KPMG

From enforcer to influencer

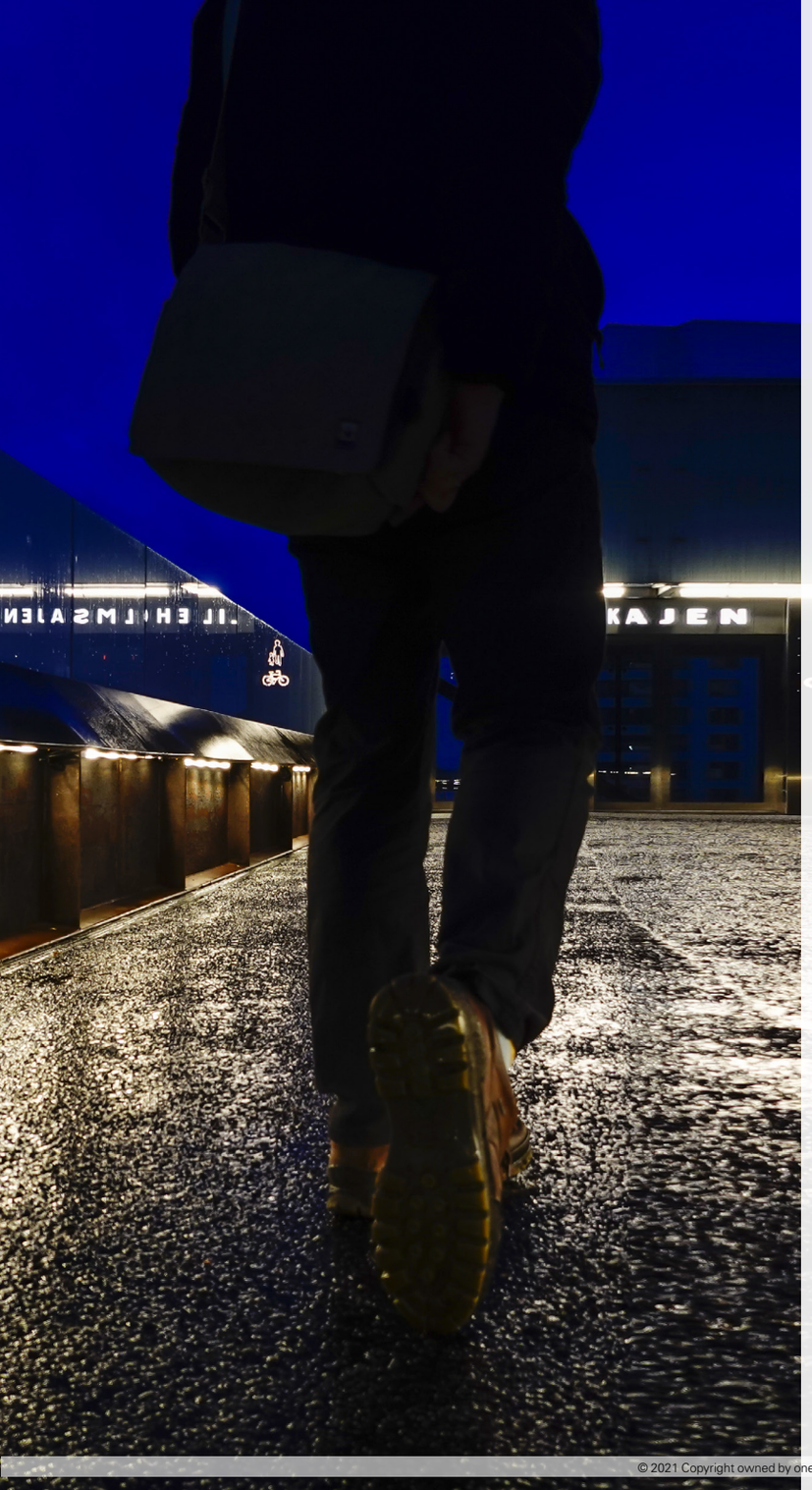
Shaping tomorrow's security team.

KPMG International

home.kpmg/cyberinfluencer

Contents

Click on the topics to learn more.



Executive summary

Enablers of digital transformation — the evolving role of cyber security

The former racing driver Mario Andretti famously said: "It's amazing how many people think that brakes are for slowing the car down." And he was right — brakes are for making the car go faster, safely. Which I feel perfectly sums up the role of cyber security in today's organizations: to enable them to enjoy the fullest benefits of digital transformation, while managing the many risks.

COVID-19 has magnified both the opportunities and threats of digitization. Organizations have made incredible strides in remote working and collaboration for employees, as well as improving digital customer experience. But this has also reminded us that physical perimeters no longer exist. With increasing reliance on third parties, and the proliferation of Internet of Things (IoT) and other devices, cyber security now involves complex ecosystems with a dramatically increased threat potential.

In a marketplace where speed to market is essential, cyber security teams are now responsible for building trust and resilience, by forging a pragmatic security culture and helping embed secure by design thinking into every aspect of digital infrastructure and data. To do this, they must see themselves as enablers and facilitators, helping others deliver services and brands that deserve cyber trust among customers, employees and society at large.

To find out more about how cyber security roles are evolving, KPMG professionals spoke to a number of Chief Information Security Officers (CISOs) from major organizations, from a wide range of industries and regions, as well as to KPMG's cyber security specialists from around the world. I would like to personally thank all those who contributed.

We have distilled insights from these thought leaders with the aim of providing pragmatic advice to help address the main challenges facing tomorrow's security team.

Fred Rica
Principal, Cyber Security
KPMG in the US

Seven actions for CISOs

1. Act like you belong in the C-suite

CISOs must speak the language of the C-suite, building consensus, demonstrating pragmatism and navigating politics, to help leaders understand the cyber implications of their strategic choices. CISOs are also becoming public figures, serving as the face of the firm to help build trust and confidence.

2. Broaden horizons

CISOs' responsibilities are broadening to include safeguarding data, dealing with disruptive events to maintain operational resilience, managing third parties, handling regulatory compliance, and helping to counter cyber-enabled financial crime. This demands they forge strong working relationships with other business leaders, including the Chief Risk Officer (CRO), the Chief Data Officer (CDO) and, of course, the Chief Information Officer (CIO).

3. Weave cyber security into the organizational DNA

Today's CISOs should be sophisticated communicators, working with other business leaders to embed cyber security into the DNA of the organization. This involves integrating security into governance and management processes, education and awareness, plus establishing the right mix of corporate and personal incentives to do the right thing.

4. Shape the future cyber security workforce

CISOs will have to acquire capabilities from outside the organization, build new partnerships and look for unconventional and diverse talent. In future, we may even see the cyber function becoming far smaller, taking on a strategic and governance role, with cyber security being truly embedded into the business.

5. Embrace automation as the rising star

Automation can reduce the manual workload and ease skills shortages, bringing in greater efficiency and helping meet growing compliance requirements in a consistent and repeatable way. It can also help embed security and improve the user experience, as well as reduce the time to respond to a major cyber incident.

6. Brace for further disruption

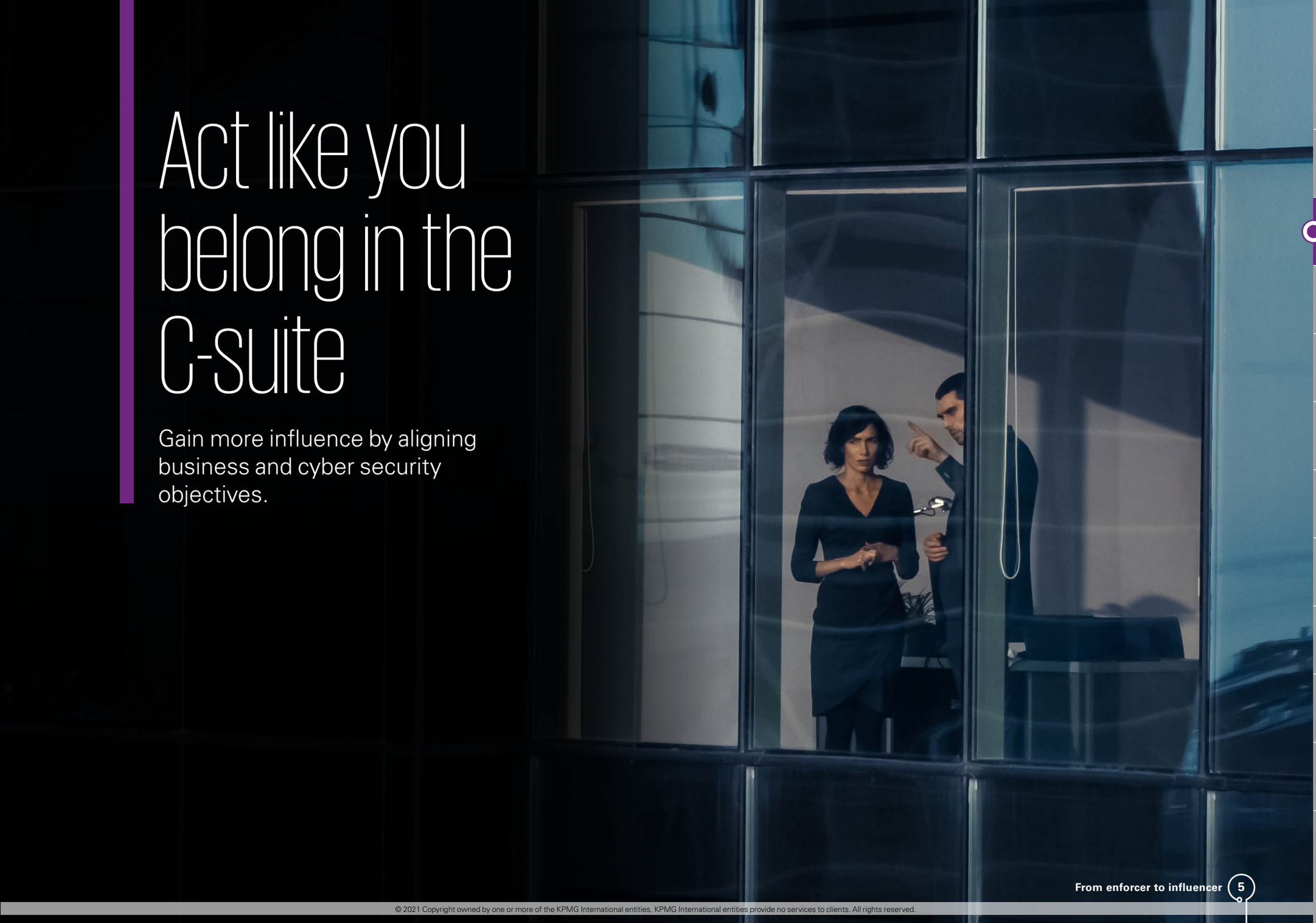
We are heading towards a hyperconnected world in which the IoT and 5G networking will massively increase efficiency and enable radically different business models. But this also opens up organizations to new attack surfaces, and raises privacy concerns — demanding a shift to new, data-centric security models such as zero trust.

7. Strengthen the cyber security ecosystem

Organizations are now part of a complex ecosystem of suppliers and partners, tied together through shared data and shared services. Conventional contracts and liability models seem ill-suited to the rapidly evolving supply chain threat, calling for a new partnership approach that brings security to all parties and individuals.

Act like you belong in the C-suite

Gain more influence by aligning business and cyber security objectives.



Cyber security is now a common topic of boardroom debate. In the KPMG 2021 CEO Outlook Pulse Survey, cyber risk was ranked as the number one organizational threat by global CEOs, with data security taking a priority over all other technology investments.

Senior executives and non-executive directors have become all too aware of the impact of incidents such as data loss, ransomware and fraud, which can bring operations to a standstill and destroy revenue and reputation.

But they also face a dilemma: They want to rapidly digitize the business, but are starting to recognize that moving too fast, without considering security at the design stage, can also bring risks.

As companies become ever more dependent upon digital technology, every business decision has a cyber security dimension. The CISO's priorities are shifting from firewalls and identity management to major strategic challenges like brand trust, product security, resilient operations, and robust supply chains.

More and more CISOs are getting a direct line to the CEO, but are they really prepared for such an elevated role? As the saying goes: "When you get to the end zone, act like you've been there before." CISOs need to start thinking that they deserve to be members of the C-suite, focusing on problem-solving and becoming business enablers, with a stake in innovation, growth and revenue.

Speaking the language of business risk and opportunity

▸ Addressing the challenge

In stepping up to a C-suite role, CISOs must acquire new skills and mindsets, to focus less on pure security and compliance, and more on broader business risks and opportunities.

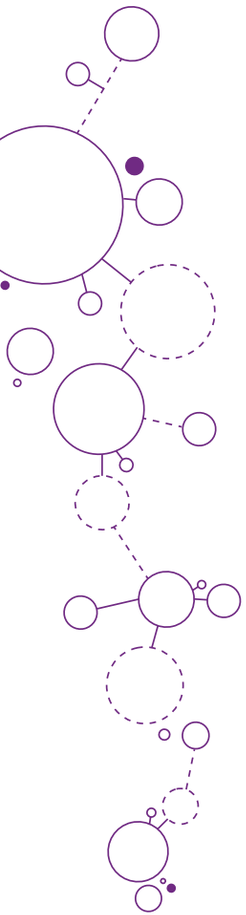
Here to help the business and enable revenue

Today's businesses must be fast to market, yet avoid releasing products and services with cyber vulnerabilities. There will always be occasions when CISOs need to apply the brakes, but, by getting involved at the earliest stage of new product development, they can embed security by design and reinvent themselves as business enablers who ultimately help the company go faster, more safely, preserving digital trust.

A common view of risk

In the words of Leon Chang, Head, Cyber Defence Group, IHiS, "CISOs that go to board meetings with ill-prepared technical presentations are setting themselves up to fail." As risk advisors, CISOs should eschew technical detail and speak to the board on its terms, explaining the cyber threat landscape and associated risks to customers, growth, revenue, costs and brand. By using a common language for cyber and operational risk, which resonates with the board, they can frame a constructive debate on cyber security risk — and emphasize the need to embed cyber security in corporate strategy and major investment approvals.

> "You need a strong CISO who can articulate the total landscape of risk. This requires a real understanding of the organization plus a technical understanding of the cyber landscape. The board discussion is about giving them the confidence that you're managing risk and moving to a better place."
>
> **Lisa Heneghan**
> Chief Digital Officer
> KPMG in the UK



Investing in risk mitigation

According to Palo Alto Networks' VP and CISO, EMEA, Greg Day, "If you can't quantify and qualify the scope of the problem, in terms of threat to revenue, it's hard to get the resources. So, I give my board three solutions: gold, silver and bronze. Gold mitigates a higher proportion of risks but requires a larger investment, and so on. Then the board can make a trade-off.

Influencing rather than enforcing

Influence at board level can often be informal, a result of relationships forged with multiple stakeholders. In navigating the corporate jungle, CISOs need to gain trust, by attending meetings of finance, marketing, operations and other functions, to both learn about business risks and educate about cyber threats. CISOs can also bring compelling individuals in front of the board, from within and outside of the cyber team, with interesting outlooks and insights into risk, to articulate the importance of cyber security. In this new, C-suite world, it's all about influence, as Greg Day, VP and CISO, Europe, Middle East and Africa, Palo Alto Networks, puts it: "A CISO is not a great CISO because of a huge budget and massive team. It's because they've empowered the business around them to go ahead and be successful."

Working in the gray zone

▸ KPMG thinks

The elevation of the CISO role into the C-suite is good news for everyone involved in cyber security, but CISOs must prove they're up to the task. CISOs should articulate to the board and executives how cyber security plays into all decisions, to reduce risk and improve business outcomes — it's not just about fear. Integrating into corporate strategy involves a more holistic approach to business, moving out of the technological comfort zone and becoming storytellers. CISOs should also avoid being reactively driven by regulatory compliance, and recognize the benefits of leading the security debate and anticipating the regulatory drivers.

Working in the gray zone of corporate politics may prove especially challenging for the many CISOs from technical backgrounds. Every organization will get hacked at some point, so the CISO has to demystify cyber security by explaining what an incident could cost the business, and the degree to which investment in cyber security can reduce risk and accelerate recovery. CISOs can bring unique perspectives and insights into the modus operandi of criminals or malicious attackers. Most mature organizations will have well-established enterprise risk management systems, and the CISO should seek to embed cyber security into these.

Managing expectations is another tricky balancing act. Sales and marketing executives want to swiftly launch and enhance new products and services, operations need to run 24/7, while customers expect their data to be secure. By working with CIOs and their DevOps teams, CISOs can help others become heroes, embedding cyber security and making full use of automation, enabling new revenue streams, keeping the lights on, and enhancing trust in the organization.

> "The real advantage of going to the cloud won't come from cost savings, but from speed to market, innovation, scaling up faster… so we must focus on what we can do to enable the business to move faster, safely, securely and responsibly."
>
> **Gary Harbison**
> VP and Global CISO
> Bayer

> "The objective of bringing a cyber person to the board is not to let others relax when the subject of cyber comes up, but to lift the understanding and capability of everyone else, which transforms the quality of discussion."
>
> **Martin Tyley**
> Partner and Head of UK Cyber Security
> KPMG in the UK

Broaden your horizons

Taking on wider responsibilities, formally or informally, calls for an open mind and an eye to the bigger picture.

Today's organizations are composed of a mesh of third parties and individuals, plus thousands of IoT devices, all with varying degrees of access to data and systems. Remote working has added to this fragmentation, with a dispersed workforce operating from geographically dispersed home offices; a very different environment to the comfortable security of the corporate office block.

If a malicious attacker in one part of the world can shut down a factory or a port thousands of kilometers away, or bring down a global bank's customer website, then cyber security must adapt to these threats. Abid Adam, Group Chief Risk and Compliance Officer, Axiata, emphasizes that "It's about more than your own organization; the fabric of nations, of society at large, can be threatened and undermined if a large telco goes down for a couple of hours. We need to embed security by design and achieve broader resilience."

All of which extends the CISO's responsibilities to digital and operational resilience. Data has become the new oil, arguably more valuable than physical assets, as Maersk CISO Andy Powell comments: "We need to become a digital business — a digital business that moves boxes, rather than vice versa. The bigger markets come from customer-facing digital platforms." But an ever-greater reliance on data puts additional pressure on CISOs to protect this precious resource.

Meanwhile, privacy regulation is growing into a complex web of transnational obligations, with regulations such as the General Data Protection Regulation (GDPR) in Europe setting requirements for how individuals' personal information is handled well beyond that geography. Information leaks can impact a company's reputation, lead to fines and other sanctions, requiring the CISO to work in partnership with the Chief Data Officer (CDO) and Chief Privacy Officer (CPO) to manage the risk of non-compliance.

It's a similar story with resilience. The proposed European Digital Operational Resilience Act (DORA) will oblige financial services companies to demonstrate their ability to maintain resilient operations in the face of severe operational disruption.

Cyber security teams should focus on data and resilience issues. Embed the principles of privacy and culture of security, and they will be well placed to meet compliance obligations, now and in the future.

Developing new skills and networks

▸ Addressing the challenge

As the scope of their role broadens, CISOs must consider how they work with other data and resilience executives, and how they adapt to their new responsibilities — formally or informally.

> "As the pandemic demonstrated, resilience is a big topic — and CISOs and their teams should be involved in response planning and business continuity, to help ensure organizations can react and recover to cyber incidents, as part of a holistic, cohesive strategy."
>
> **Hartaj Nijjar**
> Partner and Cyber Security Leader
> KPMG in Canada

> Resilience is about engaging in conversation about the business impact of an outage, and how we plan for these events. This becomes an interesting conversation, because redundancy costs money, so how much are you willing to invest and is this worth it to prevent downtime?

Tammy Klotz
CISO, Covanta

Embedding digital resilience

There is a confluence of the roles of CISO, Chief Risk Officer (CRO) and the Chief Security Officer. As cyber security matures, expect increasing technical security controls embedded into the CIO's processes, with many CISOs taking on a more strategic role that fits less comfortably with their traditional reporting line to the CIO. Some of the CISOs KPMG professionals spoke to have taken on the emerging role of Chief Resilience Officer; this is a new corporate position that takes a holistic view of the organization's resilience to all forms of stress or disruption, malicious or accidental.

This resilience role brings together diverse disciplines such as business continuity, disaster recovery, information and physical security, alongside incident and crisis management.

Others regard this as a step too far, seeing the role as diluting the necessary focus on cyber security, with a combined role of CISO and Chief Resilience Officer being too demanding for a single individual. Emma Smith, Global Cyber Security Director, Vodafone, concurs with this approach, saying "The risk areas covered in security, privacy and resilience are broad. Leading the strategy and managing the operational aspects of all these functions can require different approaches and sometimes these areas may conflict. We believe there are business benefits from keeping the functions organizationally separate, strategically aligned and with true collaboration."

Safeguarding data

As every business becomes a data business, the debate continues over the limits of personal data exploitation and privacy. Companies want to make the most of data, which means being free to mine and share information with third parties. But they also have to preserve data integrity and meet regulatory standards. In companies like Maersk, the CISO enjoys a close relationship with the Chief Data Officer (CDO), where the latter sets data standards and the CISO builds tools to help assure data, with the Chief Privacy Officer (CPO) or Data Protection Officer (DPO) helping assure regulatory compliance.

Combatting fraud and financial crime

CISOs can bring unique insights into the mind of the cybercriminal and the tactics they employ, as well as their own contacts and relationships with national cyber security, threat intelligence and law enforcement bodies. These skills and insights are vital to the fight against fraud, working closely with fraud prevention teams (another key partnership) to counter cyber-enabled crime.

> There are two points when you can try to solve a problem — before or after it occurs — and my job is to solve it before! Alongside this, we regularly look at worst-case scenarios and make an assessment of what the impact would be on our organization. We seek to always be prepared for extreme risks. Our approach is to assume that these events will happen and to ensure that SWIFT is as resilient as possible.

Karel De Kneef
Chief Security Officer, SWIFT

Broad-minded and collaborative

▸ KPMG thinks

With more on their plates, many CISOs are becoming collaborators, building symbiotic relationships with the CDO, CRO, CTO, CIO and others. But to make these relationships effective — and to take conversations out of silos — there should be defined responsibilities and a clear governance structure to avoid duplication, along with a willingness of all parties to recognize each other's strengths and unique contribution to business success.

A broader role also calls for a broader mindset, to try to appreciate the full business impact of cyber incidents. CISOs are moving beyond protect and detect, to understand how to get the business back up and running quickly after a crisis — as well as helping the CEO preserve trust with customers, suppliers and regulators.

Whether they take on the role of Chief Resilience Officer, or work more closely with this person, they should adopt a pragmatic, business-minded approach while retaining their own integrity and professionalism. Many organizations possess huge amounts of new and legacy data; managing this requires extensive collaboration between the CISO, CDO, CTO and Chief Data Privacy Officer (CDPO), both to use data to drive growth, and to keep it secure and private.

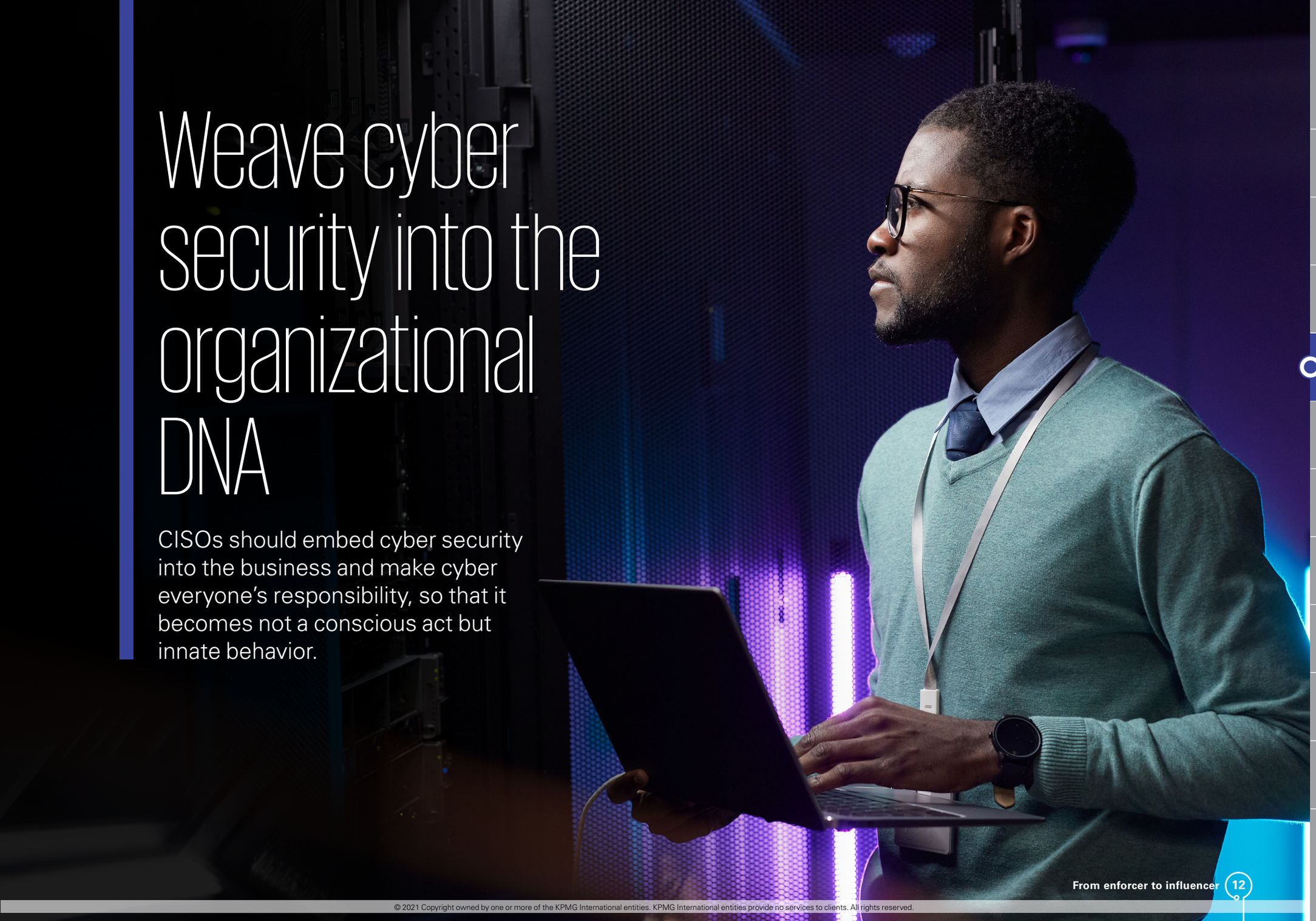
This is especially the case for global companies in an increasingly fragmented regulatory landscape, with different jurisdictions applying strict rules on usage of data emanating within their borders or derived from their citizens. CISOs have a key part to play in helping to automate regulatory compliance, tailoring controls to different national requirements, and streamlining reporting. Of course, we can also expect to see a growth in the use of supervisory technology (suptech) by regulators too.

> "Industries are being disrupted and CISOs must have a view of the changing ecosystem, or else face obsolescence. Telecoms, for instance, used to be about getting a phone connection; now there's more concern over digital fraud from online banking apps. Cyber security professionals should adapt to these and other new challenges — like data and resilience — to take a high-level view of risks across the business."

Leandro Antonio
Cyber Security and Privacy Leader and Partner
KPMG in Brazil

Weave cyber security into the organizational DNA

CISOs should embed cyber security into the business and make cyber everyone's responsibility, so that it becomes not a conscious act but innate behavior.



How often do you hear about increased cyber security budgets immediately following an incident — signposting a move from constrained spend to an overnight demand for action and investment? But security shouldn't be an event-driven, knee-jerk activity; it must permeate every part of the organization, from product design to customer service, supply chain to production.

Cyber security should be a key part of building trust and integral to corporate strategy — not an afterthought. It's the same with DevOps, where developers tend to be incentivized on speed to market and not security, with inevitable consequences. In industries like construction and oil and gas, safety has become second nature. All the operations have embedded a safety culture, helping employees instinctively avoid incidents by encouraging, measuring, rewarding and publicizing responsible behavior. CISOs should follow a similar path, and perhaps even build on that culture in those industries where it already exists.

For cyber security teams, the new, subtler role of influencer may take some getting used to. CISOs themselves should think less in terms of security empires, and more about orchestrating a resilient, cyber-aware ethos where everyone is accountable for their contribution to corporate security.

Agents of change

▸ Addressing the challenge

Embedding cyber security into the organizational DNA requires CISOs and their teams to become evangelists, to make security processes second nature and to change behavior, while also respecting the differing organizational cultures found in development teams.

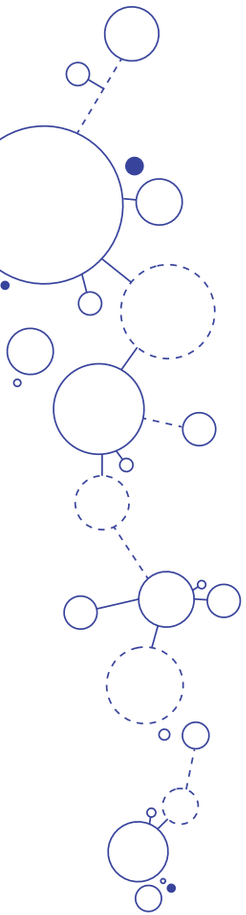
Change starts at the top

CISOs must invest time building strong relationships at board level, articulating risk and explaining how cyber, when done right, can enable the business. Once the board and executives buy into the concept of implicit security, CISOs are in a stronger position to spread the message more widely, knowing that they have leadership support.

Forging a security culture

CISOs can exert influence by being visible, and giving individuals the knowledge and the power to practice good cyber security habits. This doesn't just apply to employees, but also to any third parties handling data, such as contractors, suppliers and partners. As Covanta CISO Tammy Klotz explains, there's nothing like building one-to-one relationships with key stakeholders: "It's not rocket science. It's about having a presence, having conversations, investing time in understanding the business operations you support and protect, to show you understand what's most important. I call it 'getting into the other person's movie'. My entire first year in this job was about building relationships. You can't do Operational Technology (OT) security without visiting a facility and getting your hands dirty."

> If you haven't considered cyber security as part of your conceptual product discussions, you're probably too late."
>
> **Dani Michaux**
> EMA Region Cyber Security Leader and Partner
> KPMG in Ireland



From DevOps to DevSecOps

Development teams remain reluctant to integrate cyber security, fearing it will slow down their efforts and seeing it as a corporate overhead. In some organizations, CISOs fund cyber security specialist roles within DevOps teams as a free resource, to work to integrate security into products, using a standard approach. By doing this, the CISO enables rather than dictates, and creates development evangelists respected by their peers who can show how security practices are embedded into development pipelines.

Donating cyber skills

Vodafone is using a DevSecOps model, getting involved in product and service design and development. They want to empower development teams by appointing a security champion, providing training, tools and where possible reusable code. American Express has a similar philosophy, as Michael Papay, Executive VP, Enterprise IT Risk and Information Security, explains: "We embed specialized resources across functional areas to drive awareness and swiftly address information security and risk issues. These people understand the business challenges and apply a security lens to ensure the most effective response. This model also serves the dual benefit of creating a best practices feedback loop."

Gamification

Particularly relevant for product developers in DevOps teams, gamification is a great way to enthuse and engage people on the importance of cyber security. It lets developers integrate security within their daily jobs, with the ultimate reward of a faster release into the market. Other events like 'Capture the Flag' games can help to upskill the DevOps team and build closer relationships.

Cracking Operational Technology (OT) security

Security is not just about servers and laptops, now that computers have become ubiquitous. Today's industrial environments are heavily dependent upon software, hardware and IoT. However, the culture of managing OT can be very different, an engineering mindset, a focus on availability and safety, and a strict approach to managing downtime. In championing OT security, it's important to get into the heads of engineers, understand their objectives, win their confidence, and demonstrate that threats are real. Cyber professionals can then develop pragmatic solutions reflecting the reality of legacy systems, complex vendor landscapes and the need for 24/7 availability.

Incentivizing common good

Axiata is just one company that opts for what they call a 'Collective Brain' approach, as Abid Adam, Group Chief Risk and Compliance Officer, says: "We incentivized the different operating companies to work properly together and drive consistency. We restructured KPIs and remuneration, which meant they all had skin in the game. They were then tasked to come up with solutions that solved not only their problems, but the problems of other operating companies — and aligned with their business too."

> Our role has shifted from security awareness to behavior management. This means fostering better digital citizens, with phishing exercises, gamification and other methods to change behavior and understand the importance of information security wherever you are."

Jim Nelms
CISO, LabCorp

Segregating OT risk

With many research and manufacturing sites around the world, GSK is engaged in a multi-year program to gain an enterprise view of risk. Although each site has its own responsibility for OT upgrades, the central cyber security function will have the capability to contain the risk to one location in event of an attack.

CISO as a broker, integrator, orchestrator

▸ KPMG thinks

People are often called the weakest link in cyber security. But actually, they can be critical to cyber security if they are well educated, supported and incentivized to make the right decisions, and understand how their actions impact the security of customers, operations, intellectual property, money, and reputation. By acting as a kind of 'Chief Cyber Security Marketing Officer' CISOs can foster a true security culture, constructing an effective cyber brand that's aligned with the organization's mission and values.

The nature of the cyber threat is subtle, sophisticated and constantly evolving, which calls for learning techniques based upon social cognitive theory, to make security second nature, and enable employees to look out for and recognize hackers and criminals. This is especially so when combatting fraud and financial crime, where everybody involved in the customer journey should be fully connected and committed to protecting customers' data and money.

The new hybrid world of home and conventional office-based working brings multiple threats, often from unaware family members using the same networks. Every employee should be taught to treat the home as an extension of the workplace and become 'CISO of their own house'. The most successful awareness campaigns make it personal and educate employees on protecting themselves and their families, not just the company. It's also important to recognize the demographics of the workforce. Different age groups have very different views on data security and privacy, which will influence the messaging on cyber security.

There's more than one way to embed security. Some favor a hub-and-spoke model, with a smaller, core security team that performs security operations, with security professionals embedded into lines of business — or 'donated'. In such a structure, the cyber security function becomes a broker, integrator, orchestrator; a big leap for technically minded security professionals accustomed to enforcing from the comfort of their desks. Automation will make the task easier, taking every day manual checks out of the hands of busy workers.

> "With organizations digitizing at warp speed, we need to embed security in every process of developing solutions and products, so that people think about security before transforming and as they transform digitally."
>
> **Leah Gregorio**
> Managing Director, Cyber Security
> KPMG in the US

Shape the future cyber security workforce

A combination of outsourcing, gig workers and automation will transform the way that capabilities are accessed.

Cyber security faces a critical skills gap across a wide range of areas, including cloud security, OT security, data science and analytics, security architecture and engineering, and attack simulation. The war for talent is made even tougher due to high demand for many of the same capabilities across IT, pushing up salaries and increasing attrition.

The average CISO's tenure has been estimated by Forrester at just over two and a half years for UK CISOs and just over four years for US CISOs,[1] and many are well aware of their market value and increasing demands (not least from regulatory obligations) leading to stress and burn-out. Another challenge for busy CISOs is acquiring the 'soft' skills necessary to forge relationships and influence behavior, as they and their teams become cyber evangelists.

Consequently, there are moves to professionalize cyber security, and to formalize qualifications and career paths in this youngest and most dynamic of occupations.

Looking further ahead, new roles are evolving that may not even exist today, such as resilience strategist, cyber risk modeler, orchestration manager, behavioral analyst, and AI ethicist. Vendor management has also taken on greater relevance, with the surge in outsourcing and third party partnerships — especially for cloud-based services, where cyber teams must share responsibility for security — so perhaps an ecosystem security architect too.

> "Cyber may in future operate with a small core team and many subcontractors and gig economy workers, tapping into a global pool of resources, which could help resolve some of our talent challenges. But we need to know that people are trustworthy. I envision a kind of 'trust ring' being built around people, who are vetted by other trustworthy people."

Fred Rica
Principal, Cyber Security
KPMG in the US

> "My role as a leader and manager of people must focus even more on mental health and wellbeing. Cyber security professionals are expected to prevent or stop any incident, but we all know that's not possible — it's asking too much. If you ask a CISO about their expectations for an incident, they'll likely say 'we'll get sacked.' This is unhealthy and must change, which means focusing heavily on pastoral care of my team. I'm incredibly strong on this."

Darren Kane
Chief Security Officer, NBN Co, Australia

[1] UK CISO Career Paths, Forrester Research, Inc., March 24, 2021.

In shaping the future cyber security workforce, CISOs will have to consider how to access both existing and new capabilities needed to stay on top of emerging threats, rebalancing the skills within their organizations to meet the changing demand.

Bridging the cyber skills gap

▸ Addressing the challenge

Whether hiring, retraining or outsourcing, the CISOs KPMG professionals spoke with have some innovative ideas on how to possibly address the skills shortage.

Harnessing automation

Automation will play a vital role in the cyber workplace, as Joanna Burkey, CISO, HP acknowledges: "The cyber industry has deep structural challenges. We can't keep up with the pace of technology change from a skills perspective, we can't get enough talent in, and never will, and we can never assume 100 percent retention at any time. It's not possible to keep up with the pace of technology change without embracing automation."

Maintaining the pace

Automation is vital for low-value activities like connecting with ticketing systems and automating workflow. Global Cyber Security Director Emma Smith says "Automation helps increase efficiency and retain interest for analysts. Addressing root cause issues is essential to keep improving and learning, so we don't keep dealing with the same issues."

Are these the cyber security roles of the future?

Re-emergence of deep technical skills

The trend for cyber security generalists appears to have declined, with a new demand for and appreciation of people with strong technical capabilities, as Emma Smith, Global Cyber Security Director, Vodafone, notes: "Technical expertise, rewarding engineers and technical skills, creating a new model for building career paths, are fundamental to our strategy. I think organizations now realize the importance of both leadership and technical skills in cyber security teams."

Reskilling

Retraining existing cyber professionals is costly and takes time. GSK SVP and CISO Matthew McCormack observes that: "Reskilling is a challenge. To use a motoring analogy: Motorbike mechanics can't become Tesla mechanics overnight!" As technology transformation puts pressure on existing capabilities, it's likely to take 2–3 years to upskill the current workforce, to cope with the shift from on-premises and access protection to cloud, mobile, IoT and big data.

Looking outside the profession

CISOs can bring in people with in-demand skillsets like data analytics, risk management and cloud as core technical disciplines before 'converting' these individuals into well-rounded cyber professionals. They don't have to be cyber experts: What's more important is that they understand the business and are willing to learn. Such a move would help overcome the lack of diversity in cyber security, encouraging new skills, backgrounds, perspectives and opinions to look at the same problem from multiple angles. Decrypting Diversity, a 2020 KPMG in the UK/National Cyber Security Centre UK paper, surveyed diversity and inclusion in cyber security. Of those experiencing career barriers, 32 percent said it was due to gender discrimination, and 22 percent cited race, ethnic, social background or regional discrimination.

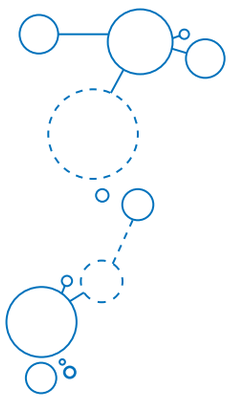
> "There's less of a skills gap than a diversity gap. A team, with diverse skills, backgrounds, opinions and perspectives will give us better answers."
>
> **Leon Chang**
> Head of Cyber Defence Group, IHiS

Collaborating to expand the talent pool

Forming partnerships with universities and colleges and investing in young talent has the dual benefit of training individuals and fostering loyalty. YPF CISO Brian O'Durnin feels that "By offering apprenticeship schemes and university places in regions with high unemployment and an underprivileged population, we'll contribute to the profession in general. Even if some of these people don't end up working for us, we'll be contributing to the ecosystem of cyber security and making the world a little safer."

Outsourcing

The trend towards outsourced labor is only likely to accelerate; with CISOs in some cases looking to lower-cost locations, as remote working rises in popularity. The gig economy is also likely to increase, with cyber security professionals seeking greater flexibility over where and when they work; a trend reinforced by the shift to remote working during COVID-19.



From 'doer' to enabler

▸ KPMG thinks

To shape a dynamic 21st century workforce, CISOs must constantly assess what capabilities they need, and then source these skills from within and outside the organization — using a hybrid model of permanent hires, temporary workers and contract models.

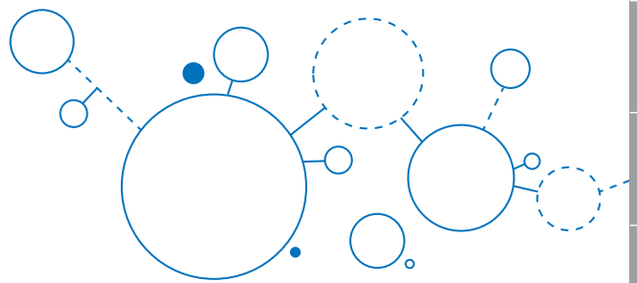
Increasingly, we are likely to see CISOs outsource some of their operations. This may be to specialist providers that can scale up and down at ease; professional services companies offering transformation support and strategic advice; and niche service providers and contractors. And, as organizations continue to migrate to the cloud en masse, CISOs will look to cloud service providers for a growing range of security activities.

With automation taking over the bulk of transactional tasks, the cyber workforce is transitioning from 'doer' to 'enabler', focusing on new product development, operational productivity and resilience, and larger, strategic cyber initiatives. However, it will take time to get this partnership between human and machine right.

A key question for CISOs will be 'What skills do I need to retain in-house?', to establish a core that lets the organization govern its security, set strategic direction, make tough and informed choices on risk, and manage incidents and crises. Beyond this core will be a complex tapestry of sourcing strategies and relationships with outsourced and co-sourced suppliers, who provide the scale and specialist skills needed for security operations, as part of the shift to a shared responsibility model. Increasing regulatory expectations around the role and competence of CISOs and their teams will also impact roles and responsibilities.

And, while it's vital to attract talent from peripheral industries into cyber security, it's also helpful to encourage cyber practitioners to move in the opposite direction. Not only will this enhance career prospects, it can also spread awareness of the value of cyber in other functions and integrate cyber security more deeply into every employees' thinking, until it becomes second nature. For instance, cloud engineering and legacy IT teams are swapping people to add greater rigor and security to the former and pace to the latter. This type of cross-fertilization extends to diversity and inclusion, as well as neurodiversity, which can bring huge benefits in terms of creativity. Cyber could also do more to embrace new workforce initiatives like returning parents, late career employees and retirees, all of whom can add to the skills base.

> "The good news for cyber security professionals is that they're becoming more important and more visible, with their roles encompassing a wider range of challenges like collaboration tools and transformation, giving them a chance to expand their commercial and strategic skills and build richer careers."
>
> **Lisa Heneghan**
> Chief Digital Officer
> KPMG in the UK



Embrace automation as the rising star

Bringing a host of efficiency and workforce benefits.

Automation has huge potential for the cyber security industry. According to global research group Research for Markets, the worldwide security, orchestration, automation and response market will be worth almost US$19 billion by 2025.[2]

By taking on tasks that previously required human intervention, automation can reduce the workload, increase efficiency, improve consistency, accelerate responses and help provide comprehensive decision support to security professionals.

As data volumes continue to increase, automation is becoming a must-have for any cyber security team. Whether monitoring intrusion detection systems, onboarding employees or third parties, responding to incidents or checking for compliance, automation reduces errors, giving you more assurance and freeing up cyber professionals.

Fulfilling automation's huge potential

▸ Addressing the challenge

Automation can have a significant and positive impact on the effectiveness of CISOs and their teams.

Overcoming the talent gap

In common with other professions, automation eases the workload for cyber security specialists in a number of ways, as Gary Harbison, CISO of Bayer, explains: "Automation is a big opportunity to reduce manual work. Rather than pulling data, your engineers are freed up to analyze the data. An incident should trigger automated data gathering, enabling engineers to assess data and size up the risk. With a greater focus on expertise and driving value, cyber jobs become more interesting, which can help attract more people into the profession."

Another useful application is chatboxes for security queries — especially helpful for third party security. Getting swift answers enhances the employee and user experience, and can help improve cyber security by spreading best practice. Onboarding new employees can also be streamlined, to automatically provide appropriate levels of access to systems and resources — once again freeing up resources.

Embedding cyber security into the organization

The relationship between cyber security professionals and developers can be fraught; the latter want to innovate and get new products out quickly, while the former aim to reduce vulnerabilities. HP's CISO, Joanna Burkey, feels that automation can align objectives and help cyber security teams adapt: "We must understand how they work and avoid being prescriptive. The development community is not typically unified, so automation helps us fit in, encouraging them to incorporate tools in a secure way."

Enhancing overall cyber security

Automation reduces human error and guides cyber professionals on sources of risk, acting as a radar to emerging threats. This should help to protect sensitive personal and private data and, when linked with Security Orchestration, Automation, and Response (SOAR) and a ticketing workflow, lead to faster responses to actual or potential incidents. Attackers are increasingly using automation, and cyber security teams need the same pace of data gathering and analysis to counter such threats.

> "I expect the role of SecOps to be almost entirely automated away. The cyber security team should design SecOps, and then manage outcomes and exceptions from SecOps — activity should be automated and repeatable."
>
> **Matt O'Keefe**
> Asia Pacific Region Cyber Security Leader and Partner
> KPMG Australia

[2] Security, Orchestration, Automation, & Response Market Research Report, Research for Markets (360iResearch), 2021.

When introducing automation across operational technology, safety becomes paramount. Maersk is a major global integrated shipping company that operates several ports around the world. CISO Andy Powell explains his approach: "We started cautiously with automation on one pier in one port and had to prove that we could 'fail safely' from a cyber attack. Once this was achieved, we were able to build a template for automation safety and expand across other operations."

Enhanced decision-making

Axiata is investing in automation to boost data analysis, ultimately hoping to automate much of its decision-making, as Group Chief Risk and Compliance Officer Abid Adam explains: "You can't be an innovative company if you don't innovate yourself. We must be automated and digitized and I'm challenging my team to work on data governance models and improve how we collect and analyze data and build analytical models."

Keeping regulators happy

Regulatory demands can be a major challenge with global companies facing different regimes from multiple countries and territories. Managing this privacy landscape calls for fast, efficient data gathering, and automation can play an increasing role in continuous controls monitoring.

Re-shaping the cyber team

▸ KPMG thinks

The rapid growth of automation comes from a low base, as CISOs everywhere figure out how best to exploit this nascent technology. Its potential is enormous and continues to grow. With demands on the security team increasing as it takes on a more strategic role in the organization, the ever expanding and complicating ecosystem, not to mention the evolving regulatory landscape — it is critical that the sector takes advantage of technology automation.

Use areas include: low-level activities, linking SOAR to workflows and ticketing; bots to take over traditional customer service tasks; and automated provisioning and de-provisioning of accesses to resources. In this way, automation can target three of the most labor-intensive areas of the classic cyber security function.

Automating security can help to shape the future of the entire cyber team, as it makes it easier to identify and report any gaps with consistent metrics, which in turn helps CISOs allocate investment.

In a complex regulatory compliance landscape, automation enables a 'test once, comply many' approach, with automated controls producing automated reporting, and rapid notifications for the regulator.

However, when integrating security into DevOps, especially in the cloud, there's currently no definitive guide, so cyber is a little behind the game. Cloud does provide the capability to embed controls in a consistent way, so CISOs and their teams must figure out exactly how to automate — and what tools are needed.

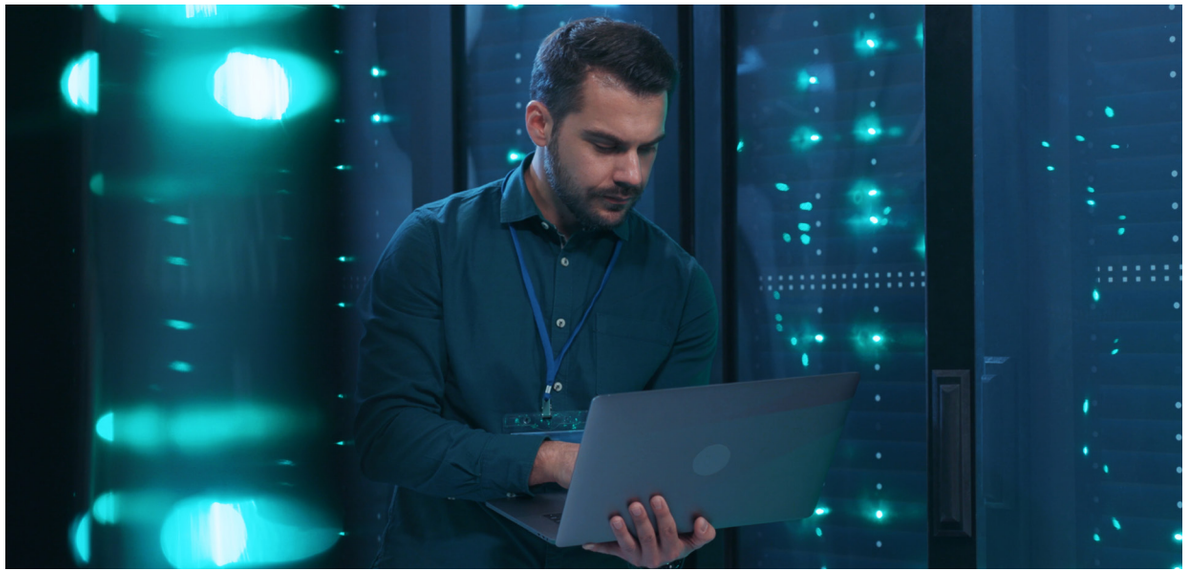
> "With automated controls, we are not doing the manual surveillance, so behaviors must now be the trigger — which means investing more in the analytics of behavior, both internally and amongst customers and suppliers, to avoid insider threats."
>
> **Sharon Barber**
> CISO, Lloyds Bank

It's important that automation does not add complexity — often, efforts fail because they're poorly planned and disjointed with multiple technologies that are not integrated. CISOs must leverage their seat at the C-suite table to partner with the CTO, so they can be part of a broader, organization-wide digital automation strategy, to make the most of shared capabilities.

Privacy has become a huge business and regulatory challenge for companies. In KPMG International's recent paper Privacy technology: What's next?, the authors argue that "… the art of privacy automation is very much a function of weaving together complementary technology for the various facets of data management, protection, and privacy to help streamline and drive efficiency and cost effectiveness in privacy program management."

One interesting development is data rights-as-a-service, which allows individuals to automate their subject access rights, reduce their digital footprint and remove personal data from search engines and other data aggregators, or mask their email identities online.

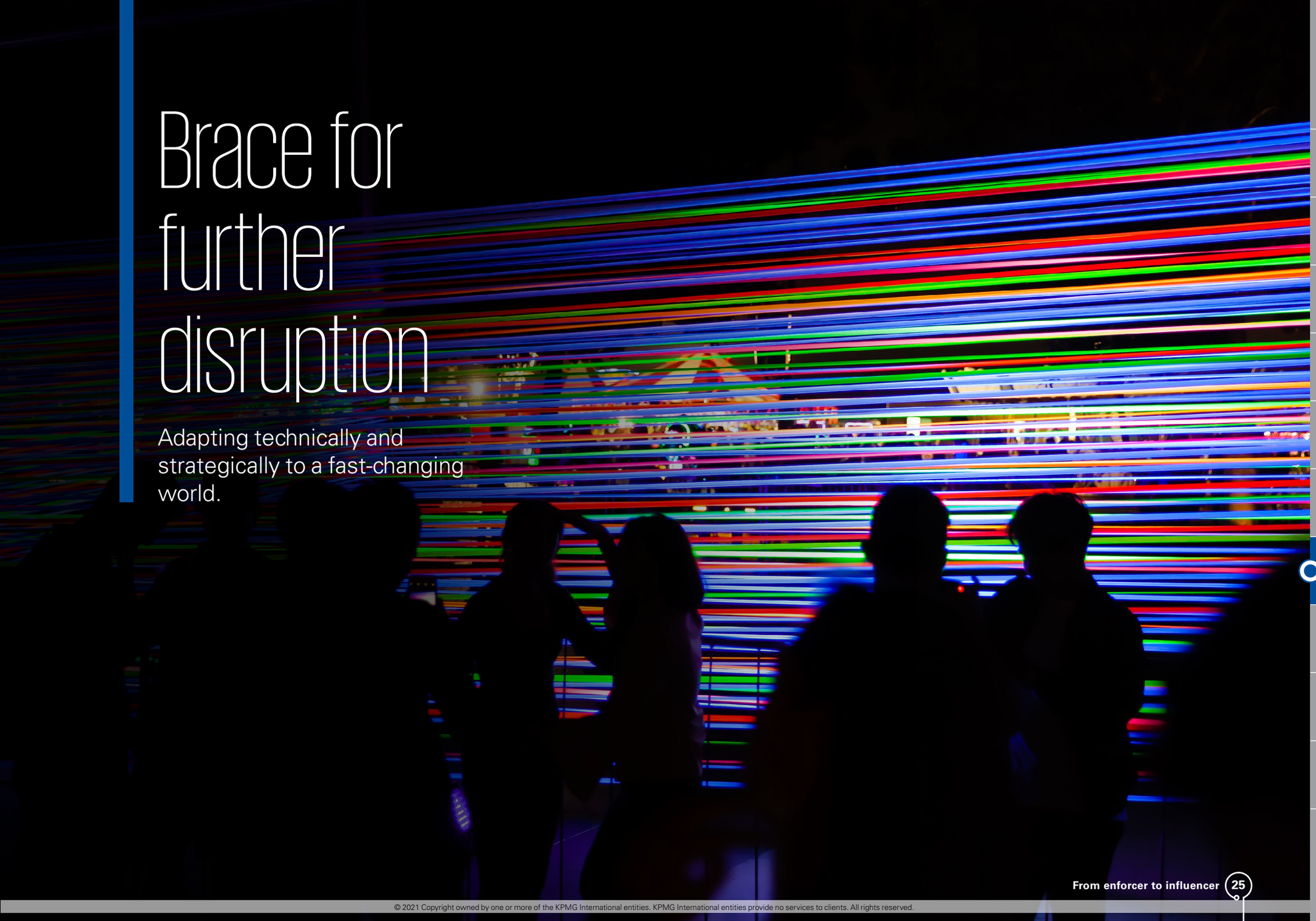
Automating security can help to shape the future of the entire cyber team. If the profession gets it right, many of the traditional process-focused roles associated with security today will disappear, with algorithms and machine learning taking over. It won't remove the needs for humans, who will be tasked with taking the more uncertain decisions and providing strategic advice and support.



> Compliance is a heavy drain on cyber security teams, especially in industries like financial services and the energy and utilities sectors. Instead of performing assessments against every requirement, they should simplify and automate so they test once and discern compliance with many. Think about automating the testing, continuously. With such automation, it can drive data enrichment and deeper correlation and analysis."
>
> **Leah Gregorio**
> Managing Director, Cyber Security
> KPMG in the US

Brace for further disruption

Adapting technically and strategically to a fast-changing world.



CISOs are also bracing themselves for further disruptors likely to have a (largely positive) impact on cyber security.

Artificial intelligence (AI) has broad possibilities: from building on basic robotic process automation (RPA), to sophisticated machine learning (ML) and analytics, covering increasingly large data sets, interacting ever more frequently with people and core corporate processes.

The new connected world has broken down traditional perimeters, with multiple parties accessing organizations' data and systems, from anywhere in the world. Add in 5G, edge computing and millions of IoT devices, and cyber security becomes incredibly complex using conventional security approaches. In this environment, the concept of zero trust or Secure Access Service Edge may provide a basis for future security models, founded as they are on the assumption that no-one inside or outside the network can be automatically trusted and must prove their identity and access rights before accessing key resources.

Challenges ahead

▸ Addressing the challenge

Securing AI

We're used to computers operating in predictable and deterministic ways, with security reviewing fixed algorithms and code. But the growth in machine learning (ML) is posing new questions: How has the ML algorithm been trained and what biases have been introduced? How can we supervise its behavior to ensure it's operating within parameters? How could it be manipulated by an adversarial AI technique and what would the consequences be? This is a new and immature field, requiring a blend of data science, security and ethics skills.

Addressing data nationalization

The democratization of data was meant to remove all boundaries. But as the monetized value of data rises, expect a return to nationalization, as GSK SVP and CISO Matthew McCormack explains: "We will start to see national fences popping up, with countries setting guardrails to protect citizens' privacy. This makes life harder for security professionals who have to meet newer and tougher regulations on use of data from multiple parts of the world, and may result in companies moving away from flat, global networks to rebuild national castles."

Embracing zero trust

Zero trust is about knowing where your data is and taking control of access to that data, with strong identity management, advanced analytics and a device inventory. Organizations can learn to better detect unusual behavior and prevent communication with unauthorized apps, servers and accounts.

This kind of thinking can lead, in the words of Darran Rolls, IAM market and technology specialist with over 25 years' experience as a CTO, CISO, to "Smarter clouds and dumber endpoints, with the endpoints merely offering browser sessions to (hopefully) smarter integrated cloud services." In such a world, notions such as bring your own device become outdated, as organizations seek greater visibility over network access.

Zero trust and SASE are not just for the security team — they should also apply to those building code and developing infrastructure.

> Organizations' capacity to defend themselves, both internally and externally, has become table stakes — although today it is still frequently talked about like an innovative differentiator. The winners will employ AI, advanced machine learning and cyber tools; not just reacting to threat actors, but proactively taking to cyber space to fight them.
>
> **Steve Bates**
> Global Leader
> CIO Center of Excellence
> KPMG in the US

> One mustn't forget that that zero trust is an idea not a technology. Too many companies view it as a finite project, but it's not. It's a mind shift, an ongoing philosophy with no beginning and no end.

Greg Day
VP and CISO, EMEA
Palo Alto Networks

Data is the future

▸ KPMG thinks

Securing data now matters more than securing end points, and companies must accept that many individuals and organizations access their data through a variety of channels. Zero trust and SASE help manage this complex mesh of rights, while major cloud providers increasingly establish secure collaboration environments to enable this new ecosystem, backed by federated identity and access management models.

Data handling policies will only become more complex as privacy regulation develops, and the rights of data subjects become clearer, while nations also assert their right to control their citizens' data within or beyond national boundaries. This places a premium on meta-data accuracy — and on control of access by applying increasingly sophisticated policy rules based on that meta-data.

These access rules will also interact with machine learning systems to control how they interpret base data. Which calls for sophisticated supervision of ML, as part of a wider extension of information governance within organizations, as the role of the CDO expands.

Strengthen the cyber security ecosystem

Collaboration should aid the fight against cyber threats.

CISOs are acutely aware of the complexity and threats resulting from the increase in third parties accessing their data, whether it's suppliers, outsourced providers, contractors or business partners.

Vetting hundreds and possibly thousands of businesses and agreeing and monitoring strict contracts is great in theory but can be very difficult in practice. While there are plenty of ideas, the cyber security profession lacks a comprehensive solution to this conundrum, with all CISOs working to find ways to verify the reliability and continuing security of third parties.

Towards greater trust

▸ Addressing the challenge

As they face the challenges of securing data across multiple parties, CISOs have a number of options.

Tightening up the supply chain

Contracts and compliance are an obvious place to start, with clear guidelines on due diligence before signing a contract, and more controlled and restricted access for third parties, if there's a concern they can't meet the required cyber security standards.

Automation also has a role to play, building machine learning and establishing automated risk assessments, which is a good way to manage the scale of the problem, with many companies already facing a backlog of a thousand or more vendor assessments.

> "As we become more virtual and digital, a CISO's role moves away from being enterprise-centric, to recognizing that this is a collective effort. They're not the only one facing this challenge, so they need to look externally to help the community become stronger, as well as reporting any violations or attempted threats to regulatory bodies."
>
> **Prasad Jayaraman**
> Americas Region Cyber Security Leader and Principal
> KPMG in the US

> "Until you build a solid platform consisting of operations, SecOps and security by design, purely to give a strong secure foundation, you can't build outward to handle third party stuff. Don't run before you can walk or a basic vulnerability will take you out."
>
> **Andy Powell**
> CISO, Maersk

Intra-industry collaboration

There's a broad acknowledgement that CISOs cannot solve this problem alone, a point emphasized by Greg Day, VP and CISO, EMEA, Palo Alto Networks: "We need to build industry communities to allow data sharing, coordinating at an international level, with more sharing of key cyber threats, rather than just trend analysis."

Working with a range of stakeholders

▸ KPMG thinks

There's no quick fix to the threats inherent in the complex web of relationships that characterize today's supply chains and outsourcing environment.

Industries like financial services have shown the value of collaboration across a number of common challenges. Working together to share intelligence and knowledge, to learn from others and present a united front, benefits all the players. Philipp Südmeyer, Group CISO, Munich Re, says "A lot is about personal relationships; when you know and trust people, you can talk about x, y and z and build deeper relationships." This extends to relationships with regulators, to work as a team to proactively manage cyber security issues and defend communities.

In the UK, for instance, the Active Cyber Defence (ACD) program's stated aim is to 'Protect the majority of people in the UK from the majority of harm caused by the majority of cyber attacks the majority of the time' — a concept that could be applied to broader ecosystems to defend against an increasingly aggressive and sophisticated threat landscape.

A new era of cooperation

Conventional third party security offers the illusion of confidence. Embedding security into contracts offers limited assurance, while point-in-time assessments don't give a real-time view of third party risks — and can become unmanageable as organizations begin to consider fourth, fifth and even sixth party providers.

In addition to addressing in-house concerns, CISOs must turn their attention to playing their part in securing the wider ecosystem through collaborative action.

Coming soon

In early 2022, KPMG will be presenting a new piece of thought leadership on the third party cyber security threat and the need for collaboration to protect the cyber security ecosystem — look out for this on kpmg.com, LinkedIn and Twitter.

> "Collective threat intelligence helps satisfy regulatory challenges and makes the community stronger."
>
> **Prasad Jayaraman**
> Americas Region Cyber Security Leader and Principal
> KPMG in the US

Next steps

As CISOs address the evolving cyber threat landscape, they must balance many responsibilities, formally and informally. This means shifting from enforcer to influencer, fostering security awareness and building vital relationships with peers. Indeed, learning how to deal in 'gray' rather than black and white may be one of the key learnings, shifting from a world of absolutes to one where outcomes are less certain, and risk avoidance and containment is the prime objective.

In approaching the seven actions outlined in this paper, CISOs should consider the following steps:

1. Speak the language of the board by thinking in terms of customers, revenue, costs and return on investment.
2. Focus on operational resilience: keeping the lights on and getting back to normal quickly following a crisis.
3. Invest time in building a network within your organization, visiting different functions, learning how they operate and gaining trust that you want to enable — safely — and not just say 'no'.
4. Think about shaping a workforce to the cyber needs of the business — as opposed to permanent roles and structures. Consider the ratio of employees to contractors and gig workers.
5. Build a business case for automation, reflecting the efficiencies it brings and the value added from workers who are freed up for higher-level tasks.
6. Work out what zero trust means for your business and see this as an ongoing philosophy rather than a one-off program.
7. Find ways to reach out to peers in your sector, either joining existing industry bodies or forming less-formal groups.

> The CISO is becoming more of a businessperson, thinking of the actual risk to the business if a product doesn't go out on schedule, balancing business risk with security risk.

Walter Risi
Global IoT Cyber Security Leader and Partner
KPMG in Argentina

How can KPMG help?

KPMG firms can help you create a resilient and trusted digital world — even in the face of evolving threats. KPMG cyber security professionals can offer a multidisciplinary view of risk. Helping you carry security throughout your organization, 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 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 can help you develop advanced solutions, assist with implementing them, advise on monitoring ongoing risks and help you respond effectively to cyber incidents.

KPMG firms bring an uncommon combination of technological expertise, deep business knowledge and creative professionals who are passionate about enabling you to protect and build your business. We'll help you create a trusted digital world, so you can push the limits of what's possible.

Acknowledgements

Our sincere thanks to the cyber security leaders around the world who generously contributed their time and insights to the report.

Abid Adam
Group Chief Risk and Compliance Officer, Axiata

Sharon Barber
CISO, Lloyds Banking Group

Joanna Burkey
CISO, HP

Leon Chang
CRO, IHiS

Greg Day
CSO, Palo Alto Networks

Karel De Kneef
CSO, SWIFT

Gary Harbison
CISO, Bayer

Darren Kane
CISO, NBN Co, Australia

Tammy Klotz
CISO, Covanta

Matthew McCormack
CISO, GSK

Jim Nelms
CISO, LabCorp

Brian O'Durnin
CISO, YPF

Michael Papay
CISO, AMEX

Andy Powell
CISO, Maersk

Darran Rolls
IAM Market and Technology Specialist 25+ years experience as a CTO, CISO

Emma Smith
Global Cyber Security Director, Vodafone

Philipp Südmeyer
Group CISO, Munich RE

We would also like to thank KPMG firms' cyber security specialists, authors and project managers, who generously contributed their support, knowledge and insights into the planning, analysis, writing and production of the report.

Leandro Antonio
KPMG in Brazil

Steve Bates
KPMG in the US

Jonathon Dambrot
KPMG in the US

David Ferbrache
KPMG International

Rommel Garcia
KPMG in Mexico

Leah Gregorio
KPMG in the US

Lisa Heneghan
KPMG in the UK

Prasad Jayaraman
KPMG in the US

Billy Lawrence
KPMG International

Dani Michaux
KPMG in Ireland

Hartaj Nijjar
KPMG in Canada

Matt O'Keefe
KPMG Australia

Daryl Pereira
KPMG in Singapore

Guillaume Rablat
KPMG in France

Fred Rica
KPMG in the US

Walter Risi
KPMG in Argentina

Kathy Robins
KPMG Australia

Martin Tyley
KPMG in the UK

Tim Wood
KPMG in the Middle East Region

Contacts

Akhilesh Tuteja
Global Cyber Security Leader, KPMG International and Partner
KPMG in India
E: atuteja@kpmg.com

Walter Risi
KPMG in Argentina
E: wrisi@kpmg.com.ar

Gordon Archibald
KPMG Australia
E: garchibald@kpmg.com.au

Leandro Augusto M Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Hartaj Nijjar
KPMG in Canada
E: hnijjar@kpmg.ca

Henry Shek
KPMG China
E: henry.shek@kpmg.com

Mika Iivari
KPMG in Finland
E: mika.iivari@kpmg.fi

Vincent Maret
KPMG in France
E: vmaret@kpmg.fr

Wilhelm Dolle
KPMG in Germany
E: wdolle@kpmg.com

Atul Gupta
KPMG in India
E: atulgupta@kpmg.com

Dani Michaux
KPMG in Ireland
E: dani.michaux@kpmg.ie

Luca Boselli
KPMG in Italy
E: lboselli@kpmg.it

Atsushi Taguchi
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

Min Soo Kim
KPMG in Korea
E: mkim9@kr.kpmg.com

Rommel Garcia
KPMG in Mexico
E: rommelgarcia@kpmg.com.mx

Timothy Wood
KPMG in the Middle East Region
E: timothywood@kpmg.com

Koos Walters
KPMG in the Netherlands
E: wolters.koos@kpmg.nl

Daryl Pereira
KPMG in Singapore
E: darylpereira@kpmg.com.sg

Marc Martinez Marce
KPMG in Spain
E: marcmartinez@kpmg.es

Matthias Bossardt
KPMG in Switzerland
E: mbossardt@kpmg.com

Siraporn Chulasatpakdy
KPMG in Thailand
E: siraporn@kpmg.co.th

Pepijn Kok
KPMG in Thailand
E: pepijn@kpmg.co.th

Martin Tyley
KPMG in the UK
E: martin.tyley@kpmg.co.uk

Kyle Kappel
KPMG in the US
E: kylekappel@kpmg.com

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

home.kpmg/socialmedia

Designed by Evalueserve.

Publication name: From enforcer to influencer | Publication number: 137595-G | Publication date: July 2021