Securing Innovations in Financial Services

Intelligent Digital

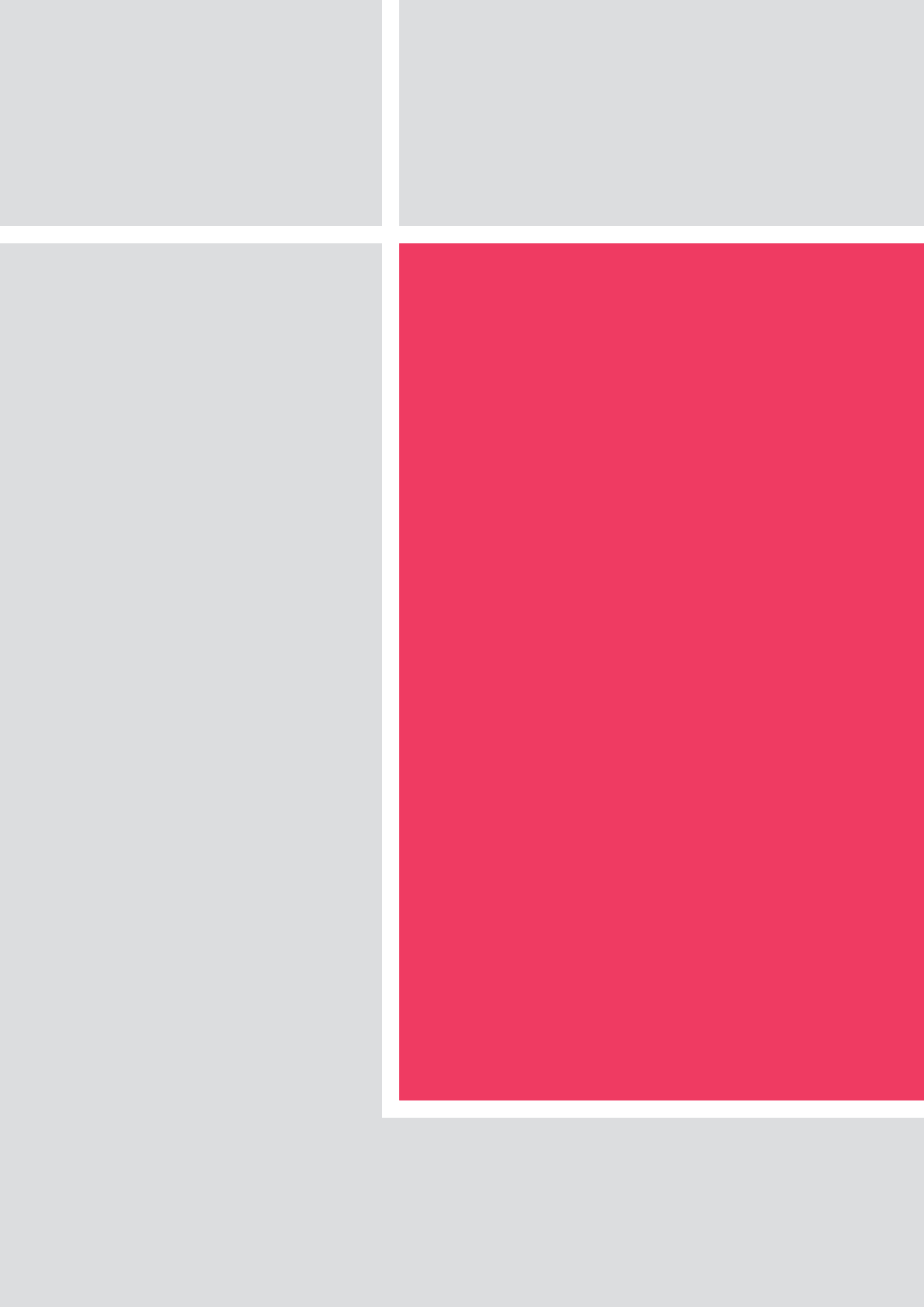
Innovations create new vulnerabilities and as such the threats faced by organisations continue to grow.

January 2019

#IntelligentDigital
pwc.co.uk/cybersecurity

pwc

Contents



Introduction

Widespread innovation has taken place over recent years. Consumers now expect to interact with products and services in ways that have meant fundamentally changing how businesses engage with their customers. The Financial Services sector is no exception.

Innovations create new vulnerabilities and as such the threats faced by organisations continue to grow. Risks are evolving all the time through the development of new channels, services and products offered, changes in industry best practice, corporate compliance, and the handling of information.

The need to understand the complex interconnection of data, compliance and enhanced performance is now greater than ever before. Organisations have a responsibility to understand what these changes mean for their operations and the increased risk that change can bring.

The Financial Services sector tends to be one of the more mature industries with regards to cyber security and investing in asset protection. Regulatory focus remains strong and cyber attacks now pose a significant threat to the stability of the global financial markets.

This paper aims to assess the business impact of the cyber threats introduced by innovations in Financial Services. The paper is structured around the six functions of Financial Services disruption that have been described in the World Economic Forum's (WEF) paper 'The Future of Financial Services'.

As it has been over three years since the publication of the original whitepaper it is useful to review the predictions, look at which ones came to fruition and analyse where the cyber security industry now needs to adapt in order to keep pace with the changes.

During this paper we outline the emerging risks now faced by organisations across the Financial Services sector and ask businesses to consider the following:

- How have current and planned innovations in your business changed your cyber risk exposure?
- Is your organisation equipped to address the cyber risk at the pace with which your business is innovating?
- What role should your CISO play in supporting a business' innovation journey?

Emerging industry trends

Innovation has always brought with it a number of challenges and threats that can hinder progress. The trends currently emerging in the Financial Services sector introduce a number of serious cyber threats. These must be analysed and managed in order for Financial Services organisations to truly adopt innovation and transition to a future state with confidence.

Increased technological advancements

Organisations continue to pursue innovative change in order to achieve market leader status in their respective industries. These innovations, however, create an increasingly complex technology infrastructure and introduce new operational and cyber risks to businesses and their customers. We will discuss the innovation in detail later in this paper, as each function of financial services will have its own unique applications, but all of these can be grouped into the following three trends:

- Externalisation of processes to better leverage innovative technology and improve customer experience and choice (Fintech). For example, insurers' increased reliance on a supply chain delivering reliable connected devices and on third parties that can collect the data from those devices, mine it and obtain useful insights for creating new products.

- Automation of processes to reduce operational cost and enhance business insights. Capabilities like big data, AI and machine learning are used to address resource-heavy data analysis requirements of investment management and market provisioning. Automation is often driven by a requirement to cut costs but more often also by the need to keep ahead of the competition.

- Requirement to prototype and accelerate delivery of minimum viable products through use of agile delivery and cloud computing. As customers' demand to consume content from any device at any time in any place grows, organisations are responding by building faster and more flexible products using a multitude of cutting edge and often unproven technology stacks.

As organisations increasingly rely on technology to handle information that is personally, commercially or financially sensitive, they will also need to understand the cyber risks they introduce or amplify.

Non-negotiable basics

The recommendations from our analysis can be grouped into two categories: function-specific ones that need to be evaluated to better manage the cyber risk in a specific area (e.g. Market Provisioning), and function-agnostic ones aimed at all service providers in the sector.

When analysing the second category, we have managed to distill four specific themes. Although not new for a seasoned cyber security leader, these are becoming increasingly important in the context of technological advancements and innovation mentioned throughout this paper. These basics are becoming non-negotiable.

Rigorously vet partner solutions

Create a rigorous process around the maintenance of approved partner solution components (e.g. cloud infrastructure, application components, integration platforms, etc.) in order to manage the risk of compromise through a third party supply chain. Enforcing the selection of multi-accredited, externally validated solution component providers will prevent your suppliers from applying shortcuts and introducing unproven solutions into your supply chain. This third party process will help you to gain higher levels of control over the concentration risk.

Control access to data anywhere

Focus and prioritise around data access. Instead of protecting all possible types of data repositories, which can be very impractical due to today's proliferation of technologies, ensure that you are protecting the mechanisms that control the access to your data, for example implementing digital rights management solutions. This will allow your data protection capability to scale within and across your organisational boundaries while adhering to privacy regulations, which put the power with the customer to decide how their data is used.

Test resilience of end-to-end processes

Expand cyber resilience stress testing and recovery planning so that consideration is given to the end-to-end process. This should span multiple third parties that may underpin the provision of a product or service in order to truly understand the operational tolerances and single points of failure that may lead to unacceptable disruption in the event of a cyber attack.

Embed security and privacy by design

Embed security and privacy by design into business innovation (vs. technology change). This might include placing enterprise security architects within or across business functions, allowing them to influence at a business process level the design of new and evolving products and customer services so they can be built with cyber resilience factored in.

Six functions and associated innovations

1 Payments

2 Connected Insurance

3 Deposits and Lending

4 Capital Raising

5 Investment Management

6 Market Provisioning

Payments

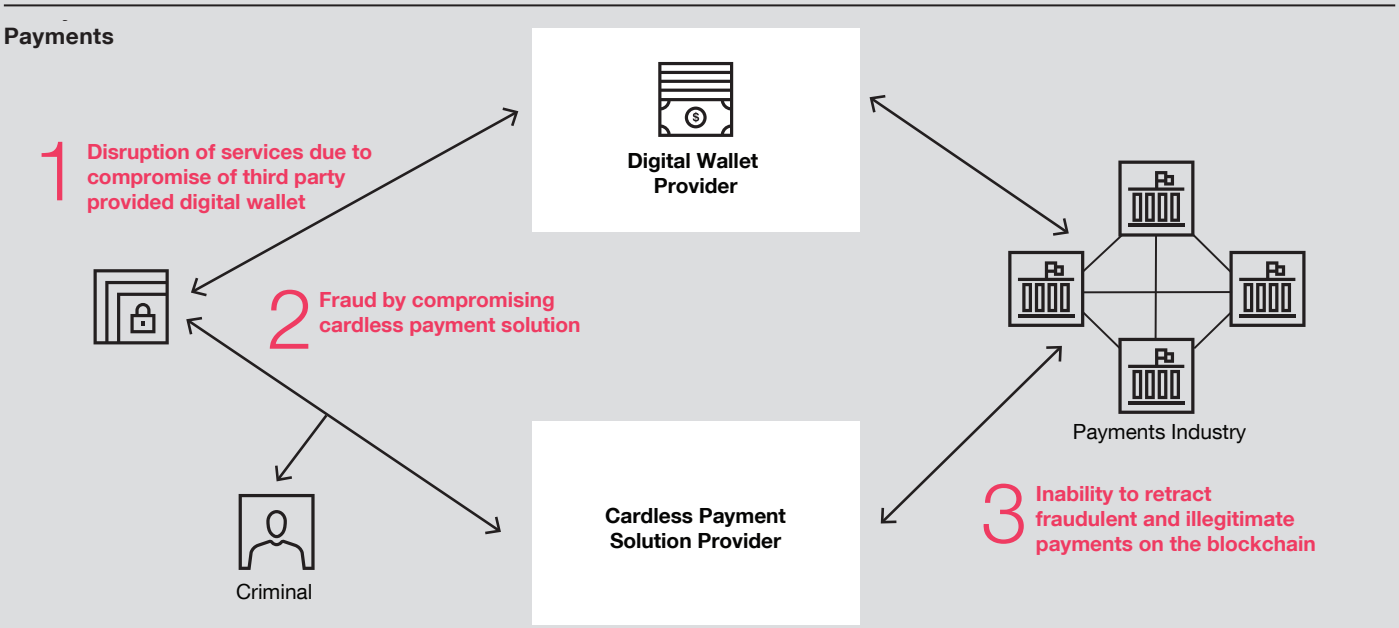
A number of innovations have emerged in the past five years leveraging mobile devices and connectivity to make payments simpler and more valuable. Examples range from digital wallets to automated machine-to-machine payments. The majority of these innovations modify front-end processes to improve customer and merchant experience, while leaving the underlying payments infrastructure undisrupted.

Cashless world

The WEF paper illustrates that innovation in this space could see the consolidation or fragmentation of payment card service providers or the complete displacement of cards altogether.

Decentralised or non-traditional payment schemes

New payment models are here to stay and as the WEF paper shows, organisations may approach this innovation in different ways – from direct competition, to augmenting their traditional services to potentially change the way traditional payment rails work – but stopping short of completely moving their business to new payment platforms.



Security considerations

Looking at these innovation clusters through the lens of our clients (for example, card issuing or acquiring banks and payment service providers), it becomes evident that the key to understanding the true cyber risks within a payment market lies in understanding the supply chain liability and risk.

Below are the key cyber risks resulting from innovation in this space which will need to be addressed:

1. **Disruptions of service resulting in the reduction in trust due to a compromise of a third-party digital wallet service provider.** Proliferation of card and wallet providers, described by WEF in one of the disruption scenarios, leads to blurring customers' understanding of security responsibilities. A breach of customer data, subsequent card replacement, and potential need for ID theft monitoring, would likely be blamed on the card issuer until proven otherwise.

As cyber security news continues to grab the headlines, customers are becoming increasingly aware of the issues and may consider switching providers if trust in security measures is lost.

2. **Increased fraud caused by the compromise of cardless payment solution service providers.** In a cardless scenario, where a customer authorises a direct link between their bank and vendor financing scheme, the integration point becomes a significant concern. A myriad of customer-triggered integrations could severely complicate fraud identification and management processes within the bank. As with the previous example, fraudulent transactions in the account could lead the customer to believe that the bank itself was compromised. Again, this could result in a customer switching current accounts – something that has now been made incredibly simple with the recent change in regulations.

3. **Inability to mitigate the impact of fraudulent transactions due to an inability to trace and retract illegitimate payments caused by an attack on the blockchain.** A number of organisations are augmenting their services by integrating them with blockchain solutions. There are a number of regulatory challenges that need to be addressed when following this approach, but there is also a very practical consideration around the inability to mitigate the impact of fraud. When the transaction is made it is forever imprinted in the ledger, together with all other data that could be included such as illegal and questionable content, personal data, etc. Due to the nature of blockchain technology, fraudulent or incorrect transactions are permanently stored, indelible and irrefutable.

Ways to Adapt

1. **Identify business triggers of security compromise,** e.g. increases in customer complaints, fraud alerts, or high-value transactions, that could mean a compromise of downstream service providers.

2. **Identify potential cyber impacts of business-critical functions,** e.g. compromise of integrity of a payment ledger. Ensure that the business/product owners are aware of the risks and include them in response planning exercises. This should include enhancing the visibility of all third parties involved across the service delivery chain and building the right processes for understanding and responding to the risks these third parties may introduce.

   As third parties, their interconnectivity and the integration points with current business-critical functions increase, the need to develop a structured security oversight programme, along with the right technical tools to support it, becomes increasingly necessary.

Key steps could include:

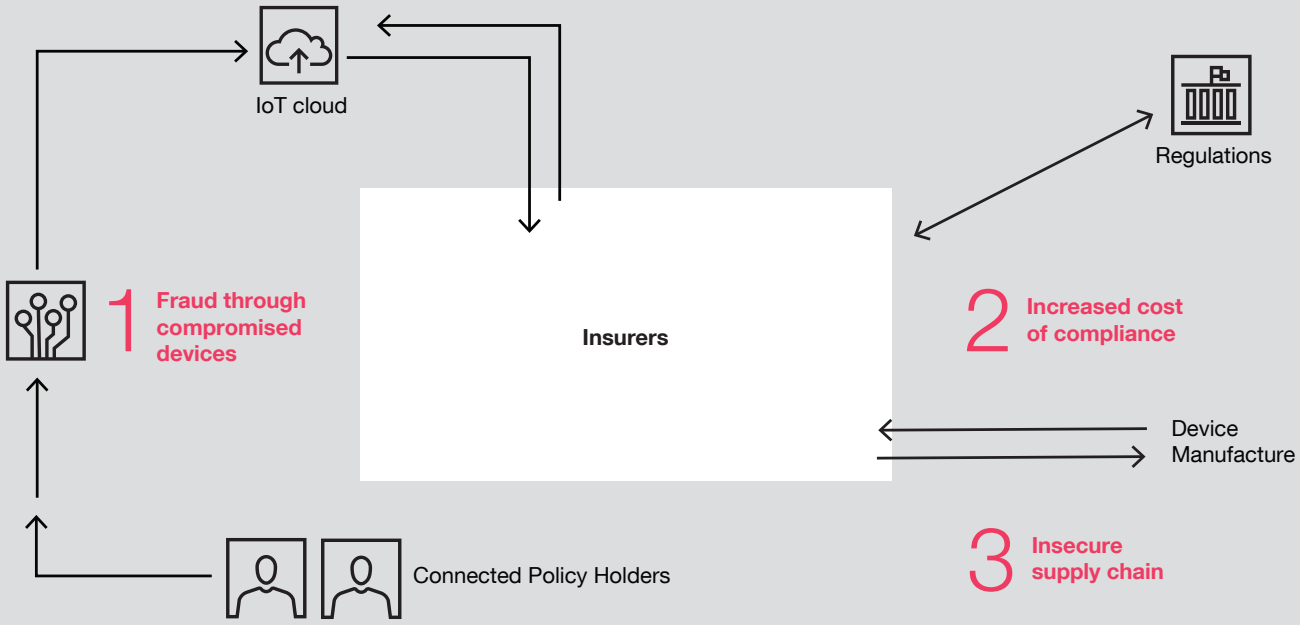
- Extending the scope of security monitoring beyond your perimeter. Traditionally, Security Operation Centres (SOCs) focus on the internal assets. Now, with advancement of Platform and Application as-a-Service offerings, suppliers are making their data available to customers. This data can be consumed and utilised to understand the real-time risk posture.

- Utilising cyber threat intelligence to continuously monitor the risks posed by existing third parties and for changes that may affect the organisation's risk exposure. Ask your suppliers questions about how they are managing the threats that may be targeting the service providers they have in place (e.g. cloud hosting, managed security services, accounting software, etc.).

Connected insurance

The insurance sector is traditionally slower than other financial industries such as banking when it comes to adopting innovation, yet a number of industry analysts believe that it will be an area facing significant disruption in the near future. E-aggregators are beginning to put pressure on personal insurance providers, and technology companies are using their brand to get into this space and sell their own insurance products directly to customers. To understand the impact of this innovation in the context of cyber security, we have analysed the following innovation clusters:

Connected insurance



Disaggregation of the supply chain

Since 2015, we have observed several potential outcomes described by the WEF come to life.

The insurance market is going through consolidation in order to obtain much–needed cost savings required in the commoditised personal insurance market. However, before the benefits of mergers are realised, CTOs have to consolidate complex technology estates, often containing custom-built life insurance policy systems.

In addition, we are seeing a shift from product-focused to customer-focused policies. This complicates the supply chain, as actuaries look to access more in-depth historical, and often heavily regulated, data, such as medical records, and niche policy distribution networks.

All of this means integration at scale and, in many cases, requires the development of new systems to replace legacy systems that fail to integrate.

Insurers also need to consider issues of data sharing due to the advancement of e-aggregators that allow customers to 'shop around'. Should policy pricing information be protected and only shared with customers that 'go direct', or should it be shared with everyone to ensure customers can obtain a most up-to-date quote from the aggregator? In the case of the latter, how can insurers make sure the aggregator displays the correct price?

Connected world

IoT platforms and connected devices – including healthcare, tracking wearables, connected cars and so on – all provide useful data that enable insurers to rethink their reactive pricing models based on historical data and allow them to create new, dynamic policies. These can be calculated in near real time and are based on customers' current needs, environment, behaviour and risk levels.

From a technology estate viewpoint, this introduces further complexity and means that organisations now need to think about the following:

- The impact of collecting the data from an extensive network of endpoint devices developed and controlled by third parties.
- The analytical capabilities required to process large quantities of endpoint telemetry to understand more about a customer's lifestyle, identity and risk profile.
- The opportunities and the mechanisms for pushing anonymised data further into the supply-chain to enable the business and its partners to create new offerings.

Security considerations

The key component underpinning the innovation in personal insurance and IoT applications and connected devices is big data and a requirement to protect it throughout its lifecycle. More specific cyber implications for the business are:

1. **Increased cost of compliance due to greater scrutiny from regulators.** This is caused by an ever-increasing amount of personal data captured and changes around the acceptable use of customer data.

2. **Financial and legal liability for insecure third-party-provided connected devices that result in an increased fraud risk, service downtime, or a threat to customer health and wellbeing.** Since 2015, the risks to wellbeing have become more significant. Insurers are using device data to build a predictive risk model to establish a regular interaction with customers in the form of a 'concierge', recommending everything from regular walks to, in some extreme examples, an injection of insulin.

3. **Increased fraud caused by the customer circumventing endpoint device controls,** such as hacking a connected car or simply by 'gaming' the system – for instance, lending a health tracker to a healthier person with the aim of decreasing their premiums.

4. **Increased cyber risk exposure due to a wider attack surface.** This is facilitated by the integration of a disparate range of new technologies and devices, such as IOT endpoints e.g. diagnostic dongles used for insurance purposes previously found to have critical vulnerabilities plus any accompanying back-end systems. This will make securing the entire IT estate more difficult, particularly with regards to monitoring ingress and egress points into the network. Furthermore, the increase in collected personal data will make organisations more attractive targets to threat actors looking to illicitly access personal data.

Ways to adapt

1. **Collate, map and normalise your security compliance requirements into a single list.** This will help create a holistic compliance programme that will allow streamlined evidence gathering and external audit request management, therefore reducing the operational costs associated with producing the same evidence 6-10 times a year. There is a growing recognition in the cyber industry around the complexity associated with managing suppliers, with the average organisation managing 300+. Organisations should ensure that there are a number of solutions in place (both process and technology orientated) that help to shape a risk-based approach to identifying and validating the security compliance of key suppliers.

2. **Owing to the importance data now plays in an organisation,** as well as the amount of data-driven business opportunities, organisations and their security leadership may want to suggest appointing a dedicated Data Protection Officer or Chief Information Officer. These roles are then able to direct the business when it comes to using customer data in a responsible and compliant manner.

3. **Deploy the right technical tools to handle the large increase in devices and data being used across the IT estate.** Advanced security analytics tools are required in order to identify, in real time, security threats and potential incidents across the network. These tools should also be able to provide full visibility and control over the whole network to allow organisations to quickly pinpoint compromised devices and isolate them.

4. **Utilise automation to address resource-heavy requirements.** For example access recertification efforts can be significantly reduced by utilising data analytics to add the risk context to application, role and privilege prioritisation.

5. **Engage with device manufacturers to evaluate any risks associated** with their product and ecosystems as well as how it could potentially expose your organisation. This should include the direct risk of customer data loss (or corruption), but also the risk of fraud and impact to customers' health and wellbeing

Deposits and Lending

The 2008 global financial crisis created a lending gap in the market, leaving a considerable proportion of borrowing needs underserved by financial institutions. According to the WEF paper, as banks tightened loan requirements due to increased safety measures, lower risk appetites amongst retail banks significantly limited access to traditional bank-intermediated lending. Moreover, alternative lending platforms leveraging P2P models experienced rapid growth.

Increased availability of alternative lending platforms

Consumers are now turning towards alternative routes to borrow money. Many of these models use different adjudication methods and lean, automated processes to offer loans to a broader base of customers, and a new class of investment opportunities to savers.

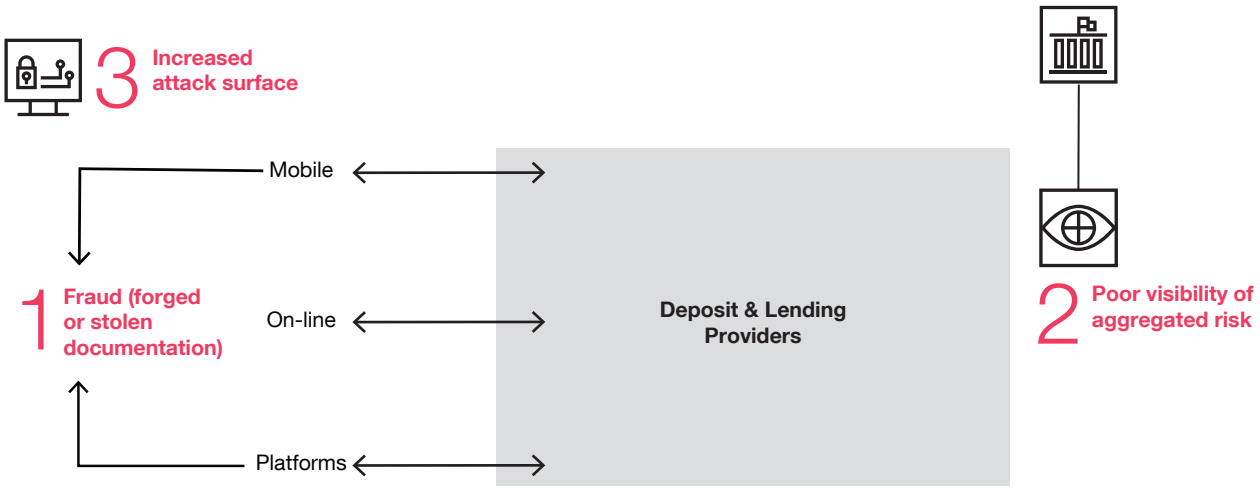
In most alternative platforms, the assessment of borrowers is at least partly automated against predefined rules for fast, transparent processing. Furthermore, unlike traditional banks, these platforms are free of legacy processes and technologies, allowing them to onboard and assess borrowers and lenders in a more streamlined fashion.

Therefore, online and P2P lending platforms provide customers with low-cost, fast, flexible, and more customer-orientated alternatives to mainstream retail banking.

Shifting (and growth of) customer channel preferences

Generational shifts and rapid consumer adoption of technology is driving a change in customer preferences for financial products. Customers are now demanding more transparency, efficiency and control over their savings and loans. The introduction of virtual banks, evolving mobile banking capabilities, and the development of the ‘banking as platform’ movement is steering this demand.

Deposits and Lending



Security considerations

1. **An increase in fraud caused by forged or stolen ID documentation.** Customers demand fast and flexible services. As the pressure for customer preferences grow, and decisions become based on automation, it will become increasingly important for organisations to improve their ability to spot fraudulent ID documents. An example of a fraud scenario would be an individual using legitimate documents stolen through a vulnerable link in the overall ecosystem (e.g. a bureau collecting data for issuing digital identities).

2. **Poor visibility of consumer credit risk caused by complex integrations between ecosystem participants.** Measuring the creditworthiness of customers may become more complex as customers will hold accounts/ products with alternative platforms with varying reporting standards, making it difficult for financial institutions to measure each customer's creditworthiness in a consistent manner.

3. **Increased risk exposure due to the introduction of more online customer-facing channels and digital services.** Shifting customer channel preferences are increasing the pressure on service providers to expand their online service offerings. The introduction of more customer-facing online channels and services is exposing providers to more threats as the attack surface continues to expand.

Ways to adapt

1. **Security architecture patterns should be developed to standardise the deployment of online services** that support new and existing customer channels. These should address the organisation's security requirements for implementing new services that are exposed to the public (e.g. web applications or APIs). In addition the software development lifecycle and assurance processes that are required pre- and post-deployment should be enhanced.

Capital Raising

Although alternative funding platforms are not likely to replace more traditional capital raising methods, their increasing popularity could change the role of incumbent institutions. Alternative funding platforms will make the capital raising market more diversified and accessible to the public, with increased accuracy and control for investors.

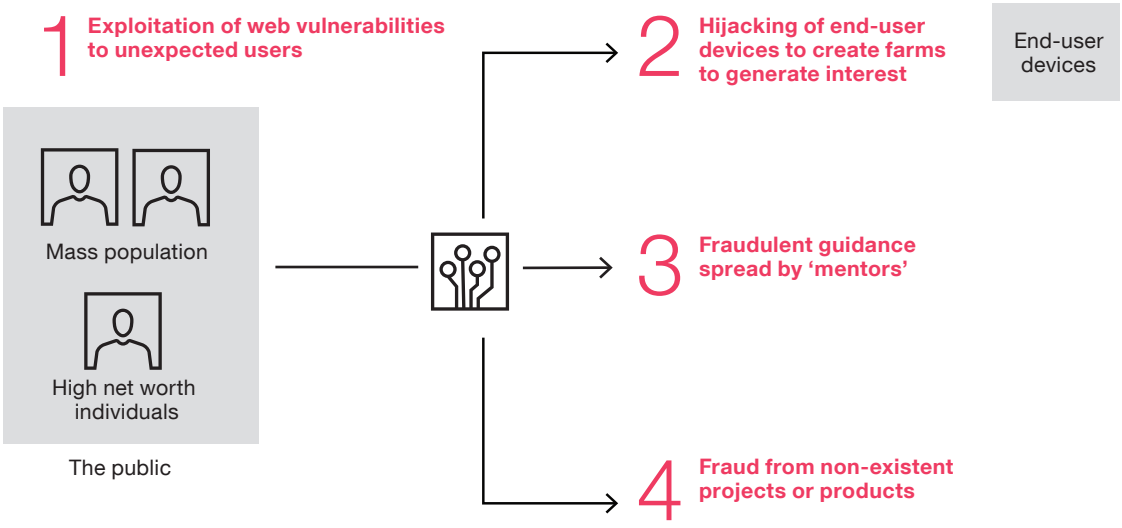
Alternative funding platforms

The growth of alternative funding platforms for capital raising has provided the opportunity for businesses to now interact directly with individual investors.

Alternative funding platforms for capital raising will continue to dominate the market and, as the WEF paper shows, the characteristics of alternative funding platforms will include:

- Crowd-based – These platforms provide a marketplace for individual investors to directly discover and invest in opportunities.
- Investment opportunities are typically only funded when a predetermined target is met, to determine less credible or less promising opportunities through 'crowds' approval'. Individual investors gain direct visibility and control over targets and allocations.
- Networking and mentorship – Many of these funding platforms allow potential entrepreneurs to leverage the expertise of more experienced investors. Furthermore, these experienced investors have the potential to earn more, through fees for mentorship.
- Customisation – Alternative funding platforms provide a number of customisation parameters for businesses to adjust and easily design funding options (e.g. term, equity share).

Capital Raising



Security considerations

1. **Hijacking of end-user devices to create farms** in order to mislead people on the popularity of startups/products advertised on crowdfunding platforms. This can then encourage genuine users to participate in a fabricated business.

2. **Loss of trust caused by false guidance spread by fraudulent 'mentors'.** As the popularity of these alternative funding platforms grow, the experienced 'mentor' entrepreneurs who are exposed to information about startup businesses need to be verified correctly. Organisations need to consider the brand value impact of fraudulent advice from these 'mentors'. If an influencer is not who they claim to be, or loses their credentials to a malicious actor, other users could potentially be exposed to misleading information. Also, mentors may fall victim of being swayed by promises of financial gain from fake startups/projects in return for publicising these projects as legitimate and worthy of investment.

3. **Increased risk of fraud from fake business/ project creators who use crowdfunding campaigns to locate unsuspecting financial backers.** These individuals are then subsequently targeted to steal their financial information through the use of social engineering and deceitful promises of financial gains in return for providing bank details and/or sending money through untraceable methods. Alternatively, there is the risk that malicious actors could impersonate influential figures in an attempt to increase the investment in or perceived value of particular commodities.

Ways to adapt

1. **Crowdsourcing platforms need to ensure authentication of participants (investors, mentors and founders).** The authentication should go beyond confirming user identity and include validation of who the participants really are, their legal standing (e.g. AML checks), etc. Due to the amount of participants on a platform, the platforms will need to introduce a risk-based approach to participants. This could be based on a reputation score – an amalgamation of credit rating, and other relevant attributes.

2. **Implement security analytics tools that can help to detect manipulated increases** in crowdfunding campaign popularity through pre-defined rules or anomaly detection.

Investment Management

Automated investment platforms are creating new market entrants that provide commodity services to mass, affluent groups of customers. In doing so they are forcing traditional investment managers to focus on high and ultra-high net-worth individuals. However, the same technology innovations also create opportunities to streamline internal processes and lower the costs of service delivery, which would allow investment managers to lower the cost of services and hence offer them to previously under-explored mass markets.

To understand the cyber security impact, we have to analyse the technological impact of both innovation clusters:

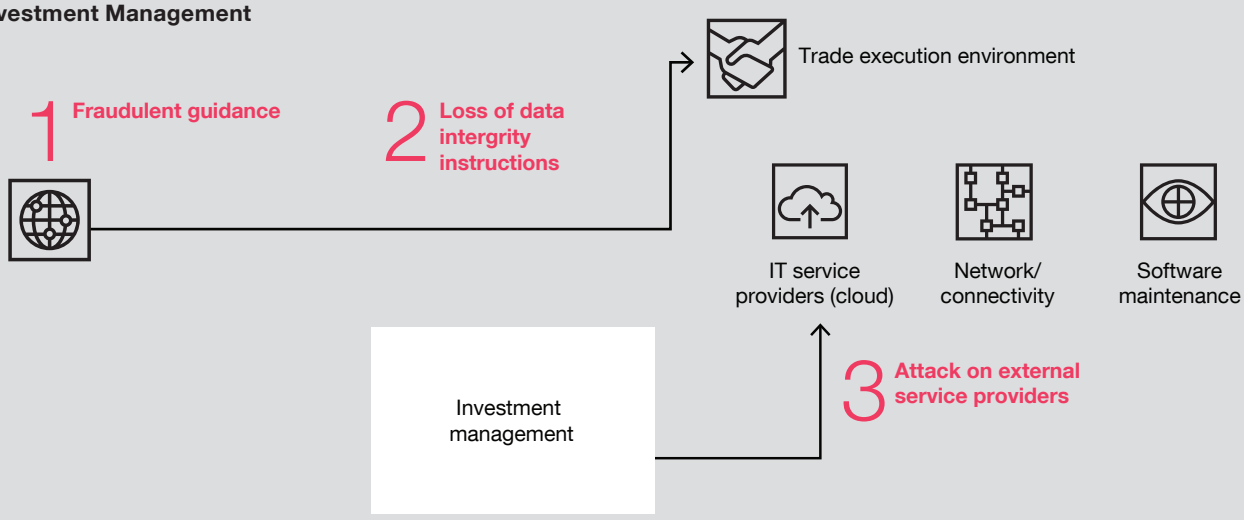
Empowerment of individuals – Automated wealth management platforms are empowering customers to control their investments without an intermediary broker. What was previously a closed community with controlled access systems is now being redefined using machine learning, and is exposed over the internet. These smaller service providers often cannot ensure the same rigour of controls to protect customer data as that seen in more established financial institutions. Additionally, smaller providers often do not consider themselves to be a Financial Services provider, instead classing themselves as technology start-ups – with accompanying contrasts in attitude.

Process externalisation – Advances in big data analytics, cloud computing, and robotics, allow the automation of many operational processes. The InvestTech propositions do just that. Automated processes can be delivered at scale using a fraction of the cost of traditional practices, so organisations are considering the outsourcing of their previously unmovable 'core' processes to external suppliers.

This raises a number of common security questions around the security of integration, supply chain assurance, and liability should anything go wrong.

Below, we have summarised the key security implications from both parties – incumbent organisations (traditional investment management organisations) and new entrants (platform service or business process outsourcing service providers).

Investment Management



Security considerations

1. **Execution of an erroneous or fraudulent trade caused by the loss of data integrity during the external aggregation or analysis of information.** This could apply to both the incumbents using third-party outsourcing, and to automated wealth management solution providers. If investment decisions are made using a complex algorithm that relies on machine learning, the integrity of the algorithm becomes paramount. Accidental or malicious change could result in financial loss and subsequent loss of trust, with the risk associated with erroneous conclusions only heightened by machine learning algorithms built as 'black-box' with little-to-no opportunity to reverse engineer those changes.

2. **Loss of trust caused by fraudulent guidance as the popularity of social trading on mass wealth management platforms increases.** Organisations will need to consider the brand value impact of fraudulent advice. If an influencer goes rogue or has their credentials stolen by a malicious actor, other users could be misled into making ill-advised investment decisions. As the number of incidents grows, customers may start turning away from the platform to seek environments more resistant to such attacks.

3. **External providers are emerging as attractive targets for cyber attacks as more institutions begin to depend on their services.** The increased dependency on specific service providers by a large number of institutions to outsource their core business processes will make these providers an attractive target for attackers who wish to disrupt these institutions or the industry as a whole.

4. **Exposure to online channel threats (e.g. business interruption)** as investment management firms increasingly move toward expanding their services to the public.

Ways to adapt

While understanding and managing supply chain risk is a common thread across all Financial Services functions, the heavy externalisation trend in investment management makes it a much harder problem to solve. The degree of complexity grows as organisations decide to outsource previously 'in-house only' or 'core' processes.

Machine learning and other emerging technologies will help investment management firms provide more accurate and tailored advice to their customers at the expense of using and producing sensitive customer information. This information will entice cyber attackers looking for personal and financial data. Firms should focus their efforts on building a strong data protection programme with the proper technical tools, processes, and people to support these efforts.

The security controls introduced by such programmes are not new, however, and understanding of the impact of control failure and required recovery procedures should be at the top of priority list for Investment Management firms as they rely heavily on data integrity and ability to quickly restore known trusted state.

Market Provisioning

Since the peak of high-frequency trading around 2010, the industry has been innovating. Advances in machine-readable news, big data, and machine learning have enabled IT departments to expand their focus from a narrow high-frequency trading area to an end-to-end automation of market provisioning activities.

This ranges from data collection enabled by machine-readable news sources, through to analytics, price discovery and order execution. New entrants to the industry have realised an opportunity to connect buyers, sellers and intermediaries through platforms that will facilitate the trading of non-exchange, less liquid assets.

Smarter and faster machines

Advances in big data and machine learning continue to reduce the necessity for humans to manually gather, analyse, and act on data. However, while the amount of effort reduces, the role of the 'operator' becomes more important – wrong decisions around configuration of the training algorithm could have catastrophic impacts.

Preservation of integrity of the source data, systems that process it and the trading algorithms will become a priority for technology and security leaders.

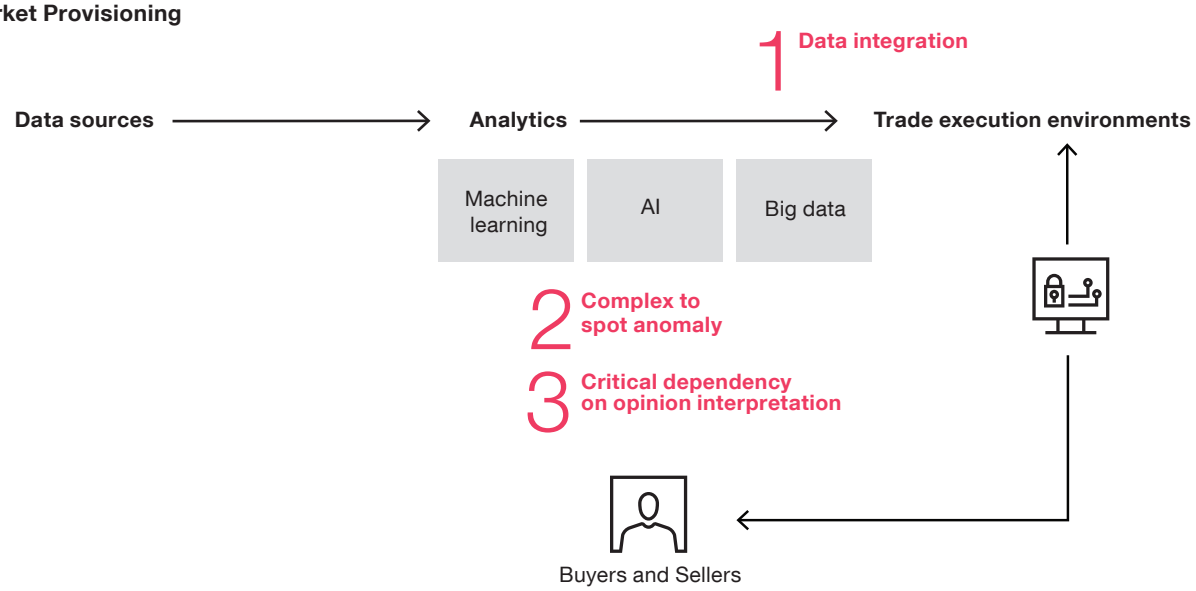
Connecting buyers and sellers

In today's model, the buyer is connected to the seller via at least two intermediaries (organisations that facilitate the trade of non-exchange assets). If the number of intermediaries grows, the cost of trade is not optimised. Since the financial crisis, increased capital requirements and reduced risk appetite among intermediary institutions have limited the desirability of acting as a market maker, reducing liquidity for many financial assets and products.

This situation gave rise to market-making platforms – technology solutions that enable standardised information flow, connection and collaboration between buyers, sellers and intermediaries.

While the technological impact on incumbent players does not introduce anything fundamentally new, beyond additional integration with third parties previously discussed in this paper, the ability to engage individual investors would require consideration from secure culture and brand protection perspectives.

Market Provisioning



Security considerations

1. **The integrity of the data utilised for decision making.** Global data feeds become an attractive target for cyber criminals looking for opportunities to launch man-in-the-middle attacks and tamper with data in transit, affecting the performance of trading decisions and potentially manipulating the market in their favour.

2. **Machine learning may reduce the identification of malicious behaviour.** Algorithms will use machine learning to self-develop, leading to increases in complexity which may make it more difficult to identify anomalous behaviour worthy of further investigation.

3. **Critical dependency on public opinion.** Future market successes will increasingly depend on changes to public views and opinions, the integrity of which may be threatened by 'fake news' and compromised media platforms. We have already witnessed cyber criminals performing similar attacks through the 'farming' of fake news to counteract genuine news and data feeds.

Ways to adapt

1. **Machine learning technologies depend on data to function correctly.** Inaccurate data can lead to inaccurate decisions that might have a drastic effect on organisations. Businesses should prioritise the protection of data source integrity as part of their overall data protection programme in order to ensure that only accurate data enters their systems. Attackers are also likely to increase their adoption of machine learning to evade security controls and to attempt to generate 'adversarial examples' in legitimate machine learning implementations that can then adversely affect conclusions.

2. **Develop industry-wide threat monitoring and response utilities** to detect and prevent cyber attacks targeting disintermediated and externalised business processes and the connections between third parties (e.g. sharing of intelligence relating to cyber threat, fraud, social media and systems activity logs by multiple market participants and key supporting service providers).

Key takeaways for the executive

Ask the right question. Often we see executives and the Board requesting “an update on cyber security”. This approach is a step forward in terms of engagement but still not adequate enough as it allows CISOs to tell a story focusing on key issues they would like to flag and discuss. This results in a tailored message that doesn’t address key points. Instead we advise Boards to set the direction by proactively asking views to be prepared on:

- What are our key cyber risks to each of our critical business services and how are we mitigating those?
- When were our cyber risk management, investment roadmap and governance approach last reviewed by an independent party? What were the outcomes?
- What are our key cyber controls and how good are these in terms of the effectiveness and coverage?

Gain a better understanding of the subject. The new digital world requires a degree of literacy in cyber security from the Board. It’s a complex topic with far reaching implications. Oversimplification of the message is detrimental to the Board’s ability to make the right decision. We often see that a complex risk issue impacting operations, and potentially resulting in serious financial liability, ends up being just another acceptable “light-amber box” on an executive dashboard. Things to do today:

- Enroll in executive cyber security training.
- Request and actively participate in cyber crisis simulation exercises.
- Speak to your peers and contacts about the issue as there is a lot to to be learned from others’ experiences.

Support and champion cyber security – Another one of the non-negotiable basics; today, when IT moves at the speed of the business, it’s essential to obtain executive support and endorsement for cyber security. Most successful organisations make cyber security part of their culture by starting with a statement from the top. Nothing works better than the CEO taking 5 minutes during meetings to explain what cyber security means to them and why it is important for the business.

Key takeaways for CISOs and security leaders

There is no question that technology innovation is disrupting Financial Services. Fintech startups, regulatory pressures (e.g. Open Banking and PSD2) and customer demand for new interaction channels are forcing old establishments to rapidly evolve.

The Agile way of adopting change doesn’t apply just to software delivery anymore; it is becoming a way of working and a moto for every organisation that wants to keep pace with innovation. This creates a unique challenge for traditional top-down, rigid, policy-driven security organisations. The security industry has been talking about “alignment to business” for a long time. Today, alignment with the business is no longer an aspirational principle for a CISO, but is in fact a survival imperative.

Achieving true alignment with the business and becoming relevant to an innovative CEO, M&A sponsor and a progressive CTO can be achieved by implementing an enterprise security architecture capability. Most successful CISOs are hiring great security architects who are given a mandate to work across transformation projects to create reusable assets, security service delivery models, architecture blueprints and patterns, and influence solution delivery cycles.

Establishing an enterprise security architecture capability will ensure there is:

- Traceability between business objectives and security requirements;
- A true understanding of cyber risk, a very pervasive and complex influencer of a broader operational risk;
- A meaningful conversation with the business/product leads less focused on specific technical capabilities (e.g. IAM maturity) and more focused on the cyber resilience of critical business services;
- A clear articulation of the value of security investments made and justification for future requirements; and
- Help to build an agile and responsive security function that can support the innovation agenda.

Contacts

Alex Petsopoulos
Financial Services – Cyber Security
Lead Partner
T: +44 (0) 7941 454210
E: alex.petsopoulos@pwc.com

Anton Tkachov
Financial Services Cyber Security
Chief Security Architect
T: +44 (0) 7769 875955
E: anton.tkachov@pwc.com

pwc.co.uk/cybersecurity

Design Services 31687 (12/18).