All hands on deck: Key cyber considerations for a new reality

Cyber threats are mounting.
Are you prepared to protect
your environment?

November 2020

home.kpmg/uk/en/cybersecurity

The world has changed dramatically in 2020. Business was already changing and the fourth industrial revolution is well underway, but COVID-19 triggered the survival instincts of businesses, who have accelerated their digitisation to succeed in the new reality. The idea that data has become the lifeblood of the organisation has been reinforced as boards seek to harness the potential of our digital economy, create new customer experiences, transform their services, and drive efficiencies and cost savings in the wake of the pandemic. The future is being created from a fusion of new business models, new technologies, and new partnerships.

In this changing world, there are ruthless entrepreneurs who are making money in this new economy. Unfortunately, they are cyber criminals and they are on the wrong side of the law. They pose new challenges to legitimate businesses, and companies need to think differently about how to protect their competitive advantage and develop new models with a goal of becoming and remaining cyber secure.

Cyber security professionals need to demonstrate they can protect the heart of the transformed business with an agility of thought and action that recognises the pace and speed at which cyber criminals operate.

They need to assemble the kind of collaborative talent — across the enterprise — that is able to take a proactive stance and meet these issues head on. The CISO can't do it all. New partnerships are needed, technology is an opportunity, not a threat, and cyber security is becoming a key business enabler.

We picked eight key cyber considerations that will likely shape the way organisations approach security in the new reality and asked our professionals to share their insights and experiences to help you meet the challenges ahead.

- **Addressing the security deficit**
- **Aligning business goals with security needs**
- **Digital trust and consumer authentication**
- **The evolving security team**
- **The next wave of regulation**
- **Cloud transformation**
- **Automating the security function**
- **Challenging assumptions around resilience**

> **Successful ongoing cyber resilience should require the strategic alignment of cyber strategies with incident response, business continuity, and disaster recovery planning.**
>
> **We've got to involve the entire enterprise — from front office to back.**
>
> **— Akhilesh Tuteja**
> Global Cyber Security
> Co-Leader KPMG International

> **Cyber security really matters this year. Working models changed forever in 2020, the threat landscape is evolving fast, and new service delivery channels are opening up. Digital isn't new, it is mainstream and security has to sit on the front line of every enterprise's relationships with their peers and customers - it's now core a part of a trusted organisation's brand.**
>
> **— Martin Tyley**
> UK Head of Cyber Security
> KPMG in the UK

Addressing the security deficit

The COVID-19 pandemic delivered a seismic shock to the working model for most organisations. In the rush to accelerate their digital transformation, the usual checks on security and privacy controls had to play a back seat role. Over the next few months, businesses adjusting to the new reality have to start by re-examining their technology environment and re-establishing control.

The landscape as we see it

When it comes to technological change, security teams prefer to take a strategic view. But for businesses who were forced to rapidly adopt remote working solutions and cloud infrastructure, onboard new technology suppliers at short notice, and switch to digital commerce channels to maintain revenue streams, security and privacy considerations understandably came second to staying in business.

The dust has settled. Businesses are now adapting to the new reality of remote working, and are beginning to understand some of the more permanent features of the change. Some people will start working from the office again when it's safe — but many employees will prefer to continue working from home. Staff will have become used to new collaboration tooling and virtual infrastructure, and customers will always be happy to have the option of digital commerce and payments.

It's up to the security team to re-establish control over the new suite of technologies that were deployed during the pandemic, secure new channels of data and payments, and adapt their controls to the new working model. But in the longer term, it's a chance to re-evaluate the operations of the security function.

The business now has higher expectations of the efficiency of the security team; they've seen how readily security was able to streamline their checks when it came to new suppliers, new application development, and new collaboration tooling. Can they take some of the lessons learned from this phase and apply them to optimise security-by-design in the new reality? With cost pressures mounting, the drive for speed, agility, scalability, and efficiency in security processes is greater than ever.

> **The more successful organisation will balance the need for addressing efficiency and staying strategic.**
>
> **Now is a perfect time to focus on cutting out the waste, cleaning up the data, and evaluating the value of your governance structures, processes and technologies, and overall controls. Is it effective in reducing risk? Think about the future of cyber in your organisation and pay attention to initiatives that enrich your data, that get you to detect faster and respond more quickly to cyber threats. Stay close to the business you are enabling and the customers you are protecting.**
>
> **— Leah Gregorio**
> Managing Director
> KPMG in the US

What we believe you should do about it

Start by understanding your assets. Your organisation's digital environment may have grown significantly over the pandemic as part of measures to transition to remote working. Speak to department leads, run detective and discovery tooling, and review procurement documents — you need to understand if any new software solutions were procured by business teams for use during remote working; what new cloud services were spun up and what applications and data they're holding; and whether there were any new endpoint devices (laptops, mobiles, hard drives, etc.) given out to support teams without your knowledge.

Once you have a view of what the new environment looks like, it's the job of the security and privacy teams to work together to review the controls of new and old infrastructure alike and understand if they're compliant to policy, and to the organisation's risk appetite. As gaps in compliance begin to show through, work with the business to remediate them. For consumer-facing applications in particular, it's critical to remind the business that the brand, and therefore revenue, is now tied to the trust that consumers place in the security and privacy of their personal data.

Think about your standard security and privacy monitoring processes as well. Have you had to skip business-as-usual assurance activities for new suppliers, review code for new consumer products, or appropriately restrict functionality on collaboration and conference tooling? Determine where the gaps are, and evidence the activities you take to remediate them — regulators may be curious to understand how you've addressed challenges.

Start planning for the longer term. Ask your business leads, development teams, and suppliers if there was anything they appreciated about security's activities during the pandemic. Review processes yourselves; were there any instances in which you realised that a streamlined process or a different set of controls still allowed you to manage your cyber risk. Think about how to embed the lessons learned into future operations.

Aligning business goals with security imperatives

Many organisations have invested heavily on cyber security, both on tooling and personnel. As businesses feel the economic impact of the pandemic, the drive to cut back on those costs is mounting. In that sense, the cost of security has became a major focus — perhaps as much as security itself. In an effort to manage costs and ensure that business and security priorities are aligned, companies are automating significant portions of their cyber functionality by putting digitised cyber risk management processes in place to ensure they ladder up to the organisation's top-line operational and business strategies.

The landscape as we see it

In reviewing many risk models, we find the concept of business-driven risk scenarios to be lacking. Certainly, the pandemic has revealed a significant disconnect between the businesses perception of value of technology and the cyber risks that come with adoption. The viewpoint of the business needs to go hand-in-hand with the viewpoint of the cyber security team and that is not the case at many organisations. The identification of these risk scenarios should be led by the business.

The process would be much more effective if it were informed by a model that enables business leads to better understand the impact security controls may have on those risk scenarios. Many companies don't get that insight consistently, making it challenging to formulate a fluid ongoing relationship between the controls and the business.

In the cyber community, we try to plan for worst-case scenarios, but many incidents happen in relative obscurity and are not earth-shattering, let alone business-shattering. From that perspective, we see many companies working to embed security, not only within the second line of defence, but within the more operationally focused first line as well as the audit-driven third line.

Larger organisations have spent, over the last 10 to 15 years, big money on IT security. The pandemic has demonstrated the increasing role of cyber security in the new reality, but there's a need to deliver that role without raising the cost. That requires them to develop a new risk-based model focused on lowering costs through an automated approach to security and putting the right people in the right roles.

> **We've seen numerous situations where security considerations are too over bearing and restrictive, inhibiting the business growth, and conversely examples where controls are too lax. There needs to be closer alignment of security with the business to ensure the right level and type of security is applied in order to maximise cost effectiveness and comprehensiveness.**
>
> **— Hartaj Nijjar**
> Principal
> KPMG in Canada

What we believe you should do about it

Think holistically about where you need to invest. Consider what risk scenarios need to be in place, and what controls are most relevant. Whatever plans companies had for digital transformation before the pandemic, they're now understanding a need to accelerate these in the new reality, while also worrying about the cost pressures. This suggests they should also explore automating their cyber and risk management processes.

Many incidents would be quite easy to detect if security policies and controls were embedded in the business. Bottom line, companies are encouraged to integrate cyber security across all three lines of defence, rather than operating in silos. Leverage threat intelligence from across multiple functions such as fraud and financial crime, and integrate playbooks and tooling to respond at speed to the changing cyber threat landscape and patterns of attack.

Make security an end-to-end priority. The foundational action is to establish an ongoing dialogue between the security organisation and the rest of the enterprise to ensure security is in sync with the business in terms of strategic and operational planning.

To that end, implement engineering approaches — such as secure by design and privacy by design — that are intended to introduce security into the daily mindset of the DevOps team as they craft new applications and services.

Ultimately, we're hoping to see cyber security professionals move away from being perceived as an IT-driven function. As such, the cyber team needs to be business-led and business-aware. Otherwise, that symbiotic handshake between business and cyber is never going to solidify.

Digital trust and consumer authentication

The world of digital commerce and banking has been thrown into warp drive this year. With that, a new set of expectations around functionality and convenience is expected from the financial sector, with trust a key component of loyalty. Many large global brands are feeling threatened as brick and mortar establishments are falling by the wayside. Whoever reigns supreme in terms of the digital customer experience is likely to enjoy the greatest market share.

The landscape as we see it

Ultimately, customers will likely go wherever the interactions are easiest and where they feel safe and secure.

In the current environment, the way to offer a better customer experience is to reduce friction. And for customers who forget a password, having a PIN sent to a mobile device via text message that has to be re-entered and confirmed is friction.

In response, many companies are leaning into a machine learning–based approach that enables them to understand their clients' typical, yet unique characteristics and behavioral patterns, such as finger or voiceprints and a variety of physical biometric traits. Financial firms, in particular, are working to understand how clients interact with them: how and when they usually log in; the types of transactions they perform, the amount of money they tend to withdraw or transfer, etc. These elements can be aggregated to produce a unique client snapshot.

For any company that maintains an interface, it's all about optimising the customer journey, establishing trust, and keeping the journey short and efficient enough to maintain engagement. If customers feel as though they're jumping through too many perceived "hoops," they will likely simply take their business elsewhere. While the customer needs to be happy and enjoy a friction-free journey to their desired outcome, it is the responsibility of the product or service provider to make sure the entire endeavour is secure.

> **Companies have to start rethinking the way they harvest data and make it available to be correlated with specific threat scenarios. The idea of data lakes certainly isn't new, but the data that is pulled in, how it's kept secure, and ensuring that only the most relevant people can access and leverage that data are all critical factors.**
>
> **— Charlie Jacco**
> Principal
> KPMG in the US

> **There's been a core focus in recent years, particularly in the U.S., on security fusion centres. It's all about becoming data-driven in the way you work to detect security incidents, and enabling a rapid-response process that is leaner, continuously adapts to the threat landscape, and seeks to remain a step ahead of the bad actors.**
>
> **— Alex Anisie**
> Director
> KPMG in the UK

What we believe you should do about it

First and foremost, companies — regardless of industry — should work to connect the data, authentication, and fraud teams systematically and programmatically. Understand the governance requirements, what data you're pulling, who owns it, where it's coming from, and how it's going to be leveraged. Build a holistic culture of security.

From there, think about how to drive a better experience for your customers where they're being asked questions to authenticate, making it easier for them to identify themselves, but perhaps more demanding to do atypical transactions. Make your clients' day-to-day interactions as easy and painless as possible, but add a little friction where it makes sense algorithmically based on common behaviors.

Make it a priority to understand the privacy and data concerns around how, and by whom, your data is going to be used. Going forward, much of it will likely be in the cloud. Think about how to encrypt and protect it. It's an enterprise-wide matter that can be solved by technology, but is ultimately based on the business' desire for customers to have a better end-to-end user experience across every interaction with the company digitally.

And companies would do well to rethink the way they evaluate data. The traditional approach of applying a massive set of rules to various data sets is no longer tenable. It's creating too many false positives and causing too many use cases to fall through the cracks for fraudsters to pick up on. The idea of leveraging machine learning algorithms to parse that data in a more efficient manner to identify behavior-based trends is key.

Finally, be alert to the correlation between people and technologies across your overall prevent/detect/respond process. recognise that the process spans the entire organisation internally, but also impacts the world outside your literal and figurative walls, considering issues can be triggered by a third party. In the end, it's about lessons learned. When it comes to authenticating users, take the time to review past incidents and reintroduce them to your security protocol for stress testing in an effort to avoid reoccurrences.

The evolving security team

Over the last few years there's been a broad attempt to elevate the importance of cyber security at the board level. In 2020 many board members are well aware of the cyber agenda.

While they understand the importance of cyber, one of the biggest challenges for security professionals is translating that knowledge into an actionable appreciation for what it actually means to the business.

The landscape as we see it

At many companies, the cyber security team remains a collection of technical, operational compliance professionals, but a transformation is underway into a more strategic, forward-looking resource that employs its worldview to impact business dynamics.

Many Chief Information Security Officers (CISOs) and their teams, in many industries, are working to adjust to the changing dynamics of the business and become a trusted and relevant voice at the strategy table. They are also working to visualise the organisation's specific operational priorities and partner with internal business heads to incorporate those insights into the company's cyber security plan as expeditiously as possible. Another critical security team focus, especially in financial services and healthcare, is satisfying regulatory requirements in a manner that is efficient from both time and cost perspectives.

The skill sets of security professionals continue to evolve. Overall, the core team needs to increase its general business acumen and product knowledge so they can better articulate cyber risk in relation to enterprise risk.

> **Accept the fact that the new world is different. Don't sit there and say, 'I've been doing security for 20 years and the way we do it is A, B, C, D — there's no other way.' Be humble enough to ask, 'What are we really trying to do as an enterprise?' Then assess the available technology and devise the best plan for your environment.**
>
> **— Dani Michaux**
> Principal
> KPMG in Ireland

> **The CISO has become a trusted internal adviser and important operational leader. Between digital transformations, a drive to extract extended value from data assets, and global priorities, every company can benefit from a business-aligned and strategically aware cyber executive with a strong, focused team to help protect and enable the organisation as it pursues new phases of growth.**
>
> **— Rik Parker**
> Principal
> KPMG in the US

What we believe you should do about it

Security teams need to get off their own island, listen to different perspectives, and communicate more with business heads about what the organisation really needs to worry about in this evolving ecosystem.

For companies that are undergoing a digital transformation — which is most of them — the cyber security team should look to insert itself into the middle of those conversations from a strategic perspective and present themselves as the connective tissue between the business, digital, and security. Have common goals.

Identify the type of data the business is planning to place on the cloud. Understand the type of interactions that will be required between the development and production environments — then map those expectations within the security plan.

Work very closely with corporate communications and the teams that are intimately involved with customer experience. Be part of the messaging strategy. Even if a worst-case scenario materialises, ensure the organisation continues to instill trust in consumers.

Ascertain what artificial intelligence (AI) is able to handle and what truly requires the nuance of human thought. Challenge yourself to automate the basic controls in your security environment. Aim for at least 50 percent.

Finally, advocate for cyber security to be a prominent feature in the organisation's environmental, social, and governance (ESG) agenda to demonstrate your comprehensive view of cyber security governance and ability to handle a broad array of incidents.

The next wave of regulation

When you examine technology risk, you're talking about IT. But when you talk about cyber risk, the ownership and accountability live outside the technology department. The trend we see in the direction and magnitude of cyber-based regulations is moving toward a more holistic approach, focusing on business priorities and responsibilities, such as customer-oriented business activities like building trust; middle- and back-office operational tasks; and board-driven corporate governance functions. In short, the focus is on management within the first line of defence, as it should be.

The landscape as we see it

In 2020 and beyond, we expect to continue to see increased regulation on a variety of topics from a variety of regulators, and since the start of the pandemic, particular attention has unsurprisingly been placed on organisational resilience, in which cyber plays a key part. In Asia, specifically, we've seen new regulations around cyber security where they've actually used the word "cyber." Previously, the regulations in that region used the word "technology," which had an IT connotation. The increased precision is a welcome development.

With so many countries having issued rules to comply with certain elements of the General Data Protection Regulation (GDPR), or their own privacy laws, we're seeing — especially with larger multinational companies — the creation of new, proactive data management departments. Essentially, businesses are looking to master data analytics as a discipline and understand not only where the data is located across the organisation, but also who owns it, what's being done with it, and, perhaps most critically, what rights and permissions users have in relation to that data. This is more important than ever for businesses to get right as data ethics and the privacy rights of individuals remain a key in the new reality.

Companies are recognising the need for additional investment, not just in tooling and process development, but in terms of a lack of cyber talent, from cyber governance and risk strategy to configuration and maintenance. There's still a large gap in this space, and, unfortunately, many companies hire IT professionals who lack cyber security perspective in relation to the regulatory environment. The result is advice that is often ineffective or well intentioned, but misunderstood or inadequately implemented by management and the board.

What we believe you should do about it

Regarding the three lines of defence model, we suggest embedding the responsibilities of cyber security, as well as the role of the CISO, in the first line — preferably formally — and linking these tasks to annual performance targets. The CISO role, at its core, should reside in the first line to cover security strategy and vision, and he or she should have a clear hierarchical or at least functional alignment with security operations regarding daily monitoring and tool configuration.

The second line (i.e., IT risk) should support design quality and resiliency policies and standards, and report back to management and the board. The third line would review and assess the work of the first two lines. This optimal state seeks to extend the company's cyber security needs, including regulatory compliance, across the entire organisation.

We also believe it's critical to institute ongoing testing of your regulatory compliance program in terms of design, implementation and effectiveness to identify where improvements are needed. Also, ensure operational cyber resilience is embedded into your overall architecture and processes to solidify security for both IT and OT.

Appoint an individual who is not strictly an IT person to oversee regulatory compliance. In fact, new CISOs should become more comfortable speaking the language of business in order to ensure his or her messages are understood and executed. This individual should have a broad mindset regarding the company's operating model — a Chief Risk Officer, Chief Financial Officer, or Deputy CEO would be ideal because they also have perspective on the company's overall risk agenda. This individual would be the sponsor or champion for cyber security across the entire organisation, working in close partnership with the Chief Operating Officer and CISO.

Take the time to unify all of your regulatory requirements, from internal controls and policies to the various regional and country-specific regulations, into a single Unified Control Framework to help enhance the effectiveness of your internal governance, risk, compliance, and testing efforts. Look for synergies between the controls demanded by privacy, resilience, and security regulations — you may be surprised by what you find.

Companies are encouraged to shift their focus from systems and technology to information. Pinpoint what it is that makes you competitive in the market. It could be intellectual property, or your supply chain, or your pricing power. Whatever it is, that's what you need to protect from a cyber security perspective.

Cloud transformation

One of the things many companies need to work on is aligning the CISO's organisation with the rest of the enterprise regarding the maturation and efficacy of the cloud. The pandemic forced many businesses to accelerate their digital transformation, and cloud adoption, which might have taken 18 months, was completed in a matter of weeks. Security may well have been an afterthought as businesses scrambled to equip themselves for the new reality. Moving forwards the CISO and his or her team must develop processes and tooling that are vital to, and fully be aligned with, the business drivers and the technology needed to support the desired business outcomes from the outset.

The landscape as we see it

Historically, IT has been responsible for infrastructure provisioning, and, before the cloud, was primarily focused on the challenges on the ground (pun intended). The security team is charged with scanning that infrastructure for vulnerabilities, but they often don't know what to scan because there often is a disconnect with IT on an updated threat list. Managing infrastructure and the related assets has always been demanding, but in the cloud, where everything is faster and more ephemeral, getting security involved early and hardcoded into the provisioning plan is a challenge many companies are struggling with.

In terms of the cloud, across multiple industries, the CISO's organisation is largely not prepared to enable the business, neither in terms of skills nor talent. In the cloud, the priority is information protection. What we're finding more and more is that the way data is being deployed in the cloud is often not necessarily resilient. We're not simply talking about multiple availability zones, but the ability to recover critical assets if there's a major breach.

At many companies, we're seeing two camps that seemingly operate at opposite ends of the security spectrum. On one side are the old-school practitioners who have been working in security architecture for 20 years or more, but haven't fully adapted to life in the cloud. On the other you've got cutting-edge security professionals who are all in on today's technology and are trying to promote and enable the cloud mindset so security can be embedded by design and at scale. In the wake of the pandemic and the rapid acceleration of cloud adoption by businesses, getting these factions on the same page is a priority.

> **Security teams have to realise that it's okay to break things as long as you learn something from it quickly and apply that knowledge productively. A lot of organisations don't have the confidence to think this way. A culture of experimentation and learning is what will attract the type of cyber talent companies need in today's rapidly evolving marketplace. The cloud enables you to build and break things fast, rebuild, and realise incremental successes.**
>
> **— Caleb Queern**
> Director
> KPMG in the US

Security team action

Become a learning organisation. The thing that attracts cloud talent, beyond money, is culture. Prospective employees need to know they're not walking into a classic, hyper-risk-averse, slow-moving organisation. You can attract strong cloud talent by creating a culture that's open to innovation and experimentation.

Similarly, think small, but act fast. Send the message that you build things fast, break things faster, and then rebuild based on what you've learned. You have already proved that you can move fast in reacting to the pandemic, now is the time to translate any lessons learned into business as usual. Security can enable success through incremental steps. For example, go live with a new container protection strategy in small bites, and enable the business to move fast.

Shift left and push controls as early into your software testing cycle as possible in an effort to deliver maximum value to both customers and users. Apply security — again, in small bites — as far left in the process as possible, which typically involves infrastructure as code. Make it happen by empowering developers to hard code the required security measures without the security team's involvement, which the cloud can facilitate.

Have an appreciation of the underlying code — the ability to read and write code can earn the respect of DevOps engineers. And seize the opportunity to really understand where you should embed yourself. Increasingly, that's what we're going to see from security professionals — the ability to code, because more and more, we're moving away from that traditional security architecture role of measuring diagrams and handing it over to a solution designer or solution architect to then build a solution, which then goes to an engineer to stand up physical infrastructure.

Work to understand — and communicate to the entire enterprise — the connection between business enablement, business resilience, and information protection. It's not much of a departure from how you would do it on premises, but it's a little bit different when you've got critical data across regions in the cloud. Making this part of your DNA enables you to weed out the "noise" from an operations perspective so you can focus on the bigger security priorities.

Automating the security function

Before COVID-19, we were already seeing a shift to automation of security functions from identity authentication through to threat detection and response. Over the course of 2020 the pace at which this is happening has picked up. A broad set of know-your-customer (KYC) and fraud detection data is being gathered and analysed by many sectors, including financial services, eCommerce/retail, technology, media and telecommunications, and automotive, among others. This information has previously been siloed by function.

In the new reality companies are beginning to realise they are sitting on a treasure trove of data that — if better organised and made more efficiently accessible — can be extracted and analysed for a variety of value-added purposes, and even to relieve rapidly growing cost pressures caused by COVID-19.

The landscape as we see it

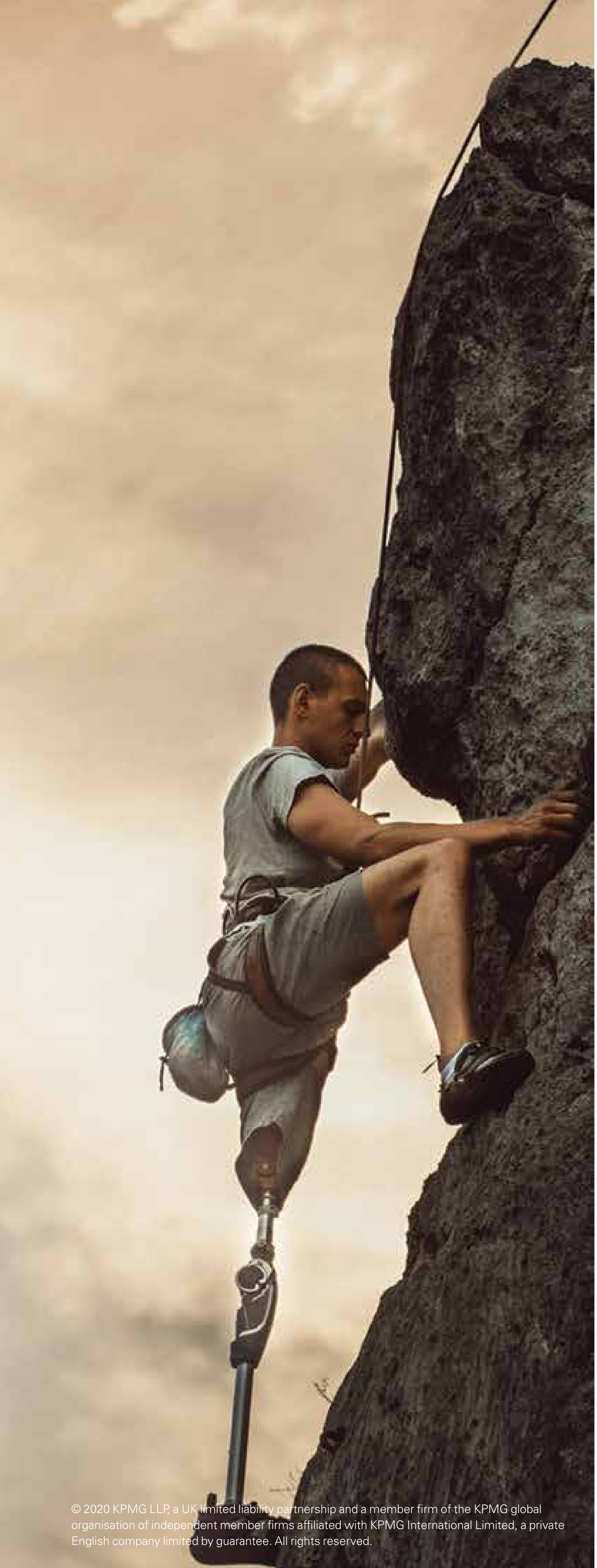
The economic impact of the pandemic has been massive for governments and business alike. Revenues have been lost for many and investment budgets have come under growing pressure. Such pressures do present companies with an opportunity though; to become more efficient across all business functions, including security. Companies are therefore working hard to automate functions that until very recently have been purely manual, by pulling together historically disparate data sets.

Not only are businesses better able to confirm that digital customers are who they say they are, they are also acquiring deeper information, such as who has a virus on their computer, who recently received a phishing email, and who tried to enter a network to which they don't have access.

Security professionals are combining third-party tools and in-house solutions to automate as much of the overall cyber playbook as possible, and align it with the organisation's business development and customer experience objectives, as well as tackling the challenge of shrinking budgets. Companies are looking to automate the first and second lines of defense via the cloud to better respond to threats across the enterprise without a human having to do that work, while simultaneously confirming that the security controls they expect to have in place are indeed operating as expected.

Unfortunately, security teams are not alone in adopting automation. Threat actors are also automating, scaling, and commoditising their attacks. These improvements help them to accelerate the speed at which they target businesses. This only emphasises the need to automate the security function and improve business ability to manage its cyber threat at pace.

> **As CISOs look to reduce spend and improve the effectiveness of their teams, automated deaccessioning of outdated digital assets should become a pillar of their overarching strategy. They should similarly explore automating their security operations center playbooks, fraud decisioning, and cyber response through partnerships with leading cloud and security information and event management providers.**
>
> **— Anthony Gawron**
> Director
> KPMG in the US



What we believe you should do about it

Always remember: Whoever controls the data has the power. With that firmly in mind, the first step is to transfer your critical enterprise data from the different third-party vendors that so many companies maintain across their systems into a centralised, accessible location.

We also suggest advocating for a data normalisation initiative within the organisation to scrub and properly label the data so you understand what data you have, how it's being posted, and what features are available within the datasets.

Organisations in the early stages of maturity in terms of data normalisation may not be equipped to jump right into insight extraction through AI and machine learning.

For these companies, it's important to prioritise the use cases they want to address — fraud detection, customer experience enhancements, operational efficiency improvements, for example — and determine how to plug in the right tools, technologies, and advanced analytics to leverage the data once it's available.

These use cases can help you determine the data you need to integrate, but more than that can ensure you focus on high-impact examples to demonstrate early benefits to a potential sceptical business and help justify the investment for the next tranche of use cases.

Cloud providers can help you achieve this, providing an increasingly flexible range of compliance and security monitoring capabilities, as well as scalable and adaptable analytics (and security orchestration) platforms.

Challenging assumptions around resilience

The events of this year have fundamentally changed the calculus of technology and cyber resilience planning. The shape of the technology ecosystem has altered; attitudes towards resilience have evolved; and regulators are considering new approaches to supply chain continuity planning. Enterprises preparing themselves for the future should reimagine their approach to understanding, planning and executing resilience efforts, encompassing security teams, the business, and the broader operating ecosystem.

The landscape as we see it

If there could be a silver lining of this pandemic for security and infrastructure teams, it would be that organisations now understand the degree to which technology underpins business productivity and revenue. In enterprises dominated by remote working and cloud deployments, it's no longer enough to think of technology as an enabler to business — it is the business.

While there's an increased appreciation for the role of security in resilience, the new reality has opened up a new set of targets and challenges, which require novel approaches. New virtual infrastructure models have changed the priorities of both threat actors — who are now being creative over their use of phishing and malware — and business continuity teams in response to the threat. And the new working models are forcing SecOps teams to review their incident playbooks, detective and responsive tooling, and shift patterns.

At the board level, some of the fundamental assumptions of business continuity planning have been challenged. Can businesses assume anymore that their network of incident response suppliers, data centres and archive services are working as normal? What does a worst-case scenario really look like in the post-pandemic reality? Organisations need to take a much more holistic view of their technological dependencies and single points of failures — including third parties and off-shore teams. And with an eye over the whole architecture of the business, security needs to play a vital role in outlining and managing the threats.

Meanwhile, regulators are paying close attention. With nation states becoming more active in the cyber threat landscape, and cyber attacks on many industries being used to serve economic and geopolitical agendas, governments will be undertaking resilience planning at the sector and nation-state level. Organisations supporting those plans will need to offer unprecedented levels of co-operation, transparency and trust, working with competitors, suppliers, regulators and law enforcement bodies to ensure resilient ecosystems.

> **Cyber has historically been quite asset-based, aiming to preserve the technological foundations of the business. If it can pivot to a more holistic, service-based approach, working laterally to focus on the primary business driver of service continuity, security teams have an opportunity to elevate cyber BCP methodologies to enterprise-wide resilience governance.**
>
> **— Andrew Husband**
> Principal
> KPMG in the UK

What we believe you should do about it

A few key actions can help an organisation to refresh their resilience planning activities in preparation for the new reality. Start by questioning some of the key assumptions that have been made in the past — did your list of worst case scenarios include the pandemic? What could be the next example? Can you rely on your ecosystem for support, or do you need security resilience skills in house?

Think about the mechanics of the first line of defence. What's changed about security operations in the new reality — can analysts work in the same way they have done? Do you need to offer new routes of access to key security incident and event management (SIEM) tooling to cater to new working modes? Communication pathways need to be updated as well — can you rely on corporate collaboration and conferencing tools? How do you interact with partners such as cloud providers? And how do you manage the containment of malware when you can't guarantee immediate access to an endpoint, as you would in the office?

Rethink how you devise your playbooks. The pandemic will have demonstrated to many businesses that a number of the same threats lead to the same fundamental impact on technology and the business. By reorienting your playbook design from scenario-based to impact-based, it's possible to cover all bases in a much more efficient way. It also helps the security team to capitalise on the new found appreciation of business teams for the impact of technology infrastructure.

Work with business teams to understand the long-term consequences of the pandemic on their working models. It may be that those models change your priorities by presenting a different threat surface. Ransomware might start targeting VDI solutions rather than databases, holding to ransom business productivity instead of data — ask yourself how to adapt your response and recovery efforts to new operating models. And re-assess your priorities — do you have to worry as much about "loss of building" scenarios as much as you used to, or are "unavailability of personnel" scenarios now a higher likelihood?

Finally, start making external connections. As cyber attacks grow in scale and complexity, we'll have to start relying on each other. Develop supportive relationships with regulators, law enforcement, industry peers, and up- and downstream suppliers. The shape of the technology has changed, both globally and locally, and a good faith culture of transparency and collaboration can help alleviate pressures on critical infrastructure and services.

How KPMG can help

At KPMG, our global organisation of cyber security professionals offers a multidisciplinary view of risk. Helping you carry security throughout your organisation, so you can anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

No matter where you are on your cyber security journey, KPMG member firms have expertise across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, we help you develop advanced solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents.

To inspire stakeholder trust and protect the future, you not only need advanced technological expertise and deep business understanding to make cyber security a strategic enabler of your ongoing transformation. You also need creative people who bring innovative thinking and practical implementation to the automated world.

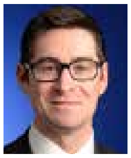
KPMG can bring this uncommon combination of strengths, and we use them to help you get an enviable combination of your own: confidence, agility and competitive advantage.

Together, let's create a trusted digital world, so you can push the limits of what's possible.

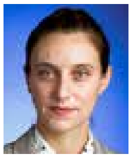
home.kpmg/uk/en/cybersecurity

Contact us

Martin Tyley
Partner
UK Head of Cyber Security
KPMG in the UK
T: +44 113 2313934
E: martin.tyley@kpmg.co.uk



Neil Clarke
Cyber Security Lead
National Markets, South
KPMG in the UK
T: +44 117 9054183
E: neil.clarke@kpmg.co.uk



Alex Anisie
Director
KPMG Cyber Security Services
KPMG in the UK
T: +44 207 6941587
E: alexandra.anisie@kpmg.co.uk

David Ferbrache
Global Head of Cyber Futures
KPMG Cyber Security Services
KPMG in the UK
T: +44 203 920 0492
E: david.ferbrache@kpmg.co.uk

Andrew Husband
Principal
KPMG Operational Resilience
KPMG in the UK
T: +44 207 6941040
E: andrew.husband@kpmg.co.uk

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/uk

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

Create | CRT132059