UK FINANCE

DRIVING GROWTH

BY BUILDING DIGITAL TRUST THROUGH CYBER TRANSFORMATION

February 2021

In partnership with PA

Contents

Foreword by UK Finance

Ensuring the security of technology and data has never been more important for financial services firms. Without establishing good cybersecurity practices, those same firms will be unable to grow and prosper to their full potential. Our members understand this, and UK Finance has been at the forefront of initiatives to build a more cyber resilient sector, including the establishment of the Financial Sector Cyber Collaboration Centre (FSCCC).

It is also true that cybersecurity has long ago shaken off the shackles of being a standalone or siloed division within firms. The need to incorporate it within software development life cycles (SDLC) is now well understood and the increased focus by the regulatory authorities on operational resilience has only highlighted the importance of cybersecurity and the need for it to work across multiple divisions within firms.

But one area that can sometimes be overlooked is innovation. The digital economy and the need for firms to transform their digital offering is clearer than ever in a world that is increasingly online and where traditional banking services can be done from the comfort of the home rather than a branch. Therefore, I am delighted that UK Finance has partnered with PA Consulting to develop this paper which aims to show how cyber transformation can be a key component when building innovation through digital trust.

This paper identifies some of the key drivers to transformation and how these impact cybersecurity strategy. It also offers guidance on how to unlock business growth through cyber transformation, including some practical steps firms can take to implement them.

I appreciate you taking the time to read this report and hope that you find it useful. I would encourage anyone with comments or observations to get in touch with our Digital, Technology and Cyber team who lead work in this space at UK Finance.

Ian Burgess
Director, Cyber and Third Party Risk
UK Finance

Foreword by PA Consulting

Covid-19 has taught us that the world can change in a matter of weeks, but also that we can survive that change and that adaptive organisations can even thrive during the most difficult of times by embracing digital transformation, underpinned by good cyber security.

In this new world, financial services firms must continue to focus on cyber security, not only to mitigate constantly evolving threats and improve business resilience, but also to unlock the growth that digital trust enables. Trust is increasingly a business differentiator, with customers demanding security by default. Taking cyber security beyond a technical specialism and putting it at the forefront of strategy at every level of an organisation has the potential to greatly improve business performance and people's experiences, setting leaders in safe digital systems ahead of the competition. Making such a radical shift requires a cyber transformation.

This report sets out how financial services firms can transform their cyber security resilience by:

- building a cyber savvy mindset and cyber secure culture
- embedding ingenious processes that encourage compliance
- adopting a trusted systems approach.

Together, these will enable organisations to safely seize the opportunities that digital transformation offers.

Elliot Rose
Head of Digital Trust & Cyber Security
PA Consulting

Cate Pye
Head of Cyber Transformation
PA Consulting

Introduction

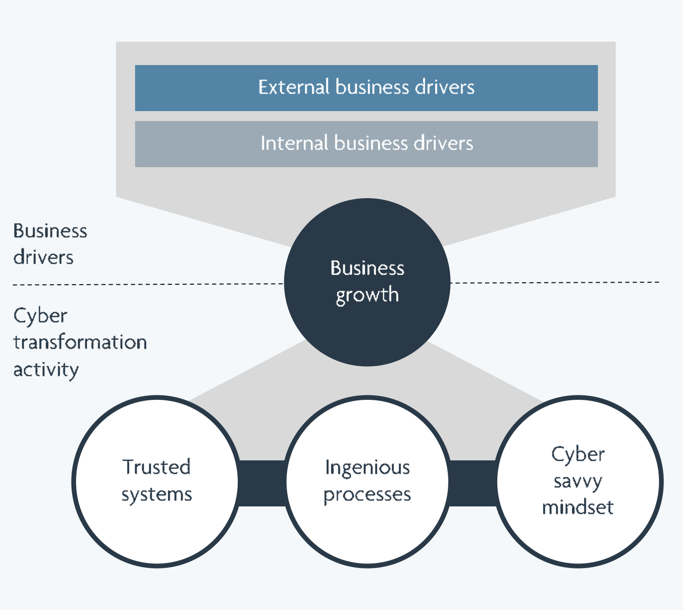
Financial services firms must continue to innovate in the current digital economy, focusing on digital transformation to grow their business and build further trust amongst stakeholders. Digital leaders expect 23 per cent higher revenue growth than other companies in the next two years[1] and with the ongoing changes caused by Covid-19, customers, investors, suppliers and staff will all expect enhanced digital experiences as our lives shift into a more remote environment for the foreseeable future. With this increasingly digital existence comes a growing need to strengthen cyber security – not only to mitigate constantly evolving threats, but also to unlock the growth that digital trust enables.

The need for cyber security can be seen as presenting challenges to digital transformation. But with the number of cyber security breaches within financial services rising, and the impact of these growing, the ability to demonstrate good cyber security is increasingly a major benefit and can help firms to build digital trust internally and externally.

According to cyber security leaders in a recent Cyber Security in Focus 2020 report from Stott and May[2], the business perception of cyber security is moving away from unnecessary expense (15 per cent) towards strategic priority (54 per cent) in the wake of greater need to work and grow remotely, and well-publicised breaches resulting in fines and reputational damage.

There has been a significant shift in attitude, with organisations now investing more in their cyber security activities. These efforts, however, still tend to focus on setting up protective technology and systems; treating cyber transformation as an IT concern. Organisations should be applying cyber security at all levels of the organisation to provide the best protection; doing so will enable digital transformation and provide opportunities for growth.

Figure 1: Aligning cyber transformation activity and business drivers to business growth



To achieve this, there must be a commitment across the whole organisation to align transformational cyber programmes with business strategy to ensure everyone focuses on the same outcomes and benefits.

A firm-wide approach with programme-level governance across transformational and BAU activity will help improve resilience and build a more cyber secure organisation.

This paper discusses how firms can drive growth by using cyber transformation to go beyond simply protecting technology and data.

We highlight how targeting internal and external business drivers, while building a cyber savvy mindset and culture, embedding ingenious processes and building trusted systems, can improve trust, drive growth and deliver firm-wide opportunities.

[1] **www.sap.com. 4 ways leaders set themselves apart**

[2] **Cyber Security in Focus 2020; Stott and May**

Identify internal and external business drivers as the guide for cyber transformation

Where to start with cyber transformation?

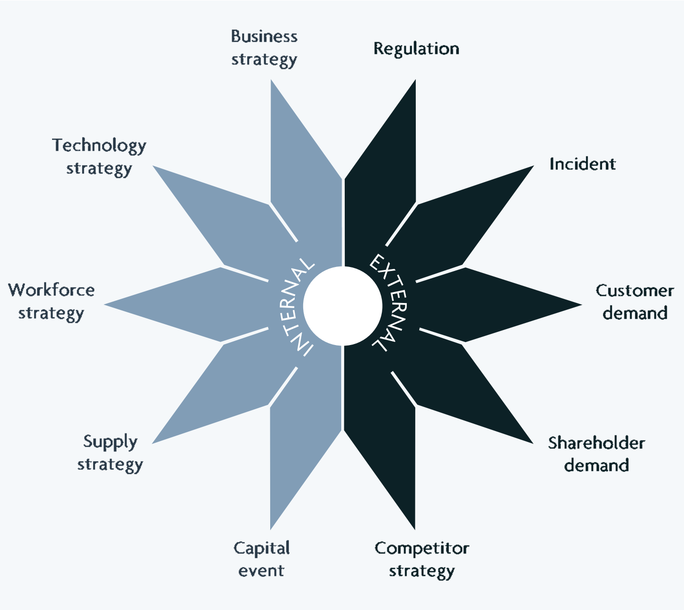
While not exhaustive, the business drivers in Figure 2 provide a clear guide for thought and discussion when embarking on cyber transformation to drive growth. These are a good route to discussion with 'the business' on growth and how good cyber security can support that. By starting with these as the foundation for developing cyber capabilities, rather than current risks and securing information and systems, you will begin to identify a raft of opportunities, such as more efficient services to customers, better adaptability and faster growth.

External drivers

External drivers are generally not under your control but understanding them may provide the catalyst to improve digital trust in the search for future success and growth. There are countless external drivers, but we have highlighted some that have been a major part of the financial services industry in recent years.

- **Regulation** – There has been a lot of new regulation over the past few years, such as the EU GDPR, UK Data Protection Act, EBA guidelines on Information and Communications Technology (ICT) risk, Digital Operational Resilience Act (DORA) and the PRA and FCA regulations on Operational Resilience. Although these can sometimes feel restrictive for operations and growth, firms can exploit new regulations as opportunities to build trust, especially as customers become more mobile and expect more security by default in the digital world.
- **Incident** – A cyber security incident, for example a major compromise of customer data, whether in your firm or the wider industry, can be an opportunity to demonstrate how you prepare for such events and how their cyber security capability could protect customers, leading to greater trust. It may also provide the catalyst to improve capabilities as post incident reviews highlight where the firm could respond more effectively; a well-executed response will go a long way to building trust and attracting new customers.

Figure 2: Internal and external business drivers to consider when embarking on cyber transformation



- **Customer demand** – A good customer experience is vital to growth, especially as customers can switch financial products more quickly and cheaply than ever. Understanding your customers is the foundation of a great experience, so cyber programmes should consider ways to build sustained customer trust through more secure and personalised services.
- **Shareholder demand** – Shareholders may require easy to understand reporting and communications to demonstrate confidence in cyber security across the firm. Explaining the linkage between good cyber security maturity and growth is vital. As a result, improved governance and reporting may help to support further investment in the areas that matter most to the firm.
- **Competitor strategy** – The actions and reputations of competitors can often cause a firm to reshape strategic decisions as they seek competitive advantage. This is just as true in the increasing move to digital services in which good cyber security is expected without any sacrifice of user convenience.

Internal drivers

Internal drivers come from within your firm and can help you to set strategy, policies and decisions to enhance your operations.

- **Firm strategy** – Cyber security programmes should align to the firm strategy; looking to protect the most vital parts of the firm's services, not just ageing technologies, enabling more effective service delivery and a competitive advantage.
- **Technology strategy** – In addition to the firm strategy, integrating cyber security solutions into the technology strategy and creating security by design will help firms prioritise and protect investment in areas that support the direction of the firm rather than protecting less strategically focused assets.
- **Workforce strategy** – Deciding how to develop skills, knowledge and experience amongst a firm's workforce, with further investment in education and awareness, will be important in working out how to deliver good cyber security, as well as having the right skills in your internal information security team.
- **Supply strategy** –Third-party service providers and partner organisations help you deliver your aims, but they also carry cyber security risks and liabilities (especially under GDPR) that you need to mitigate. Firms can design and implement cyber security to encompass third parties so that they support sustainable growth.
- **Capital event** – Capital events, such as mergers or acquisitions, will require firms to design and rationalise cyber security capabilities that complement the culture of the firms involved to maximise the potential of the new workforce and improve the operations.

Cyber transformation – building digital trust to unlock growth

Firms need to be responsive to customer demand. Cyber transformation is about moving away from just protecting technologies and data to a point where cyber security activity transforms the way a firm operates, aligning to the internal and external business drivers mentioned above in pursuit of further growth, trust and competitive advantage.

According to the Cyber Security in Focus 2020 report from Stott and May, customers are becoming more educated and demanding around the issue of cyber security, driving most respondents (69 per cent) to conclude that their business feels that functions can add value to their companies' overall proposition.

To attract new and retain existing customers, firms need to continually focus on ways to build trust through a workforce, processes and technologies that has security built in.

Trust is built through a firm's continuous demonstration that they are doing all they can, and are doing what they say they are doing, to protect their customers' data. As customers spend more time doing business with trustworthy financial institutions on and offline, they will remain loyal and continue to engage for as long as they have confidence in the firm's ability to protect their information and offer tailored or differentiated services aligned with their financial goals and life circumstances.

With customer protection at the core of the latest round of global regulations, and ideally also a firm's culture, having the whole workforce taking ownership of security measures, and pride in protecting customers' data, as a day-to-day responsibility will enable faster response and open up greater opportunities. This is especially true when it is led and endorsed by those at the top.

There was a major shift in the use of digital banking throughout 2020 as a result of Covid-19, increasing the demand for firms to treat security as a major priority for new users – many of whom are hearing of and becoming more anxious about increased cybercriminal activity. Done well, cyber security will minimise the number of incidents and increase the level of trust from consumers, opening avenues for more personalised, customer-first offerings based on the data stored and user habits.

Security monitoring capability, whether internal or outsourced, is another important way to show customers you are set up to spot fraudulent transaction activity and protect their data. Where it is the customer that spots the fraudulent activity first (whether it be incorrect transactions or they have been approached by a scam phone call), firms must be able to respond quickly, showing empathy and investigating the issues with the customer at the forefront of the response.

Firms should look at ways to be transparent with their customers on the activity they are doing to protect them, building trust along the way. For example, by being clear from the outset on what your firm uses customer data for and how it helps you provide a better service to them.

An innovative way for firms to improve their service may be to consider polling for customer priorities and product offerings; the more services can be tailored, the more trust builds, and the more customer loyalty will lead to opportunities for business growth. Where such interactions take place, an approach of "you said this, so we've done this" will show customers that you are putting them first.

Three keys to unlocking business growth

The challenge of unlocking business growth lies in building a cyber savvy mindset and culture across a firm, embedding ingenious processes and integrating trusted systems as a collaborative set of transformational activity. See figure 3.

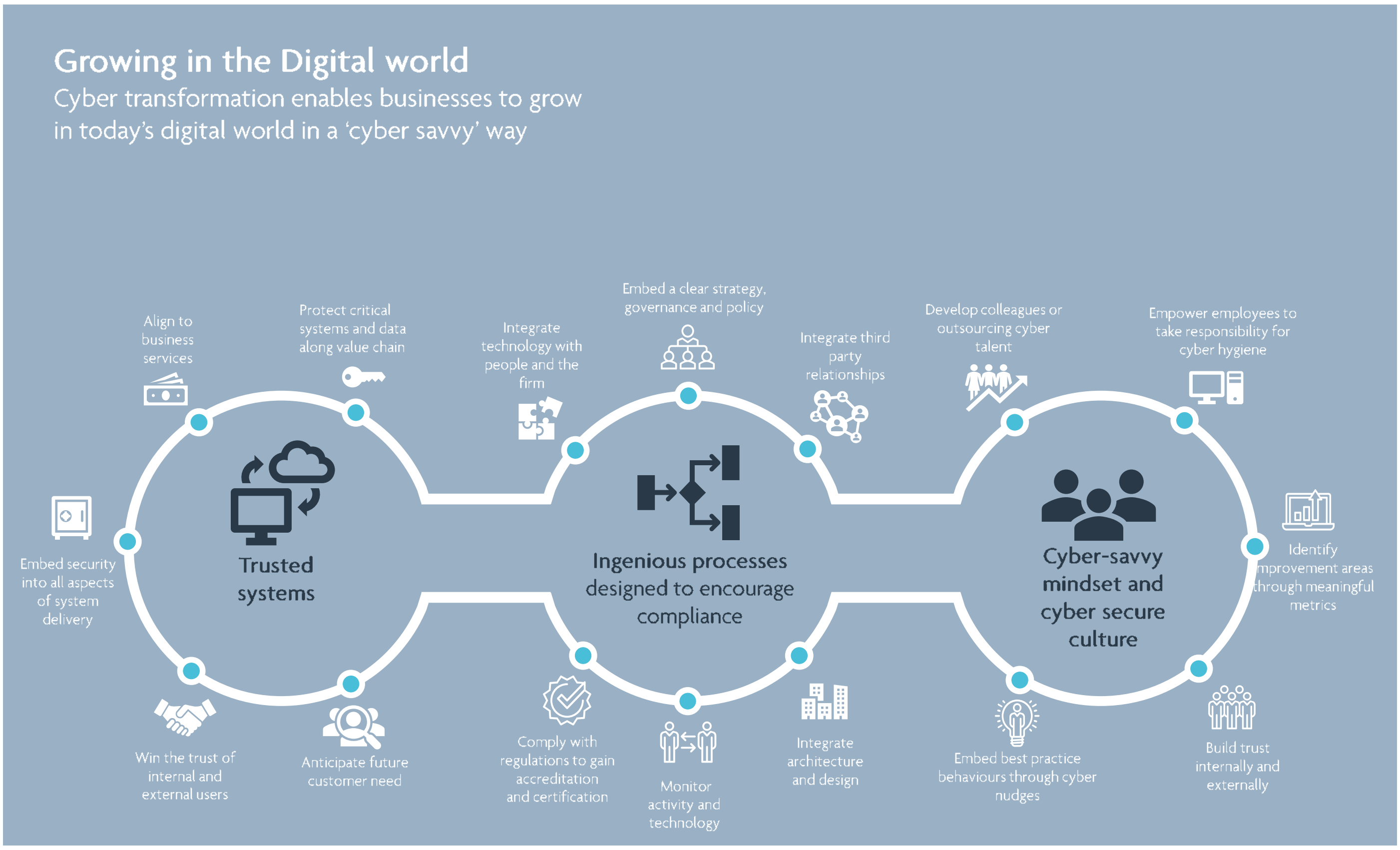
1) Build a cyber-savvy mindset and cyber-secure culture

A cyber-savvy mindset and cyber-secure culture brings the whole organisation together to look for growth opportunities while building pride in the workforce that is trusted to look after customers' data. In this environment, knowledge of cyber and information security becomes second nature and is expected of everyone.

Employees remain one of the top cyber security risks, given the access some will have to critical systems and data across the firm, and as cyber criminals invest in more advanced ways to attack firms, people play an extremely important part in building resilience, protecting information and helping the firm grow.

According to analysis by CybSafe, 90 per cent of the data breaches reported to the Information Commissioner's Office (ICO) in 2019 were attributed to 'mistakes by end-users'[3]. Furthermore, phishing attacks, a tactic through which attackers target individuals, accounted for 45 per cent of all the reports to the ICO in 2019.

Figure 3 – Cyber transformation capabilities aligned to the three core elements of a secure organisation


Growing in the Digital world
Cyber transformation enables businesses to grow in today's digital world in a 'cyber savvy' way
Trusted systems
Ingenious processes designed to encourage compliance
Cyber-savvy mindset and cyber secure culture
Align to business services
Protect critical systems and data along value chain
Integrate technology with people and the firm
Embed a clear strategy, governance and policy
Integrate third party relationships
Develop colleagues or outsourcing cyber talent
Empower employees to take responsibility for cyber hygiene
Embed security into all aspects of system delivery
Identify improvement areas through meaningful metrics
Win the trust of internal and external users
Anticipate future customer need
Comply with regulations to gain accreditation and certification
Monitor activity and technology
Integrate architecture and design
Embed best practice behaviours through cyber nudges
Build trust internally and externally

[3] CybSafe: Human error to blame for 9 in 10 UK cyber data breaches in 2019

Creating a culture which empowers employees to take responsibility for their own cyber hygiene

Building a cyber-secure culture starts with seeing your people as the potential to be the strongest link in cyber security rather than the weakest. It's about increasing your people's awareness of their personal risks and responsibilities during training and onboarding, from the Board all the way through the workforce, to alter their behaviours. Just as the opportunities created by digital transformation will benefit the whole firm, the cyber security that underpins those advances is a whole business responsibility as well. Firms should not be treating security as a capability that is just owned by security teams, it is something that spans the whole firm.

Your employees could be resistant to change, in some cases because they simply don't know what to change and why. Achieving an enhanced cyber-secure culture cannot be treated as a short-term project; it requires time, open communication on the benefits involved for all parties (including improved customer service, more efficient day to day working etc.) and awareness of the implications of poor behaviours (e.g. data theft, loss of customer trust, restrictions on the efficiency of day to day working).

The culture needs to instil confidence and empower the workforce, so it is important firms do not create a culture of fear around individual errors and provide an easy way for employees to report threats. Any of us can fall victim to phishing attacks, even security professionals. Firms will benefit greatly if employees feel confident in communicating with security teams that support rather than accuse. Attackers can meticulously design their efforts, and it's undeniable that criminals are getting increasingly sophisticated with their messaging, aligning to world issues and social trends to manipulate the emotions of some of the world's most influential people.

We are seeing increasing trends to exploit social media posts whether using Instagram, Facebook or LinkedIn. The information cyber criminals gain from these posts to tailor their attacks (e.g. phishing emails) is limitless. For example, details and dates of events you have shared on LinkedIn could lead to targeted messages on that topic, and holiday photos posted on Instagram could provoke holiday-related scam emails offering the latest deals.

Training programmes, awareness activity and leadership behaviours should be the focus when building a secure culture across your firm. Engaging stakeholders at all levels will be critical to success, helping them to understand how their actions can build trust with consumers and improve the firm in the face of increasing cyber criminal activity. This is particularly true of leadership behaviours. The rest of the organisation will emulate these so it is vital that leaders exhibit the behaviours you want to see in the rest of the workforce. Otherwise they will instantly undermine the security culture.

One innovative approach to build a secure culture based on behavioural science is 'cyber nudges', continual reminders such as pop-ups and double checks (that ask people to verify the safety of attachments or external email addresses), message boards, a security-focused section in newsletters, or security-based messaging on screen savers.

Most people respond to a helping push in the right direction, but struggle to remember exactly what the training course they did a few months ago told them to do – particularly when they are in a rush or up against a deadline.

Such nudges do not intrude on work yet deliver impressive results over time at low investment. With frequently updated messaging, firms will begin to experience a change in attitude to cyber security from password security through to reporting and responding to incidents.

Make the most of the increasingly available information to identify improvement areas

Operating in the digital world means firms have increasing quantities of security-related management information, such as internet usage, links clicked, files downloaded and erroneously addressed emails.

There have been many psychological studies that evidence people changing their behaviour when they know they are being observed – this is known as the Hawthorne effect.

Firms should examine whether security teams could analyse and report this level of information to senior executives in the form of 'meaningful metrics'. Used correctly, this can empower a firm to drive continuous improvement in security and efficiency, and help steer communications, firm wide decisions and cyber nudge campaigns based on information that is aligned to the firm-wide objectives and growth goals.

As well as building trust internally with colleagues, it is important to focus on building trust with customers.

An important way for firms to build customer trust is to demonstrate they can respond effectively to cyber security incidents.

Firms should be preparing for a cyber breach, and it is important to ensure that there are the skills and resources to quickly identify and isolate problems, determine the level of investigation and response required, to maintain business as usual, and protect customers.

A well-coordinated cyber incident response by people across the firm, who have practised together, will help protect your reputation and maintain the trust of your internal and external stakeholders.

Cyber testing and training should be used as a transformative activity to help enhance a cyber secure culture and should include all staff across the technical, operational and strategic responses, not just those in senior roles. This will create more cyber-savvy teams with a culture built on trust and an understanding of the real business impact a cyber incident can cause.

Thorough scenario exercises and a training programme that includes short, sharp exercises for more people across the organisation, will help improve the many aspects of a cyber response, such as containing incidents, collecting and analysing incident information, customer communications during the crisis, and making strategic decisions.

Developing the right cyber talent whether it's internal or outsourced

According to the Stott and May report, organisations are still struggling to source cyber security talent (72 per cent of respondents) with no material improvement around time-to-hire from 2019. In addition, it showed that internal skills still represent the biggest inhibitor in delivering cyber security strategy (39 per cent) and its associated culture.

To overcome this skills shortage, firms should be looking to become more innovative with hiring, developing, retaining and/or using external cyber talent and expertise. Firms should question whether cyber security is a core competency they need or whether they are in fact best placed to provide it. There is an increasing trend to outsource services to deliver improved cyber security capability. These may include services such as security monitoring, technical incident response and vulnerability scanning.

In any event, firms should map the change required to the current skills available within the firm. Not all firms will require or have access to the same skills. Identifying gaps internally could accelerate decisions to increase training or even tap into an undiscovered pool of people who had not so far considered cyber security as a career within the firm but have an aptitude for cyber security. There are examples of cooks, beauticians and firemen switching to cyber careers after passing tests designed to identify individuals with the necessary aptitude to excel in cyber roles. Those who pass the tests are then provided with training and before long they are able to join the cyber workforce.

Retaining staff with niche technical skills and keeping them engaged is a challenge. Colleagues are demanding the right balance of career progression and intellectual challenge to keep them motivated, innovative and driving for continuous improvement. We see firms needing to collaborate closely with employees to create progression paths that optimise their technical skills.

Depending on the size of your firm, the cyber skills you possess and the sensitivity of data to process in house, this may lead to a decision to source technical capabilities from third parties. Firms should look at the opportunities such a model can bring to increase growth, in addition to the immediate benefits of improved security and digital trust.

Practical steps to build a cyber-savvy mindset

In summary, four steps can help harness the potential of your workforce and ensure cyber security enables digital trust and future business growth:

1. Implement cyber nudges to embed best-practice behaviours in a non-invasive way for all staff either in the office or working remotely.
2. Identify the skills gaps within your information security team and implement new ways to upskill existing teams, identify untapped talent in colleagues from across the business, or outsource specialist technical skills.
3. Mandate security teams to report on more meaningful metrics that focus on business opportunities, rather than just technology risk and show that this is important to, and advocated by, the leadership.
4. Involve more people with technical, operational and strategic expertise in cyber resilience exercises so they can practise their responses as a team and not in silos.

2) Embed ingenious processes that encourage compliance

An often-overlooked way to improve a firm's cyber security engagement is by making it easier to comply with cyber security processes than to circumvent them. That means designing processes to encourage compliance; making them secure, intuitive, fit for purpose and seen to make the day job easier. It might also mean making the 'wrong' way of doing things harder or longer to do.

In deconstructing and redesigning processes, there is also an opportunity to engage people, to get them to take pride in doing things the right way and encourage their innovation. We have seen financial services firms involving their teams in this process, creating a sense of ownership that helps people feel empowered to do the right thing and to police the processes themselves.

As firms look at ways to improve their cyber security capabilities – in ways that build trust with customers, support growth and a more effective workforce – leaders should be considering the processes that link their operations, the supporting technology solutions and their people together.

There are three main groups of process-focused capabilities that, if considered as part of a cyber transformation, will help integrate cyber security into every part of the firm and lead to operational improvements:

Governance processes	Integration processes	Accreditation and certification processes
Align cyber security capabilities with business improvement and growth goals.	Integrate cyber security across your firm with technology solutions and maintain traceability of controls to your strategic aims.	Benchmark your cyber security performance, understand your strengths and weaknesses, and demonstrate your capabilities to interested stakeholders.

Governance processes

Well designed and managed governance and policy procedures will help firms to focus on growing, operating more effectively, adapting to new situations and grasping opportunities without security being a barrier to ingenuity. When firms govern security well, and align it to the business strategy, they can often identify opportunities to influence decisions around digital trust, business growth and efficiencies.

For example, including cyber security at the Board will allow the firm to understand the cyber security capabilities required to open new opportunities – some capabilities may also lead to new opportunities presenting themselves through partnerships or strategies to increase customer trust.

Earlier we discussed the positive impacts of reporting on meaningful metrics. Firms should look to implement intuitive methods for understanding the current cyber security posture of your firm by reporting on meaningful, strategic metrics. Too often, system logs, compliance reports and threat intelligence muddy the risk management reporting with too much detail and technical information. Risk management teams should instead report valuable insights and business impacts, such as industry trends, impact on business drivers, customer demands and regulatory change. Governing teams can then make decisions about opportunities for improvement and growth, not just about risks and issues.

Integration processes

Integration processes help to embed and sustain cyber security capabilities across a firm, so teams can focus on operational roles rather than constantly battling security barriers.

When talking about integrating processes, firms should consider:

- **technology integration**, to get the most out of systems and gain efficiencies
- **third-party integration**, to improve relationships with, and services provided/consumed by, third parties, partners and suppliers

Technology integration

Technology integration is critical from a security and operational perspective.

Choosing a new tool or technology capability often requires large financial decisions that put pressure on maximising return on investment. As a result, many capabilities are delivered in isolation of the broader technology landscape without considering the wider implications, benefits and integration requirements. The result is often a project that under-delivers and does not sufficiently increase a firm's security posture.

With current technology there can also be a risk of overlap whereby multiple solutions provide the same capability. When looking to increase your cyber resilience it is always advisable to review your entire security architecture to avoid unnecessary investment.

Firms should consider the following areas for opportunities to integrate cyber security with technologies as part of their growth plans:

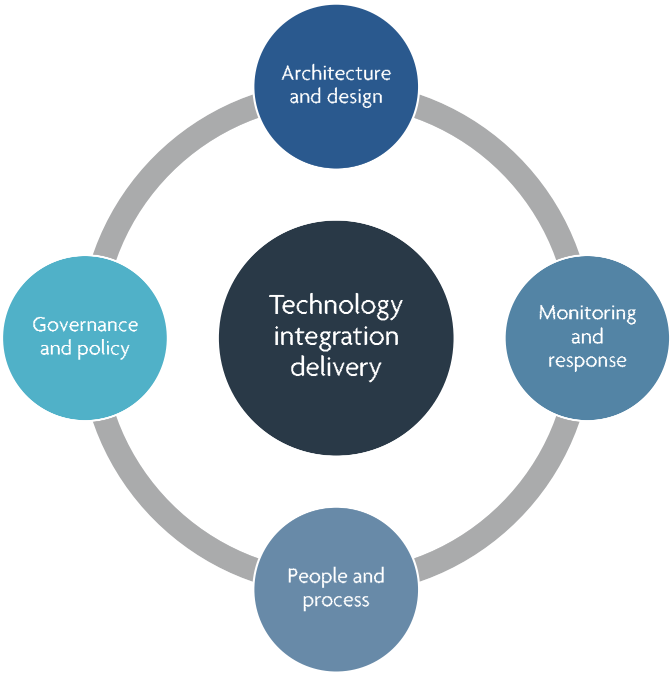
Architecture and design: visibility of the whole security architecture enabling you to create a solution that increases security posture and reduces risk or exposure. Solutions should complement and integrate with existing capabilities to improve the security of the whole firm.

Governance and policy: every capability requires governance including third party and supplier due diligence, alignment to existing governance processes and policies and amendments.

Monitoring and response: technology solutions should integrate seamlessly into current monitoring and response activity. For example, custom alerts and response activities should be written and tested as part of delivering new solutions.

People and process: delivery of any technology solution requires tailored communication and training to help manage the change. Where new processes are deployed, they should be streamlined, user friendly and ideally as intuitive as possible; users are accustomed to learning small changes quickly, due to years of training on Apple and Google products. Any new processes should also integrate as much as possible with existing processes.

Figure 4: Opportunities to integrate cyber security with technologies as part of their growth plans



Third-party integration

While the increasing use of third parties often makes processes more efficient, resilient and innovative with greater skills, services and scale, it can also add new vectors for cyber criminals to try to exploit.

Understanding the relationships and putting controls in place to make the most of them will be done by teams across the firm. It will involve complex processes, training and the involvement of people who may not fully understand cyber security.

Because of this complexity, supply chain improvements should be conducted as a transformation activity rather than a simple capability delivery project. Improving trust to support business growth within your supply chain is a multi-disciplinary process requiring clear governance, risk management, process design and integration activity. It should involve discussions across several departments, such as procurement, technology, information security, legal and compliance, as well as service owners.

An improved supply strategy should focus on partner integration, building tighter relationships and mutually beneficial security agreements to create trusted and effective supply chains.

Firms will need to ensure there is skilled resource in place to complete third-party risk processes and hold suppliers to account on contracts, resilience, cyber security and service level agreements. It is important from the outset to invest in these relationships and worth considering a review of third-party contracts to align them to your firm's security and growth objectives. Also, where longstanding agreements are in place, consider whether you have become overly reliant and trusting of their performance.

Accreditation and certification processes

Accreditation and certification help to establish the trust of customers and partners.

Internally, the correct foundational security not only provides basic guidance to bolster confidence in your security environment, but ensures no stone is left unturned under increasing pressure from a regulation, compliance and governance perspective. This is rapidly becoming a differentiator in competitive, highly regulated and increasingly digitised environments.

Firms should use standardised approaches to measure cyber security posture (such as ISO27001 and NIST cybersecurity framework) and to gain a good view of strengths and weaknesses as this will aid decisions when it comes to further cyber security investments. It will also allow you to track improvements and risk areas in your firm, allowing you to invest appropriately to maintain operations.

Another useful assurance tool, which complements the NIST cybersecurity framework and is accepted by supervisors, is the Financial Services Sector Cybersecurity Profile; a scalable and extensible assessment that financial firms of all types can use for internal and external cyber risk management, and as a mechanism to demonstrate compliance with various regulatory frameworks, both within the UK and globally.

Practical steps to take to implement ingenious processes

To design processes that encourage good security behaviours, consider the following:

1. Include a regular item at management board meetings to talk about the business impact of cyber security and help board members understand the opportunities and threats the firm faces.
2. Review how the firm integrates cyber security across technology, third party, people and firm-wide processes to understand whether further improvements can be made to support business growth and customer trust.
3. Where applicable, align cyber security activity to firm-wide policies and processes (e.g. enterprise risk management, governance, reporting and third-party relationships) rather than setting up separate processes.
4. Ensure that the cyber security team is visible across your firm as an enabler of business objectives, that they work closely with other departments and are included in all change initiatives. This will enable security to become better embedded into business and technology strategies.

3) Adopt a trusted systems approach

System security is often considered in isolation, with security mitigations applied as an afterthought.

This severely restricts the ability for security to contribute positively to the growth of an organisation and usually results in less effective security outcomes that are delivered at high cost.

A trusted systems approach changes this, firstly by encouraging consideration of systems in the context of a rounded approach to cyber security (linking to people and process), and secondly by asking value-based questions at every step of an investment. Stakeholders should be continuously challenging cyber security initiatives and asking, "How can this improve trust in the firm?" and "How does this enable us to grow?".

We recommend that firms should:

- think in terms of business services
- build strong relationships with those to whom trusted systems matter
- make sure security is embedded in all aspects of technology delivery.

Think in terms of business services

Outlined in the recent Consultation Papers on Operational Resilience[4] (CP19/32 FCA and CP29/19 PRA), there is an increasing focus on the need for firms to demonstrate their resilience across Important Business Services to minimise the impact on customers, the firm and the wider financial services industry.

Cyber security and the protection of technology and data is recognised as one of the key drivers for that resilience and carries a high expectation from consumers as previously mentioned in the Stott and May report. This growing focus on operational resilience means that communicating and addressing cyber security risk needs to be framed in these terms. The primary change that is required to existing approaches is ensuring that service-based thinking is embedded to protect the critical systems and data along the internal and external value chain. Taking a services-based approach will help firms to focus on what is important, protecting the 'crown jewels' such as customer data, transaction information and critical payments systems, while helping to prioritise investment and resources for the technology and data required to deliver faster and better services. It will also help firms focus their investment spend, since such systems will typically be linked very closely to areas of potential growth and revenue.

In addition to protecting existing business services, firms should also ask how trusted systems might support future business services in line with future strategy.

For example, we have seen enormous interest in areas such as artificial intelligence, where projects are rapidly moving from proof of concept to new product launch and from new product launch to core business.

Providing trusted systems to support initiatives that personalise customer offerings can often be the difference between success and failure in fast moving markets, and the potential for growth when done properly cannot be understated.

Build strong relationships with those to whom trusted systems matter

Trusted systems are about winning the trust and endorsement of those to whom system security matters. This includes internal stakeholders (for example, critical system users in finance or HR and accountable officers) and external stakeholders (typically customers, counterparties and regulators).

From an internal stakeholder perspective, users are key. Alongside giving confidence in the security of existing systems (ensuring that they are used to their full potential), good relationships can also inform the future direction of the business and help identify the most likely areas for growth.

[4] www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper

For external stakeholders, the picture is more complex, since firms may not wish to actively promote the maturity of their system security for fear of attack.

In this case, a genuine commitment to secure systems is of course most important, with the most compelling case for trust being the absence of breaches.

In the case of customers, providing tools and advice to protect online access to services is an increasingly important way of building trust in systems, particularly in banking, while from a regulatory perspective, an open dialogue that shows progress on securing key systems can be important, particularly where it is underpinned by recognised good practice.

Make sure security is embedded in all aspects of system delivery

Traditional risk assessment approaches have treated systems as black boxes to which cyber security risk mitigations must be applied. Where changes to systems have been made, they have occurred late in the development or delivery lifecycle, often as the result of late-stage pen testing, meaning significant and often unplanned for cost.

Many firms are starting to embrace 'secure-by-design' thinking for new systems, where security is considered as a key requirement from the outset. This can make new system delivery more efficient and in doing so enable firms to be more agile in responding to market need.

For example, we are seeing significant interest in the use of automated security tooling as part of continuous development pipelines for firms, particularly those that could be considered market leading. Such tooling enables much of the security testing that would be done manually, and often late in the day, to be moved forward and conducted far more efficiently. Not only does this reduce the overall effort required to deliver code (by addressing security issues early) but it also makes change faster, enabling firms to respond more rapidly to market need.

However, there are often tensions in terms of security measures and time to market for the delivery of new services. For example, a technical-only risk assessment might conclude that substantial hardening of a software platform is required before it can be rolled out to frontline staff. Those changes might take months to deliver or worse, might be entirely dependent upon a supplier update that does not yet have a delivery date.

A blended approach, however, might conclude that process controls could provide sufficient coverage of the risks. While inefficient, this might be the difference between launching a new service to market now or being beaten to it by a competitor. We have seen examples of this in the insurance sector, where additional controls are required for claims handling systems linked to high-value services.

Practical steps to take to deliver trusted systems

Firms moving to a trusted systems model should:

1. Align cyber security initiatives with the incoming finance sector regulations to improve your most important business services.
2. Ensure essential cyber hygiene activities, such as patching and encryption, password protection and access management are mapped out and delivered quickly. Although harder than many realise in practice, these can guard against the loss of trust following a simple breach, for both internal and external stakeholders.
3. Test existing cyber security initiatives with system users, and even customers, to determine whether they can unlock additional value elsewhere in the firm (e.g. better encryption meaning more services can be delivered remotely or using specific data to personalise services).
4. Help cyber security individuals and teams to build and evolve their relationships with the firm so they can anticipate demand, improve their understanding of what needs protecting and provide secure platforms from which to grow.

Critical success factors in delivering a cyber transformation?

As many early adopters are beginning to learn; the elements of a cyber transformation work best when integrated with other transformation activity at the heart of a firm's growth and business objectives.

This section focuses on three principles to help push transformation activity in the right direction.

Effective cyber transformation will rely on transformation leads, senior executives and sponsors investing time on the following:

Focus minds on outcomes, benefits and growth opportunities for the firm as a whole.	**Gain commitment from leaders across the firm to set the tone and create momentum.**	**Remove silos and build relationships across the firm.**

Focus minds on outcomes, benefits and growth opportunities for the firm as a whole

Where firms embark on this type of change, similar to other transformation activity, it is critical to agree the desired outcomes and benefits early.

Example areas to focus on include:

- ✓ CIOs and CTOs should create senior level consensus on the benefits and growth goals for cyber security, for example, a reduction in onerous security checks to complete tasks, increased personalisation of services or a more personal way to communicate with customers.
- ✓ Reinforce the need for delivery and leadership teams to anchor current or future decisions against the internal and external business drivers.
- ✓ Be clear on the benefits you are creating for customers and wider firm environment. For example, if you are proposing a more secure payment process or greater insight into spending behaviour, consider polling to gain clarity on the specific needs of customers and anticipated benefits.
- ✓ Track and communicate short, medium and longer-term benefits, as they are realised, to sustain motivation and momentum among colleagues and stakeholders within and outside the immediate transformation teams.

Gain commitment from leaders across the firm to set the tone and create momentum

Firms move twice as fast on digital transformation when there is a shared understanding — among senior leaders, strategists and the firm as a whole — of the digital path ahead (Gartner).

Commitment from leaders will be critical to the success of a cyber transformation; where they openly show the passion for the change, celebrate successes and behave in a cyber secure way, it will be easier for employees to follow.

Example areas to focus on include:

- ✓ Engage business leaders to align cyber transformation decisions to the overall vision and strategy of the firm, as well as all other major transformation and enterprise risk activity to ensure security is considered across the change.
- ✓ Empower technology and cyber specialists who may have previously lacked senior level decision-making authority to make decisions or propose new strategies. Diverse opinions and specialisms with technical and cultural insight will contribute to a growing firm.
- ✓ Create opportunities for people to step up and develop their leadership and cyber security skills to help them and the firm grow; regularly assess whether the right people lead the right activities with sustained motivation, direction and decision-making authority.

Remove silos and build relationships across the firm

To create opportunities for growth, cyber security will need to span the different services and functions across the firm. Removing silos, upskilling stakeholder groups and creating a culture which embeds agile and responsive decision-making will help harness the firm-wide support required to meet firm-wide objectives.

Example areas to focus on include:

- ✓ Include a set of short, medium and longer-term cyber secure behaviour principles, specific to the new processes or systems, in all delivery, training and onboarding activity. This builds consistent personal and cyber security behaviours between teams throughout the change and in the transition to BAU.
- ✓ Share successes, milestones, challenges or efficiencies to create greater trust and momentum. This is an opportunity to ensure there is a focus on the benefits and outcomes for all involved.
- ✓ Consider deploying coaches directly to, or across, different teams before and after any handover – this helps manage expectations, identify concerns and maximise opportunities the change can present.
- ✓ Identify opportunities and concerns within different teams to ensure teams mutually benefit from the change. As an example, finance teams may see cyber security as a cost centre, customer services teams will wish to do what they can to provide the best services possible and legal teams may only be interested in regulatory compliance.

By keeping these three principles in mind and aligning all activity to firm needs, people, processes, technology and wider transformation programme activity, firms could see significant improvements in their cyber security capability that lead to:

- aligned technology solutions that are easier to manage and integrate into the firm
- collaboration and alignment between IT operations and cyber security teams
- sustainable security behaviours that are adaptable and aligned to business growth
- innovative and modern solutions that drive business growth and customer trust above and beyond protection capability.

Summary

This paper highlights the core cyber transformation capabilities required to build digital trust to enable further business growth and opportunity, moving the discussion away from just protecting systems and information. It highlights ways to align all activity to the example internal and external business drivers in Figure 1.

Rather than simply looking at protecting systems and information, we seek to improve senior-level engagement and endorsement by focusing on the growth that digital and cyber transformation enable; examining the positive outcomes and benefits for the business as a whole across its technology, people and processes.

As the cyber security focus from staff, customers, regulators and the wider financial services industry increases, the expectations on firms to demonstrate compliance with regulations (notably EU GDPR and the Data Protection Act) will rise. Firms should use these business drivers as an opportunity to enhance secure services and build a competitive edge.

Cyber security needs to form a major part of any digital and cultural transformation activity as your firm looks to grow, open up new services and attract new customers in an increasingly digital environment.

A well thought through transformation approach, which brings together secure systems, ingenious processes and a cyber savvy mindset, will put your firm in a position to seize the opportunities for growth in a digital world, underpinned by cyber security capabilities that your customers trust.

UK Finance

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation. We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry.

We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

Ian Burgess
Director, Cyber and Third Party Risk, UK Finance

Ian leads UK Finance's operational and policy work on cybersecurity and third party risk management. In this role he engages with key industry stakeholders to determine the applicability of collective action on behalf of the financial sector. Through this engagement he is currently creating a single standard to assess the resilience of critical suppliers, having previously operationalised the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Before joining UK Finance Ian worked for BNY Mellon, where amongst other things he led the development and deployment of a global system to map technology risk regulatory controls to global cyber, technology and data privacy regulations. Prior to this he served as a British Army Officer for eight years.

Oge Udensi
Principal, Cyber Security, UK Finance

Oge is an experienced cyber security resilience lead working within UK Finance's Cyber and Third-Party Risk team where she engages with key stakeholders within Financial Services to ensure the collective voice of the financial sector on cyber and resilience policies is maintained. She is currently leading on cloud adoption practices and the definition of a standardised cloud security and risk framework, while she continues to play a key role in the expansion of the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Prior to her role in UK Finance, Oge established her career in cyber security resilience and has a demonstrated history within the Financial Services sector. Her expertise ranges from virtual infrastructure & cloud deployment to years of experience working in the Security Operating Centre as a Cyber Risk & Threat Analyst. She has also gained extensive experience working across the 3LoD providing Risk and Controls assurance on Technology, Cyber and Operational Resilience.

PA Consulting

We believe in the power of ingenuity to build a positive human future in a technology-driven world. As strategies, technologies and innovation collide, we create opportunity from complexity.

Our diverse teams of experts combine innovative thinking and breakthrough use of technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

An innovation and transformation consultancy, we are over 3,200 specialists in financial services, consumer, defence and security, energy and utilities, government, health and life sciences, manufacturing, and transport. Our people are strategists, innovators, designers, consultants, digital experts, scientists, engineers and technologists. We operate globally from offices across the UK, US, Europe, and the Nordics.

PA. Bringing Ingenuity to Life.

Elliot Rose
Head of Digital Trust & Cyber Security, PA Consulting

As a member of PA Consulting's management group, Elliot leads the global Digital Trust and Cyber Security capability. He has over 25 years' experience working across a wide range of sectors including financial services, defence & security, life sciences, consumer and manufacturing. Elliot's background is in information assurance and exploitation, and he has specialist knowledge in how to formulate and implement national strategy, policy and legislation. In particular, striking the balance between what is practically achievable by industry versus that which is required by legal and compliance needs.

More recently Elliot has provided evidence to the UK Parliament on the cyber challenge facing Critical National Infrastructure and supported organisations across the world on the latest data privacy laws and regulations.

Cate Pye
Head of Cyber Transformation, PA Consulting

As a member of PA Consulting's management group, Cate leads the Cyber Transformation capability and established our Women in Cyber network. She helps clients with their most challenging transformations and programme deliveries as they grow their organisations in an increasingly fast-moving and digitally enabled world. Cate is an experienced strategic partner and advisor who has worked extensively at senior levels in the defence, security and cyber sectors, advising on policy, strategy and delivery of large and high profile programmes and change initiatives.

Tom Wootton
Operational resilience expert,
PA Consulting

Chris Goslin
Cyber transformation expert,
PA Consulting

Rasika Somasiri
Cyber transformation expert,
PA Consulting

Tom Everard
Cyber culture expert,
PA Consulting

This report is intended to provide general information only and is not intended to be comprehensive or to provide legal, regulatory, financial or other advice to any person. Information contained in this report based on public sources has been assumed to be reliable and no representation or undertaking is made or given as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of UK Finance or any of their respective members, officers, employees or agents shall have any liability to any person arising from or in connection with any use of this report or any information or views contained in this report.