look at some of the key cyber security themes required to build an effective capability and outline the key frameworks that can help you structure your approach.

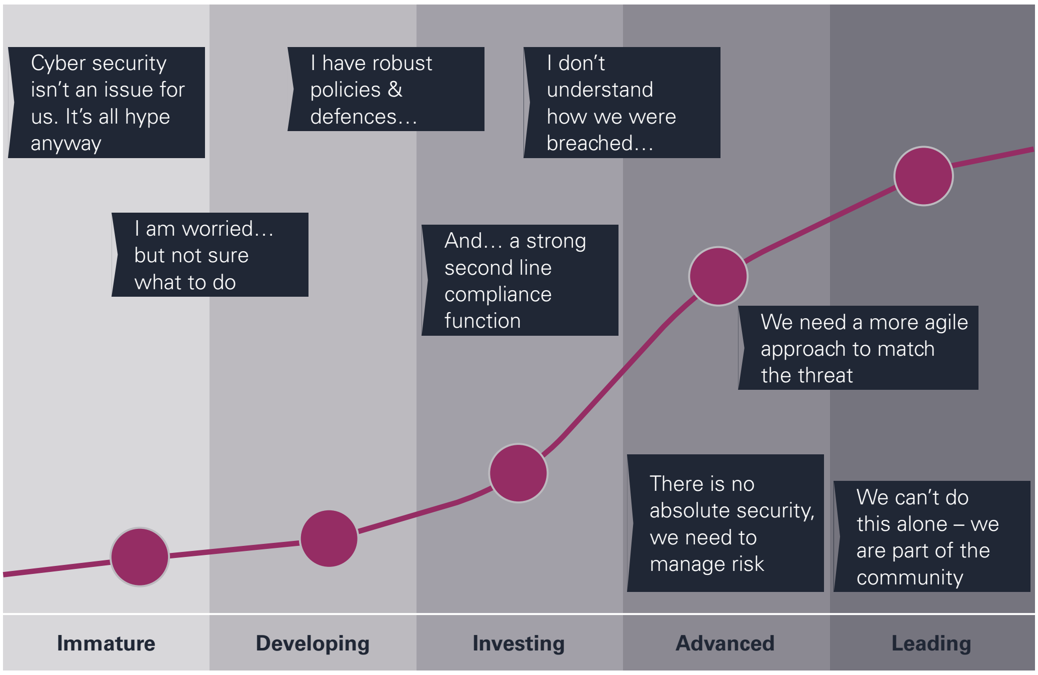
It is essential to invest in and maintain a cyber security capability to address the risks that we described in the previous section. When it feels like nothing can be done to defend against cyber-attacks, there are practical steps that can be taken.

The first of these is to get the Board engaged. Ownership and accountability needs to sit with the Board, who must approve and track progress against the cyber security strategy. As part of the strategy work, it is critical to determine an understanding of your current capability and define the future direction of your cyber security controls. Part of this can be to take a maturity led approach.

WHERE ARE YOU ON YOUR SECURITY JOURNEY?

Based on KPMG's experience of working with asset managers, we see a range of capabilities with some operating towards the upper end of the "investing" level in Figure 4, while others are still "immature". Where would you position your organisation now and where do you want to get to?

Figure 4: Measuring your cyber maturity


Cyber security isn't an issue for us. It's all hype anyway
I am worried… but not sure what to do
I have robust policies & defences…
And… a strong second line compliance function
I don't understand how we were breached…
There is no absolute security, we need to manage risk
We need a more agile approach to match the threat
We can't do this alone – we are part of the community
Immature
Developing
Investing
Advanced
Leading

MEASURING YOUR MATURITY...

Immature	Developing	Investing	Advanced	Leading
Limited awareness	Discussion of what it means for firm	Investing to improve	Boards demand better risk reduction & MI	Lead as part of the community
Reliance on basic technology	Reaching out for support / advice	Still adopting point technical solutions	Move towards structured security programmes	Build a cyber ecosystem with clients & suppliers
No controls or compliance process	Policies in place & basic security processes	Strengthening policies & compliance	Build out security operations	Intelligence led approach linked to business
Seen as a technology issue	Often driven by regulatory concerns	Initial security architecture	Ramp up testing	Cyber resilience
		Education & awareness campaign begins	Early stage supply chain security initiatives	Risk quantification & mitigation strategy
				Technology enabled & data driven

Source KPMG International

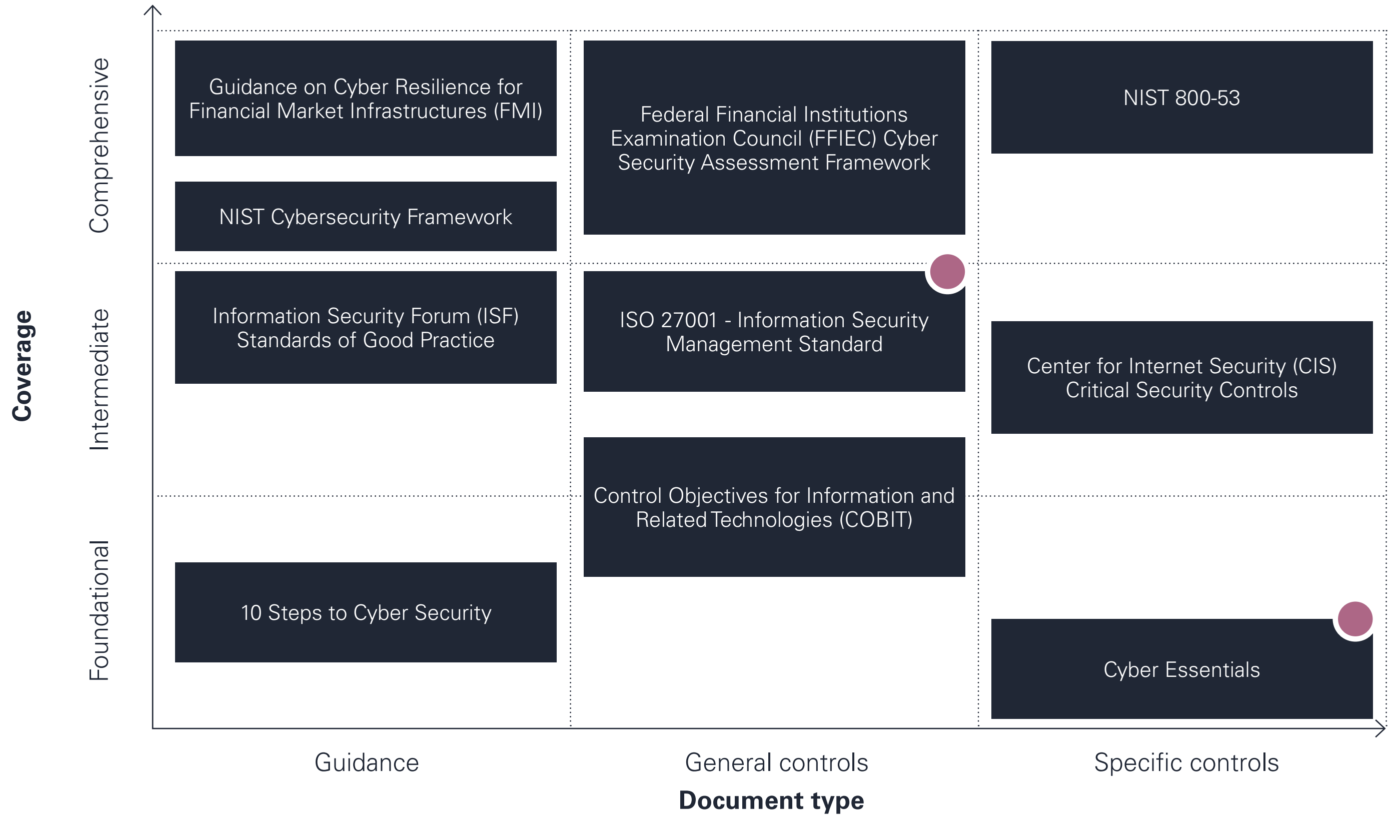
There are a range of frameworks that you may wish to align with in order to begin or continue your cyber security journey, depending on your current level of maturity. In Figure 5 we have identified the leading industry frameworks and guidance that can help you to get the most from your cyber security budgets and programmes.

Basic guidance such as 'Cyber Essentials' is an important first step on the cyber security journey – as its focus is on establishing core operational security controls that will mitigate many of the commoditised attacks (such as the WannaCry and NotPetya ransomware attacks[9]) that have impacted organisations. A natural next step after this is to adopt the UK Government's '10 Steps to Cyber Security'.

Firms that are further ahead on their journey may already be aligned to, and in many cases compliant with, some of the frameworks in Figure 5. More mature organisations are building their cyber security defences around the National Institute of Standards and Technology (NIST) Cybersecurity Framework's five capabilities – identify, protect, detect, respond and recover. This framework has been widely adopted across financial services and has been utilised by a number of financial services regulators.

For some, frameworks that allow for a formal certification (e.g. ISO 27001 and Cyber Essentials Plus) may be attractive as a means to demonstrate a level of capability that can be shared with key internal stakeholders, customers, supply chain partners and regulators.

Figure 5: Cyber security industry frameworks


Coverage
Comprehensive
Intermediate
Foundational
Guidance on Cyber Resilience for Financial Market Infrastructures (FMI)
NIST Cybersecurity Framework
Federal Financial Institutions Examination Council (FFIEC) Cyber Security Assessment Framework
NIST 800-53
Information Security Forum (ISF) Standards of Good Practice
ISO 27001 - Information Security Management Standard
Center for Internet Security (CIS) Critical Security Controls
Control Objectives for Information and Related Technologies (COBIT)
10 Steps to Cyber Security
Cyber Essentials
Guidance
General controls
Specific controls
Document type

● = Certification Available

Source KPMG International

KEY STEPS TO IMPROVE CYBER SECURITY

To build an improved cyber security approach in your organisation, it helps to think across five different aspects which we have set out below. The combination of these working together can significantly strengthen your defences and resilience.

Board

There should be a single point of contact on the Board who takes ultimate ownership of cyber security. At the same time, everyone on the Board needs a level of understanding of the issues so that they are able to engage in credible discussions. It helps to either have someone on the Board with technology and security experience or to have an advisory panel of external experts who can support the Board. This panel may attend parts of Board meetings or pre-read documents from management to discuss them with the Board ahead of meetings. The advisory panel model is a growing trend amongst large banks in particular. Another alternative is to recruit a non-executive director with technology and security expertise.

Whatever approach is adopted, you need to ensure that the Board is taking cyber security seriously, understands its importance and has an ongoing commitment to ensuring it is being effectively managed.

Cyber security risk

To have a secure organisation, you need to understand the risks that you face. This means mapping out the assets that you have (e.g. information, data, IT systems, etc.) and going through a methodical process of assessing who would want to target them, why/how, and the relative likelihood of that occurring.

These risks then need to be articulated as part of the organisation's enterprise risk management framework and validated against other forms of risk – such as operational, conduct or financial. Choices will need to be made about how to mitigate the cyber security risks and regular management information reporting then needs to be put in place.

It is also key to be clear about the organisation's cyber security risk appetite. What tolerance levels are there, for example, around acceptable downtime for digital channels? Mature organisations make conscious choices about their tolerance limits, which need Board-level endorsement and oversight.

Education

The adage that an organisation is only as good as its people is especially true with cyber security. That is why it is crucial to educate, train and empower staff at all levels. It starts with building a culture of security awareness, which has to come from the top. Basic good behaviours have to be instilled, such as not sharing passwords or clicking on unknown links.

The aim of every organisation must be to create a community of informed users, who are aware of the risks, have clarity over what is expected of them, and have the tools they need to do this. It is important to keep messages simple and easy to understand and to make them seem real and relevant by using personal life examples ("Would you share your online banking password with an acquaintance?"). It can also be highly effective to take a positive approach, recognising and rewarding people for good behaviours. For example, if you run phishing tests internally, you might have a "Hall of Fame" for members of staff that have helped identify and report phishing emails.

On top of this general education and awareness-raising, you can then provide bespoke training for high-risk members of staff. This is likely to encompass senior members such as Board executives and privileged users, but also other staff in roles that may have particular risks attached to them – for example, the finance team, personal assistants to senior executives or call centre staff.

Detect, respond and recover

No matter how much you invest in your defences, cyber-attacks will happen. It is therefore crucial that you are able to detect when you are being attacked, so that you can then respond and recover. In order to get detection right, you have to gain an understanding of your baseline – what normal looks like – by mapping flows of traffic and data across the organisation. Only then will you be able to detect unusual activity and understand what the genuine triggers are that need investigation. Some firms outsource their Security Operations Centres while others have benefited by building their own in-house capability that has an intimate knowledge of the business.

Clearly, you need to be able to respond as quickly as possible to an incident in order to limit its impact. Mature organisations have invested in developing a cyber response framework which contains clear policies in the event of different forms of cyber-attacks, cyber playbooks for the crisis management team and cyber runbooks for the technology teams. It is now commonplace across leading financial services organisation to run regular exercises – internal simulations of cyber security events in a safe and controlled environment – for the Board.

In addition, businesses are increasingly taking out cyber insurance. This is a rapidly growing market, with the two most in-demand areas being insurance for data breach and business interruption. An additional attraction of cyber insurance, particularly for smaller firms, is that policies often have as part of the package extra benefits such as access to cyber forensic investigators, legal teams and public relations / communications professionals. These can provide valuable support in a moment of need and can often provide access to a skill set that may not exist within the organisation.

Third party management

A key part of the cyber security puzzle is to coordinate internally to ensure that cyber security is an integrated risk that is being managed effectively across your external supply chain. Privacy, financial, conduct, operational and performance risks all need to be managed holistically.

To do this, you need to know who all of your third parties are, what access they have to your data, and where their connections are into your network. You also need to understand who your fourth and fifth parties are – the organisations that your supply chain relies on. Make sure that the right provisions are included in contracts with suppliers, and that you have an effective on-boarding process for new ones that includes consideration of cyber security. You need a regular and ongoing assurance programme for suppliers based on risk prioritisation. There may be room to collaborate and leverage a shared assessment programme with your peers to gain more in-depth assurance.

At the same time, technology solutions now offer a rapid way to gain a view on the security of an organisation from the outside, and new platforms are emerging to facilitate shared approaches and automate work flows. There are a host of options to explore.

3: COLLABORATIVE ACTION

How can the asset management industry improve its approach to tackling cyber threats? One avenue is to work more collaboratively to benefit from economies of scale across the industry.

SHARE THREAT INTELLIGENCE

Subscribing to cyber threat intelligence, and putting in place the resources to interpret that data, can perhaps be prohibitively expensive for many but the largest firms. However, the benefit of access to regular up-to-date cyber threat intelligence is not in doubt.

Therefore, creating a dedicated place where firms can come together to swap, share and leverage each other's cyber threat intelligence updates and lessons is a compelling way of reducing systemic threats across the entire industry.

The Investment Association is working to produce a tailored threat intelligence information sharing platform to facilitate such collaboration across the industry.

COLLABORATE TO CREATE SOLUTIONS

Due to limited resource and budget capabilities, security teams at asset managers may not have the capacity or skills on an individual basis to develop an extensive range of solutions to deliver effective cyber security risk mitigation tools and policies.

There is a great opportunity to work collaboratively to create best-in-class solutions and share best practice that all firms can use and benefit from. Examples where community-wide solutions could be created are: security awareness campaigns, board cyber security risk reports and security policies.

RESPONSE AND RECOVERY

Regardless of the size of the organisation, incident response is a collaborative effort, which involves cross-functional participation internally within an organisation, and with third parties, law enforcement agencies and regulators.

In a similar vein to the previous point, asset managers can collaborate to address different threats affecting the industry, aggregate threat data, collectively train staff to equip them with cutting-edge skills and invest in new technologies as a consortium. Asset managers can also share specialised resources and offer a hot/cold site for expediting recovery efforts in case of a cyber-attack.

INDUSTRY-LED INFLUENCE

By proactively driving the promotion of minimum core standards, the buy-side would be in a strong position to influence any future external cyber security regulation, helping to shape legislation in a way that works in the asset management industry's favour. The industry would be able to feed key lessons and issues to regulatory bodies through a single, united voice.

COLLECTIVE THIRD PARTY OVERSIGHT

Creating a forum dedicated to collaboration would also increase the industry's lobbying and influencing powers over key third parties. It is essential that cyber security standards are high across the asset management supply chain, whether that be technology providers or suppliers of critical financial market infrastructure such as market data providers, stock exchanges or custodian banks.

Equally, as retail clients begin to account for a growing proportion of assets under management, the necessity of ensuring that they too are aware of cyber security risks increases exponentially. An element of retail outreach would therefore be needed.

By creating a client industry forum, asset managers will share the burden of developing training materials and delivering sessions to clients, ensuring that industry-wide best practice is provided across the board.

ENHANCE INDUSTRY & CLIENT STANDARDS

Arguably, the buy-side has the greatest vested interest in the cyber security wellbeing of other public firms. After all, research by CGI and Oxford Economics demonstrated that cyber-attacks have a permanent impact on a company's share price.

The study found that, for 65 firms that had suffered a cyber-attack which had legal or regulatory consequences, the incident led to a permanent 1.8% decrease in their share price. The overall cost of these attacks was a $42 billion devaluation[10].

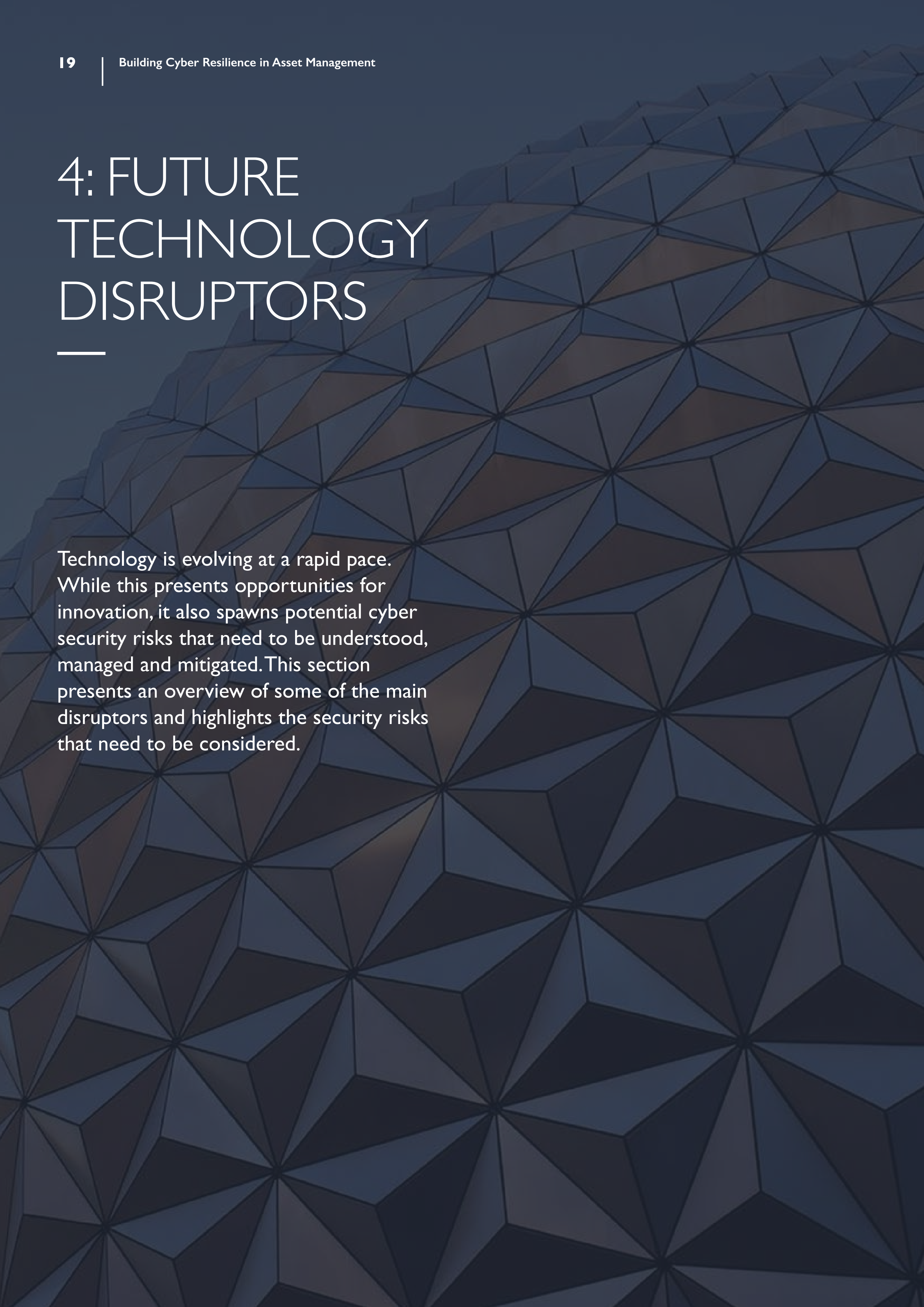
There is a clear incentive for the buy-side to drive a programme of improvement across all market participants. A minimum first step is to ensure that companies in which they have a holding have appropriate cyber security policies in place. Increased rigour would potentially pay for itself many times over.

SUMMARY

There is now an opportunity to significantly increase collaboration, and an even greater and more challenging opportunity to re-define the way financial services organisations tackle the cyber security issue. Chief Information Security Officers and security/IT risk leads will need to build trust with each other and show leadership to make this happen.

The Investment Association's Cyber Security Committee will develop an action plan which will address the following four points:

- Develop cyber security industry guidance based on best practice, working with clients, firms, regulators and public authorities to ensure the industry is leading edge.
- Promote operational robustness by coordinating with other bodies and developing security briefings, training, and thought leadership.
- Develop robust mitigation measures and controls to minimise the impact of cyber-enabled financial crime on the industry and its customers by working with the Financial Crime Committee and other stakeholders
- Provide a focal point to support members in addressing these and related issues by building a trusted community of practitioners, clients, and public authorities.



4: FUTURE TECHNOLOGY DISRUPTORS

Technology is evolving at a rapid pace. While this presents opportunities for innovation, it also spawns potential cyber security risks that need to be understood, managed and mitigated. This section presents an overview of some of the main disruptors and highlights the security risks that need to be considered.

BLOCKCHAIN:

There have been multiple proof of concepts by industry first movers to integrate blockchain technology into different aspects of the asset management value chain. To date the focus has been on increasing transparency, designing future-proof trading platforms, transaction processing, trade settlements, document management, decentralising index data, improving know your customer (KYC) processes and regulatory reporting.

Already this year, a bank-owned asset manager was able to complete an end-to-end transaction using blockchain technology[11]. Multiple stock exchanges have also announced their plans to transition to a blockchain based clearing and settlement platform[12].

SECURITY IMPLICATIONS

Cryptographic Key Theft & Access Management:
Criminals with access to a private key can use this to make fraudulent transactions and withdrawals[13]. Blockchain relies heavily on cryptography and there is a risk of a node private key, or a user, being compromised due to insufficient endpoint security measures and key management practices.

Complexity and Availability:
If the blockchain grows beyond a certain size, there is a possibility of performance and availability issues due to inherent limitations in the underlying technology[14].

Crypto Mining:
There has been a major increase over the last six months in cases of criminal organisations harnessing the combined computing power of compromised systems to perform 'crypto mining' to create new digital coins, with research suggesting that 8% of organisations have suffered such an incident[15].

Anonymity:
Tracing and assigning responsibility for criminal activity can be difficult on the public blockchain as attackers are able to hide their identity[16].

Denial of Service:
Private networks can be overwhelmed by a rogue or compromised node, making the system unavailable to other nodes in the blockchain.

CLOUD:

Firms are increasingly adopting cloud-based solutions as a means of reducing costs, centralising data, reducing the burden of managing it and improving data security.

The business advantages of using the cloud are obvious, from moving away from the overhead of managing large corporate data centres, to the flexibility offered by cloud to rapidly scale storage and processing power to meet demand.

SECURITY IMPLICATIONS

Cloud Migration:
Once you have made the decision to move to the cloud, security should be a key factor influencing your vendor selection. After that, you enter another high-risk period as you begin to move your data off your network and onto the cloud. To mitigate the risk during the migration, firms should draw up robust migration plans, with programme governance focused on people and change management throughout.

New Operating Model:
Increasingly, firms can expect their cloud providers to embed good IT security, but firms still own the problem of setting their requirements and determining just who can access what. The shift towards DevOps and agile development also demands new ways of securing the development lifecycle and an equally agile testing regime. Security can no longer only engage at the end of development cycles and, if it does, it risks being seen as a blocker rather than an enabler.

Third Party Risk Assessment:
By moving to a cloud-based solution, you must acknowledge that you are now reliant on a third party to manage your data and critical business processes. Cloud providers come in all forms with some possessing industry leading security capabilities. Nevertheless, all firms using the cloud to store their data should perform due diligence and on-going risk assessments to ensure the cloud provider aligns with the organisation's risk appetite.

Shadow Cloud & Data Mapping:
Be wary of a 'shadow cloud' emerging in the organisation, whereby employees use un-approved and high-risk cloud service providers to store confidential information. Firms have a clear opportunity to move to a 'secure' and approved cloud provider, thereby streamlining the process. If you have not done so already, you should begin by performing a 'discovery' phase to map where data resides and the cloud services being utilised by your employees.

Denial of Service:
No matter whom you choose, there is always a risk that your cloud provider suffers a denial of service event, rendering your data and applications unavailable[17]. So it is essential to prepare resilience and continuity plans against such an eventuality.

ALGORITHMS, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Algorithmic trading strategies have revolutionised the capital markets industry. The buy-side in particular has embraced and benefited from the automation of the entire capital markets ecosystem[18]. Many benefits have been cited from the increasing deployment of algorithms in the front office, including: lower fees, tighter spreads, greater consistency and, more lately, enhanced investment decision-making.

But as the source code increases in complexity - moving from simply executing orders within certain parameters towards machine learning and AI - the value and risks have increased. These risks do not only apply to the firm operating the algorithm, but to the market more generally.

SECURITY IMPLICATIONS

Access Management & Supervision:
The complexity of the algorithms means that they are only understood by a small number of people. It is vital that those with the ability to write code are given appropriate levels of access which is reviewed and audited on a regular basis. Due to the complexity and systemic importance of algorithms, firms must be prepared to comprehensively test and monitor the behaviour of those algorithms.

Data Integrity:
Algorithms rely on accurate inbound data feeds in order to operate effectively within their parameters. A failure of integrity of a data feed could lead to the sub-optimal performance of the algorithm, forcing it to make decisions or 'learn' from incorrect information it otherwise would have avoided. Audits of data feeds should be conducted continuously.

ROBO ADVICE:

One innovation that has generated much publicity is the rise of robo-advisers, offering intelligence-driven investment advice to retail clients[19]. Robo-advisers run on a set of programmes to provide advice within certain parameters, speeding up the investment process and tailoring it to a client's needs – all of which requires the collection of specific client information.

Linked to robo-advice, firms are steadily harnessing the data available to them to provide a more tailored product offering. Large data-lakes allow them to run advanced analytics on the data, resulting in custom products, with distribution and marketing plans aligned to individual customers.

SECURITY IMPLICATIONS

Penetration Testing:
To ensure the on-going security of critical business applications, it is vital to undertake regular penetration tests of web-facing systems, particularly those used to interact with clients. Manipulating part of the source code behind a robo-adviser could result in questionable investment decisions and advice.

Data Collection:
In order to improve customer experience, firms are striving to tailor products and offerings based on client needs and emotional requirements. The thinking behind this is that over time the automated tool can learn to deliver better and more personalised results and outputs. This type of data will often contain personally identifiable information which could be considered very high-risk, and consequently attract cyber criminals[20].

Data Privacy:
The data that firms are now in possession of has been built up over multiple years. If firms are using newer technologies like robo-advice and machine learning – in conjunction with client data – to improve the customer experience and tailor products to their requirements, they must beware of the privacy implications of collecting swathes of personal data in data-warehouse style repositories. The ramifications of a breach of one of these would be very serious in the eyes of the Information Commissioner. It is essential to reconcile whether you have permission to hold and use this data and, if not, make immediate plans for its deletion.

No Shortcuts:
Whilst it is a priority to improve the customer experience, it is important that critical security processes are not bypassed. For instance, the importance of two-factor authentication should always be considered even when attempting to reduce the time and effort involved from the client's perspective.

BUILDING CYBER RESILIENCE: ACTION PLAN

Cyber security and its implications can no longer be overlooked by the asset management community.

Whether you are just beginning on your cyber security journey, or whether you are a firm with a significant annual cyber security budget, it is key that you are acknowledging the growing importance of cyber security risks to your organisation and taking steps to make sure you can operate securely in an increasingly digital world.

As a result, the Investment Association and KPMG believe these are 10 steps that all firms in the industry should consider to make this happen:

1. Allocate accountability for cyber security risk to a Board member.
2. Appoint a person into a senior role with responsibility for managing cyber security.
3. Develop a cyber security strategy and seek board approval.
4. Implement the UK Government's Cyber Essentials framework.
5. Perform regular cyber security risk assessments of your business.
6. Educate all staff on their cyber security responsibilities and train those in high-risk roles.
7. Implement controls to protect privileged user accounts.
8. Implement logging and monitoring on your network and critical systems.
9. Document your cyber incident response plans and perform regular simulation exercises.
10. Identify and assess the cyber security risks in your supply chain.

REFERENCES

1. Center for Strategic & International Studies, “Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II,” Intel Security, McAfee, Santa Clara, 2014.
2. KPMG AG, “Disrupt and grow - 2017 Global CEO Outlook,” KPMG International, Zurich, 2017.
3. HM Treasury, “The UK Investment Management Strategy II,” 2017. [Online]. Available: http://www.gov.uk/government/publications/the-investment-management-strategy-ii.
4. U.S. Securities and Exchange Commission, “Observations from Cybersecurity Examinations,” National Exam Program: Risk Alert, vol. VI, no. 5, 7 August 2017.
5. CNN Tech, “Ransomware attack: Who’s been hit,” CNN, 15 May 2017. [Online]. Available: http://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html.
6. BBC News, “Could new data laws end up bankrupting your company?,” BBC, 7 July 2017. [Online]. Available: http://www.bbc.co.uk/news/business-40441434.
7. Huffpost: The Blog, “What Businesses Can Learn from the SWIFT Cyber Attack,” Huffpost, 7 June 2017. [Online]. Available: http://www.huffingtonpost.com/otto-berkes/what-businesses-can-learn_2_b_10320982.html.
8. KPMG AG, “Clarity on Cyber Security - Ahead of the next curve,” KPMG AG, Zurich, 2017.
9. SecurityNow, “Ransomware: Still a Security Threat & Still Evolving,” LightReading.com | Networking the Communications Industry, 17 April 2018. [Online]. Available: http://www.securitynow.com/author.asp?section_id=715&doc_id=742260.
10. Reuters UK, “Cyber breaches have cost shareholders billions since 2013 - report,” Thompson Reuters, 12 April 2017. [Online]. Available: http://uk.reuters.com/article/uk-cyber-companies/cyber-breaches-have-cost-shareholders-billions-since-2013-report-idUKKBN17E0SI.
11. FTfm, “Blockchain ‘could save asset managers $2.7bn a year’,” Financial Times Group, 22 February 2018. [Online]. Available: http://www.ft.com/content/b6171016-171f-11e8-9e9c-25c814761640.
12. BBC News, “Australian stock exchange to move to blockchain,” BBC, 7 December 2017. [Online]. Available: http://www.bbc.co.uk/news/business-42261456.
13. KPMG International, “Securing the chain,” KPMG International, 2017.
14. Forbes Tech, “Eight Reasons To Be Skeptical About Blockchain,” Forbes, 31 May 2017. [Online]. Available: http://www.forbes.com/sites/jasonbloomberg/2017/05/31/eight-reasons-to-be-skeptical-about-blockchain/#728839685eb1.
15. Financial Times, “‘Cryptojackers’ steal computer power to mine digital coins,” Financial Times Group, 8 April 2018. [Online]. Available: http://www.ft.com/content/a0d4d8ce-2231-11e8-add1-0e8958b189ea.
16. Indy/Tech, “Bitcoin price is so high because criminals are using it for illegal trades, research suggests,” Independant, 24 January 2018. [Online]. Available: http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html.
17. Infoworld: Tech Watch, “Dyn DDoS attack exposes soft underbelly of the cloud,” IDG Communications, 24 October 2016. [Online]. Available: https://www.infoworld.com/article/3134023/security/dyn-ddos-attack-exposes-soft-underbelly-of-the-cloud.html.
18. BBC News, “How artificial intelligence is transforming the financial industry,” BBC, 16 September 2015. [Online]. Available: http://www.bbc.co.uk/news/business-34264380.
19. FTfm, “Robo-advice turns heads of leading fund houses,” Financial Times Group, 5 February 2017. [Online]. Available: http://www.ft.com/content/fb690b40-dd9d-11e6-86ac-f253db7791c6.
20. HBR, “AI Adds a New Layer to Cyber Risk,” Harvard Business Review, 13 April 2017. [Online]. Available: http://hbr.org/2017/04/ai-adds-a-new-layer-to-cyber-risk.

Figure 3 references

1. MarketWatch, "Hacked? This is what the top 5 brokers will do for you," Dow Jones & Co., 28 October 2015. [Online]. Available: http://www.marketwatch.com/story/hacked-this-is-what-the-top-5-brokers-will-do-for-you-2015-10-27.
2. Reuters, "Ex-Morgan Stanley adviser spared U.S. prison term for taking data," Thompson Reuters, 22 December 2016. [Online]. Available: http://www.reuters.com/article/us-morgan-stanley-cybersecurity-crime/ex-morgan-stanley-adviser-spared-u-s-prison-term-for-taking-data-idUSKBN0U521Z20151222.
3. Thompson Reuters, "UPDATE 1-Data breach at bond insurer MBIA may affect thousands of local U.S. governments," Thompson Reuters, 8 October 2014. [Online]. Available: http://www.reuters.com/article/mbia-cybersecurity/update-1-data-breach-at-bond-insurer-mbia-may-affect-thousands-of-local-u-s-governments-idUSL2N0S22LB20141008.
4. Financial Times, "CME discloses FBI probing July hacking attack," Financial Times Group, 15 November 2013. [Online]. Available: http://www.ft.com/content/a5b4b1b4-4e25-11e3-8fa5-00144feabdc0.
5. Reuters, "American Funds urges password change to counter 'Heartbleed' bug," Thompson Reuters, 16 April 2014. [Online]. Available: http://www.reuters.com/article/us-cybersecurity-heartbleed-funds/american-funds-urges-password-change-to-counter-heartbleed-bug-idUSBREA3F1B520140416.
6. U.S. Securities and Exchange Commission, "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach," 22 September 2015. [Online]. Available: http://www.sec.gov/news/pressrelease/2015-202.html.
7. The Switch, "E-Trade notifies 31,000 customers that their contact info may have been breached in 2013 hack," The Washington Post, 9 October 2015. [Online]. Available: http://www.washingtonpost.com/news/the-switch/wp/2015/10/09/e-trade-notifies-31000-customers-that-their-contact-info-may-have-been-breached-in-2013-hack/?noredirect=on&utm_term=.a436e4f3bac6.
8. Reuters, "Asia's rich wary of global banks managing money: Portcullis TrustNet," Thompson Reuters, 16 June 2014. [Online]. Available: http://www.reuters.com/article/us-wealth-summit-portcullis/asias-rich-wary-of-global-banks-managing-money-portcullis-trustnet-idUSKBN0ER0NI20140616.
9. Bloomberg Technology, "CME Hack Draws FBI Probe While Renewing Market Structure Anxiety," Bloomberg, 16 November 2013. [Online]. Available: http://www.bloomberg.com/news/articles/2013-11-15/cme-group-says-its-computers-were-hacked-no-trades-affected.
10. SC Media UK News, "Spearphishing attack nets hundreds of thousands from investment firm," SC Media UK, 6 May 2016. [Online]. Available: http://www.scmagazineuk.com/spearphishing-attack-nets-hundreds-of-thousands-from-investment-firm/article/530921/.
11. Weath Manager, "Hedgie giant targeted by Chinese scammers," CityWire, 11 April 2018. [Online]. Available: http://citywire.co.uk/wealth-manager/news/hedgie-giant-targeted-by-chinese-scammers/a1109276.
12. Weekend Investor, "Check Brokerage Statements and Online Accounts for Signs of Fraud," The Wall Street Journal, 25 July 2014. [Online]. Available: http://www.wsj.com/articles/check-brokerage-statements-and-online-accounts-for-signs-of-fraud-1406307043.
13. SC Media UK News, "Charles Schwab data breach exposed client investment data," SC Media UK, 05 May 2016. [Online]. Available: http://www.scmagazine.com/charles-schwab-data-breach-exposed-client-investment-data/article/528002/.
14. Reuters Staff, "Cyber attack briefly shutters Charles Schwab website," Thompson Reuters, 24 April 2013. [Online]. Available: http://www.reuters.com/article/net-us-schwab-website/cyber-attack-briefly-shutters-charles-schwab-website-idUSBRE93M1DV20130424.
15. FT Adviser, "Adviser support service hit by cyber attack," Financial Times, 23 March 2017. [Online]. Available: http://www.ftadviser.com/your-industry/2017/03/23/adviser-support-service-hit-by-cyber-attack/.

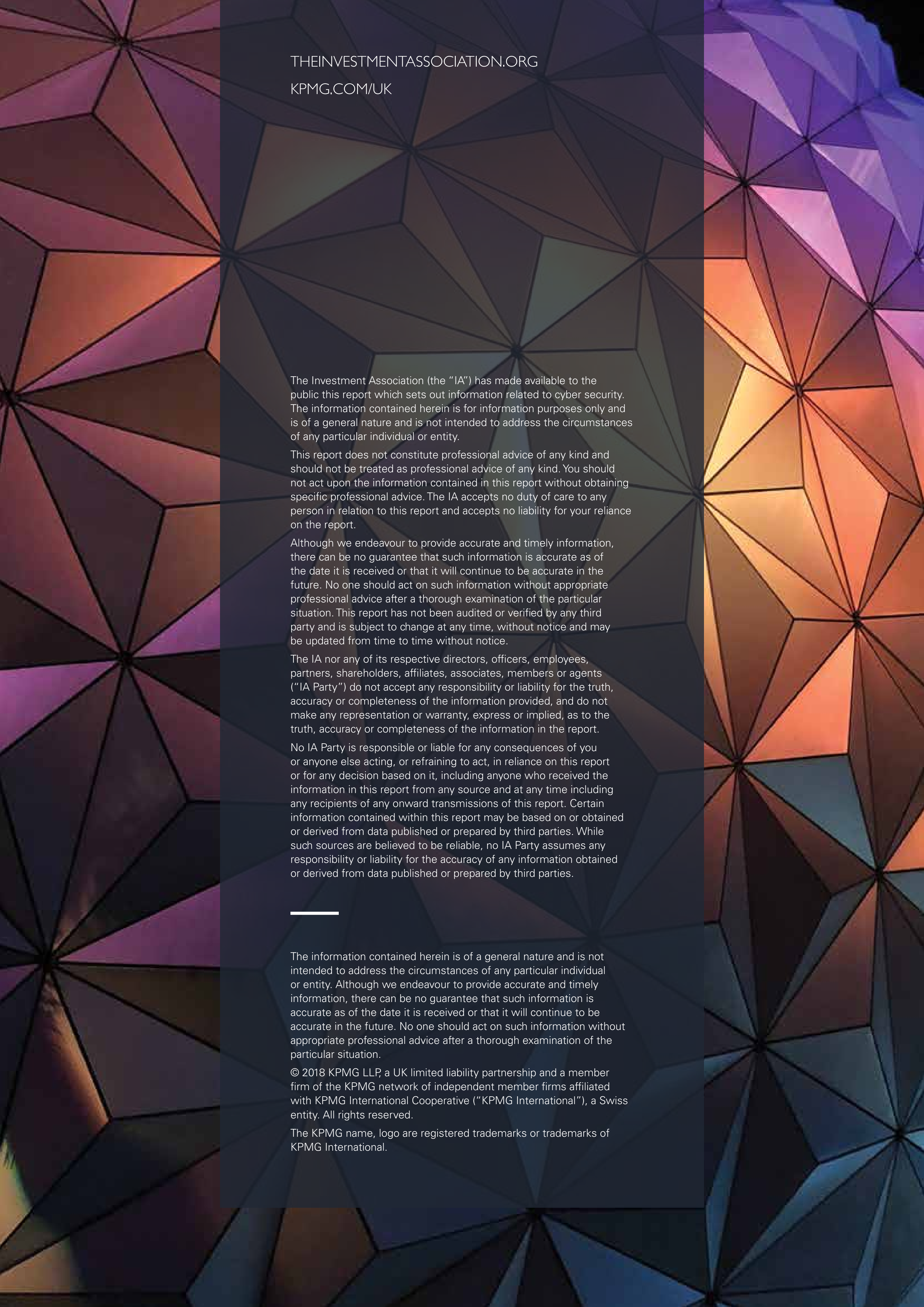
Glossary for Figure 1: Cyber security risk radar

	Term	Definition
1	Distributed Denial of Service (DDoS)	Overloading a website or application with heavy traffic in order to exceed its capacity and disrupt services.
2	Sabotage	Intentional disruption of operations by a person abusing their existing access to the network and systems.
3	Website Compromise for cryptocurrency mining	Infection of a victim's computer with a malicious code designed to 'mine' cryptocurrencies. The victim does not lose out financially, but the functionality of their systems may be compromised.
4	Social Engineering	Tricking or manipulating people to provide confidential information.
5	CEO Fraud & Business Email Compromise	Impersonation of C-suite executives via email and instructing people to transfer funds to an account or disclose confidential data.
6	Social Media Impersonation	Creation of a replica corporate social media account which could be used to distribute false news or communicate with stakeholders.
7	Ransomware	Malicious software that threatens to publish an organisation or individual's data or encrypts its computer systems unless a ransom is paid.
8	Malware	Short for malicious software, and includes intrusive software, viruses, worms, ransomware, spyware, adware, scareware, etc.

At KPMG, we believe in proactively incorporating cyber risk management into all activities. Cyber security is not just a reactive technical fix – it can also be a driver of change and secure the future of your business.

With over 2,000 security practitioners world-wide, KPMG can give you the support and guidance you need to adapt to new global threats. By evaluating business resilience, optimising the relationship between people, process and technology, and bringing the latest industry insights, we can help turn risk into advantage.

KPMG in the UK employs 12,000 people across 22 offices in the country and we are part of a global network operating in 155 countries around the world. Providing audit, tax and advisory services we combine our multi-disciplinary approach with deep industry knowledge to help clients meet challenges and find opportunities each and every day. The independent member firms of the KPMG network are affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. Each KPMG firm is a legally distinct and separate entity.



THEINVESTMENTASSOCIATION.ORG

KPMG.COM/UK

The Investment Association (the "IA") has made available to the public this report which sets out information related to cyber security. The information contained herein is for information purposes only and is of a general nature and is not intended to address the circumstances of any particular individual or entity.

This report does not constitute professional advice of any kind and should not be treated as professional advice of any kind. You should not act upon the information contained in this report without obtaining specific professional advice. The IA accepts no duty of care to any person in relation to this report and accepts no liability for your reliance on the report.

Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. This report has not been audited or verified by any third party and is subject to change at any time, without notice and may be updated from time to time without notice.

The IA nor any of its respective directors, officers, employees, partners, shareholders, affiliates, associates, members or agents ("IA Party") do not accept any responsibility or liability for the truth, accuracy or completeness of the information provided, and do not make any representation or warranty, express or implied, as to the truth, accuracy or completeness of the information in the report.

No IA Party is responsible or liable for any consequences of you or anyone else acting, or refraining to act, in reliance on this report or for any decision based on it, including anyone who received the information in this report from any source and at any time including any recipients of any onward transmissions of this report. Certain information contained within this report may be based on or obtained or derived from data published or prepared by third parties. While such sources are believed to be reliable, no IA Party assumes any responsibility or liability for the accuracy of any information obtained or derived from data published or prepared by third parties.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.