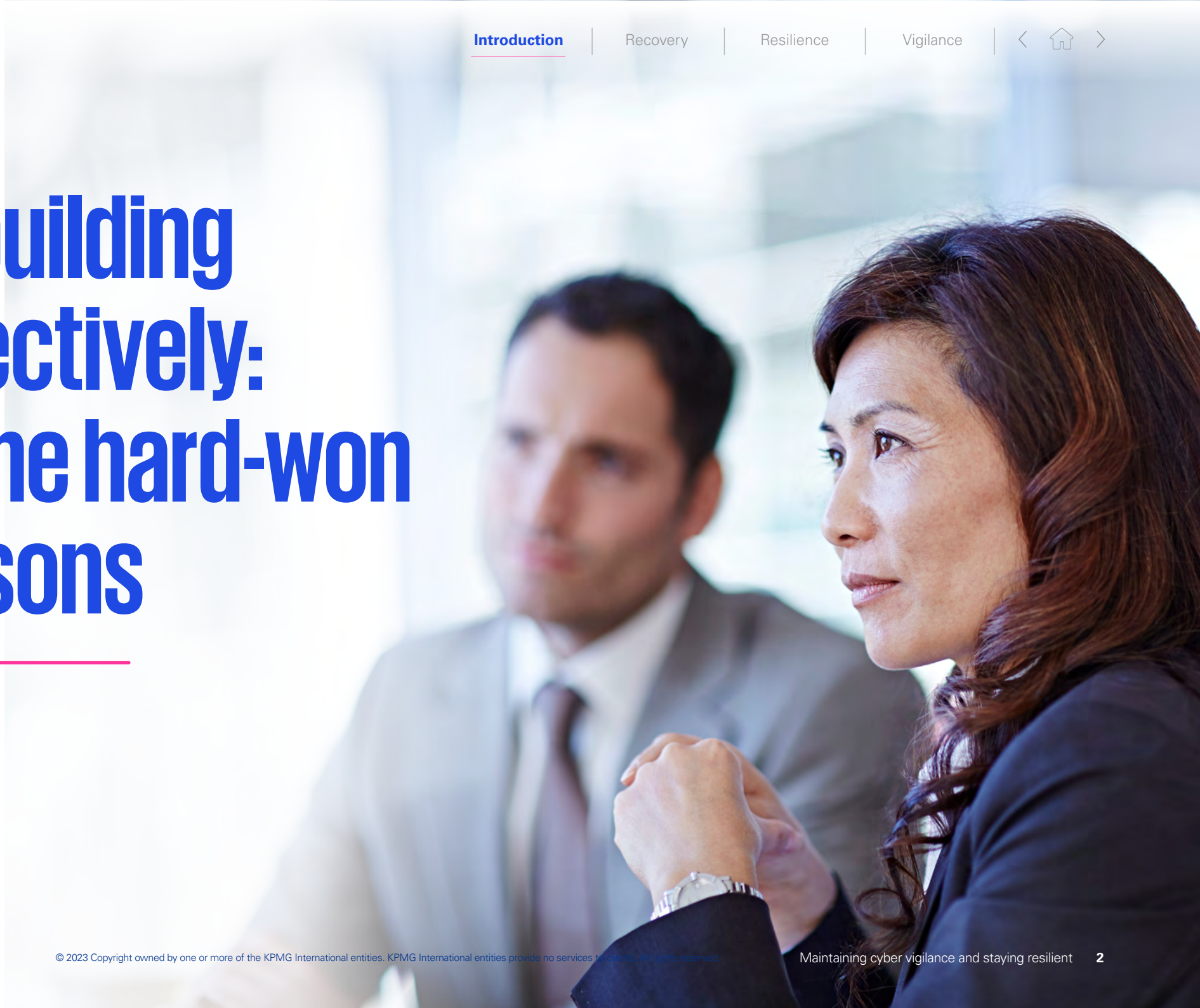
KPMG

Maintaining cyber vigilance and staying resilient

How to recover from a cyberattack, rebuild effectively and avoid complacency.

KPMG International | kpmg.com/cybersecurity

Rebuilding effectively: Some hard-won lessons



The rules of engagement in cybersecurity are constantly shifting. Yesterday's defenses are little match for hybrid, evolving criminal gangs profiting from lucrative cyberattacks and nation-states investing millions in cyber capabilities.

Both seek to exploit new attack routes using new technologies, while still using old reliable solutions. New criminals are also leveraging artificial intelligence (AI) to their advantage. According to the KPMG 2023 CEO Outlook, 82 percent of CEOs agreed that generative AI (genAI) is a double-edge sword that will help detect cyberattacks but also provide new attack strategies for cyber criminals.[1]

While prevention remains a high priority, leaders acknowledge that cyberattacks will succeed despite the best defenses, resulting in the theft of intellectual property and sensitive data, leading to extortion and fraud. In the same study, 74 percent of CEOs identified cybercrime and cyber insecurity as factors that will impact prosperity.[2] Rapid detection, response and recovery matter more than ever to help minimize damage and rebuild effectively to increase resilience.

Complacency is one of the biggest enemies of resilience: once the white heat of a cyber incident has cooled and business as usual returns, it's perhaps understandable that attention moves on to more pressing business and operational matters — and old, lax habits return. In that moment, don't be surprised if events repeat themselves. And don't be surprised if customers and shareholders show less sympathy for the same errors the second time around.

Cyber resilience is vital to maintain business operational capabilities, safeguard customer trust, and reduce the impact of future attacks. According to the KPMG Global Tech report 2023, 71 percent of businesses say they have to become more proactive at integrating trust, security, privacy and resilience into technology rollouts.[3] Across the world, regulators are increasingly focused on cyber resilience, whether it be the EU Digital Operational Resilience Act (DORA) and updated Network and Information System Directive or the recent US Securities and Exchanges Commission (SEC) cyber regulations.

Organizations are obliged to be more transparent about their ability to respond to breaches before, during and after an incident. In some critical sectors — such as financial services — regulators demand service restoration within specific time periods, while others require a focus on protecting customers and clients from the harm that results. In July 2023, the SEC issued a final rule requiring companies to provide enhanced disclosures about cybersecurity risk management, strategy, governance and incidents.[4]

The post-breach objective is not just about getting the organization back on its feet; it's about making it stronger than before, less vulnerable to future attacks, more secure and more resilient.

In this eBook, we share hard-won lessons to help organizations confidently and proactively address cyber threats, recover from cyber incidents — and come back stronger.

Security is being acknowledged as an opportunity

74% of CEOs identified cybercrime and cyber insecurity as factors that will impact prosperity.

71% of businesses say they have to become more proactive at integrating trust, security, privacy and resilience into technology rollouts.

82% of CEOs agreed that genAI is a double-edge sword that will help detect cyberattacks but also provide new attack strategies for cyber criminals.

[1] KPMG 2023 CEO Outlook, KPMG International, 2023.
[2] Ibid.
[3] KPMG Global Tech report 2023, KPMG International, 2023.
[4] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216; 34-97989; File No. S7-09-22, (September 5, 2023).

Key steps to help you recover from a cyberattack, rebuild effectively and avoid complacency.

Click on each step to learn more.

In the heat of the moment:

Recovery

01 **Define your criticality** — it's all about the business

02 **Focus on what matters** — that may surprise you

03 **Be clear on who is doing what** — and help them succeed

04 **Communicate** — with timeliness, clarity and consistency — to all who need to know

05 **Pause for reflection** — even in the worst moments

06 **Be adaptable** — and realize the playbook may be wrong

07 **Know when the crisis is over** — and move on quickly but carefully

When the worst has passed:

Resilience

01 **Be honest about what has happened** — and learn from it

02 **Build resilience** — and keep improving

03 **Clean up** — data and applications

04 **It's organization-wide** — not just one team's role

05 **Understand your supply chain** — and its role in your resilience

06 **Use retainers** — to quickly access the skills you need

07 **The world changes** — don't assume today's challenges are tomorrow's

But most of all:

Stay vigilant.

In the heat of the moment: Recovery

01 Define your criticality — it's all about the business

There's a risk that senior executives underestimate the extent of the impact of a breach, treating it as primarily a technical matter. Early conversations with the executive team can help convey the gravity of the situation, explain what could happen in the coming days, and present a realistic picture of likely timescales and uncertainties. External advisers can add essential insights from their own experiences. Once the CEO and CFO recognize that fundamental elements of their operations are under threat (e.g. they may not be able to pay employees or suppliers nor engage with customers), they are likely to take a more involved leadership role — while also accepting the reality of what lies ahead.

02 Focus on what matters — that may surprise you

In the heightened atmosphere following a breach, it's natural to want to fix everything fast; however, counter-intuitively, that impulse should be resisted. Instead, leaders should establish which business processes and systems are most critical to recovery and give these 'crown jewels' the highest and most immediate priority.

For instance, in a resource-heavy sector, such as construction, the ability to pay contract workers is paramount to ensure they continue to turn up on site. On the other hand, doctors and health workers in a hospital require patient data and functioning equipment. A global manufacturer should focus on those facilities that generate the most revenue and maintain liquidity. In other sectors, safety issues may be the overriding concern. These varied business choices sit alongside the realities of rebuilding technical infrastructure.

> **"One company that suffered a breach had no employee records, so couldn't pay their staff — which would have jeopardized their entire business. Once they recognized this, they focused on recovering and restoring payroll details from back-ups."**

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG International and Principal
KPMG in the US

03 Be clear on who is doing what — and help them succeed

In a difficult and highly stressful environment, some senior executives may struggle to relinquish responsibilities and feel they should steer the ship. CEOs are accustomed to calling the shots, but in these instances, they should give the CISO and CIO the space they need to fix the issues.

The CEO's role is to 'own' the overall recovery strategy and ensure it focuses on business needs. As the public face of the organization, CEOs are also pivotal to stakeholder communications, to give customers, regulators, shareholders and citizens confidence in the viability of the business.

Supporting the CEO should typically be the COO — accountable for technical recovery (including managing IT vendors), while other business leaders assume responsibility for understanding and mitigating the business impact.

During an incident, you're going to be pushing key individuals very hard, with long working hours commonplace, and many will risk burnout. It's, therefore, essential to have deputies in place and a plan to rotate people in and out to enable them to rest and return refreshed. This includes having third parties and vendor support on retainer-based contracts with defined service level agreements (SLAs) that mirror the recovery priorities outlined above.

> **"Make sure you understand how the various teams interact. Clarify the touchpoints between the incident response team, crisis team, continuity team, disaster recovery team and communications team. Build these into plans and frameworks so everyone is clear on their remit, and exercises these capabilities."**

Campbell Logie-Smith
Director, Business Resilience Services Leader
KPMG Australia

04 Communicate — with timeliness, clarity and consistency — to all who need to know

Firstly, decide whether or not you need to disclose the incident and if so, how much information you're prepared to share. You may be legally compelled to do so.

If external stakeholders are affected in any way, then at the very least, explain that services may be temporarily affected, consulting with external counsel to address legal obligations. Internally, ensure strong and regular collaboration and information sharing between the crisis team (consisting of senior executives, Human Resources, Communications and Legal) and the technology team who are conducting the hands-on investigation and performing breach response activity.

Be aware of any regulatory or contractual requirements to report breaches: these will vary in degree, but typically, they give an organization a maximum time period to disclose what happened and the impact on critical operations. Timely, measured discussions with regulators should disclose what they need to know and when they need to know it. Avoid telling them too much, too early or too little too late.

"In my experience, it's wise to tell the world you have a plan for good communication — communicating in a balanced way is important; otherwise, no one knows what's going on, and they may draw their own conclusions. If you let others define the narrative, then you're not in control of the situation."

Dani Michaux
EMA Cyber Security Leader and Partner
KPMG in Ireland

05 Pause for reflection — even in the worst moments

It may seem as if your world will collapse if you don't act immediately, but you're likely to make better decisions by taking a few deep breaths and waiting until the situation becomes clearer. Discovering the 'state of the nation' is key in the battle for recovery, which requires time to gather and process insights. Create strategic space and avoid getting sucked into the detail. In a highly stressed environment, the leadership needs to be 'comfortable being uncomfortable' and be prepared to live with the inevitable uncertainties accompanying a major cyber incident.

Avoid making assumptions that are not evidence-based. By asking technicians and other specialists to investigate — possibly for up to 24 hours — the leadership should gain a clearer picture of the breach and its impact.

For instance, if you just shut the system down, you won't necessarily find out the attacker's intent — or indeed trace where else they've moved in the environment. This is especially important in cyber espionage, where the adversary tends to be sophisticated with a longer-term strategy. In a 'smash and grab' ransomware breach, on the other hand, the attacker uses aggressive tactics to achieve maximum extortion.

Subtle nuances can determine when to isolate, contain and eradicate an attacker from your systems and when to monitor and better understand their activities. It's wise to seek expert advice and draw on threat intelligence, which in some cases may even involve engaging with the criminal group to understand their intentions. There is no perfect answer and judgments may differ quite radically across sectors. In a critical sector like healthcare, for example, closing services has far greater consequences beyond data security.

"When you're dealing with a threat actor, you should follow the trail, find out where they are, what they changed, what they stole and sweep the environment, making sure they haven't deployed additional back doors that would allow them back in."

Matt Dri
Partner, Cyber Response and Forensic Technology
KPMG Australia

06 Be adaptable — and realize the playbook may be wrong

Testing and drills are useful training, building muscle memory and confidence. But nothing can fully prepare you for a cyberattack. Be open to changing direction as events dictate — possibly deviating significantly from the playbook.

Accept there will be conflicting priorities — so be ready to deal with uncertainty. Often, impacted organizations busy 'firefighting' a cyber crisis fail to see 'the forest for the trees.' External experts with experience responding to cyber incidents and rebuilding impacted environments can identify the pros and cons of different paths to recovery and advise on feasibility, complexity and timescales.

Understand what 'minimum viable processes' look like and keep track of them — and the adaptations you have made — to give yourself a greater chance of restoring the business.

07 Know when the crisis is over — and move on quickly but carefully

Establish metrics and reporting to monitor the restoration of business and use these to track how quickly you return to normal, including system and service availability, customer queries and complaints, and, of course, media attention. Reliable, easy-to-read data helps you update senior executives on progress by providing 'one version of the truth.'

As you move out of crisis, the forensics should have been largely completed and the risk mitigated. But be prepared to continue ongoing 'hypercare' activities for a period to try to avoid a second assault through any additional attack vectors that may not have been detected in the initial onslaught.

Try and move on quickly but carefully from the response to be confident you have cleared all exploits and made it hard for attackers to return. The focus now shifts to recovery and rebuilding more effectively to become more secure, resilient and robust.

When the worst has passed: Resilience

01 Be honest about what has happened — and learn from it

A comprehensive post-incident review (PIR) should determine how the attack happened and the root cause (e.g. a lack of multifactor authentication or poor phishing awareness). It should also honestly appraise how the organization dealt with the incident and how it could do better in the future. The PIR is not about blame; it is about reflection and improvement.

A well-conducted PIR is independent, challenging and looks at the business aspects and technical security lessons. Expect to find issues around risk management, crisis management, supplier engagement, communications, skills, culture and awareness and, of course, cybersecurity. No organization can handle a major crisis perfectly, and all can improve.

02 Build resilience — and keep improving

In attempting to become more resilient, organizations can embark upon large-scale programs that, given legacy infrastructure, could take many years — during which time they may suffer another breach.

Of course, these improvements are necessary, but ask yourself what swift actions can be taken within weeks to build resilience. The question: "How could the organization respond better if attacked again next month?" will likely yield some 'quick wins.'

For example, are there ways to pay suppliers and staff more quickly in a crisis? Can we maintain liquidity? Could we improve our ability to communicate? And could we mobilize our response faster next time around?

03 Clean up — data and applications

A major cyber incident can have one surprising — and positive — outcome. It can focus attention on whether organizations genuinely need specific applications and legacy systems. In many cases, the answer may be "no," leading to a clean-up of the IT estate.

Your organization may also hold a lot of data you don't necessarily need, presenting an opportunity for a culling exercise. File servers, which may have been around for decades, contain significant amounts of unstructured data, posing relatively easy pickings for threat actors who've managed to breach the defenses. By only storing what you need, you reduce the threat significantly.

04 It's organization-wide — not just one team's role

Digitalization has blurred the lines between operational functions and between safety, protection, cybersecurity and ethics disciplines. Barriers between enterprise IT, operational technology and product security have begun to break down. Now that everything is connected, organizations should take a holistic view of resilience rather than concentrating on just one dimension.

Something as simple as an unprotected laptop can be the vector for all sorts of attacks ranging from data theft to fraud to hacking manufacturing systems to manipulating key control systems. Cyber resilience demands an organization-wide approach to drive the right behaviors across very different business unit cultures and focus on what really matters to the organization, be that data, services or infrastructure.

> **"In a cyber breach today, more likely than not, you'd have user IDs compromised in locations that are not considered part of your core business function or core office locations. In many cases, these can also belong to other trusted organizations or suppliers within your broader supply chain. But through this apparently innocuous entry, the attacker could potentially gain access far deeper into your organization — possibly leading to the shutdown of facilities, prolonged information leakage, even the ability to cause environmental damage and more."**

Dani Michaux
EMA Cyber Security Leader and Partner
KPMG in Ireland

05 Understand your supply chain — and its role in your resilience

The complexities of modern supply chains and the growth of everything-as-a-service (XaaS) have left organizations reliant on an increasingly large number of third parties. It's critical to understand the capabilities of these parties in managing cyber breaches — and just where liability might lie. One challenge is that service-based contracts, with thin profit margins, leave suppliers with fewer resources to build cybersecurity skills.

Be clear on the responsibilities and liabilities of your suppliers when it comes to a cyber breach. Where you can, embed this into contracts, although suppliers will understandably, wish to limit their potential liability. Given the high potential financial consequences of a cyber incident, specialist legal support may be necessary to understand contractual obligations for all parties and clarify any regulatory requirements.

Expect regulators to be unforgiving of organizations that cite the failure of a supplier as a reason for not meeting service or client obligations. They will demand higher levels of due diligence in the future.

"There's a significant push towards understanding your supply chain more effectively and having governance in place to manage it. You need to know whether the organizations you deal with, especially your critical IT providers, can deal with a cyber breach and whether they will notify you should such an incident happen."

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG International and Principal
KPMG in the US

06 Use retainers — to quickly access the skills you need

Cybersecurity is a highly specialized discipline and incident response skills are scarce — and often come at a premium in an emergency. When a breach occurs, having a capable and experienced team on hand can make a huge difference to the speed and effectiveness of any response. By placing response and recovery experts on retainer, you can ensure rapid mobilization in the event of an incident and build a trusted relationship in advance, where your chosen experts can help train and exercise your response capabilities.

07 The world changes — don't assume today's challenges are tomorrow's

A plan based on historic cyber-breach patterns may not be suitable as attacker tactics change and evolve. Five years ago, DDoS (distributed denial-of-service), 'smash and grab' attacks, and ransomware cryptoworms (such as WannaCry) were common, as the IT estate was the main target. Today's attacks have shifted to supply chain compromises and double or treble extortion, all backed by a sophisticated 'crime-as-a-service' ecosystem. Attacks have become 'cloud savvy' and increasingly sophisticated in targeting and destroying online backups while showing a growing interest in operational technology and industrial control systems.

Keep your plans and playbooks under review and make sure they reflect not just the fluctuating threat landscape but also the changes in your organization and its dependency on IT.

"Threat actors continually change techniques, so plans should be flexible and evolve, or you may find your team is unable to respond effectively."

Matt Dri
Partner, Cyber Response and Forensic Technology
KPMG Australia

But most of all: Stay vigilant

Establishing resilience means that if, in the future, you have a repeat of a past incident, you'll be better equipped to deal with it and hopefully reduce the potential impact. You can't control the external environment threat but can control your ability to respond and recover. In the aftermath of a breach or near miss, do not miss the opportunity to improve resilience.

Organizations naturally tend to become complacent over time or allow 'drift' in the technical ecosystem as memories of past events recede, potentially leading to reduced cyber budgets and a general relaxation of attitudes. The CISO (or increasingly the Chief Resilience Officer) has the difficult role of reminding boards and senior executives of what has happened, what is happening to others and what might happen in the future.

From a people perspective, a cyber-resilient culture involves education and preparatory drills so that everyone is aware of the threat and is ready to respond if necessary. This is harder than it may seem, as the severity of a major cyberattack can never be fully replicated in an exercise. However, it still helps to build understanding and 'muscle memory.'

Those leading any response should be prepared to deal with conflicting priorities and major uncertainties — demanding a focus on what is truly critical to the organization and an ability to make tough choices to protect these critical areas.

"There's an ongoing race between you and the bad actors, and they're constantly evolving and innovating faster than we can. By having the right conversations in advance and preparing thoroughly, you're much more likely to have that muscle memory to call upon when you need it."

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG International and Principal
KPMG in the US

How this connects with what we do

Organizations, even with the best cybersecurity controls in place, are at risk of disruptive cyberattacks. The KPMG Cyber Resilience Framework is designed to help organizations protect, detect and recover from a major cyber incident.

The framework covers the most significant standards and regulations and is supplemented by KPMG firms experience to develop leading technology solutions. Each phase of the KPMG Cyber Resilience Framework embeds Recovery, Resistance and Resilience and ensures that all employees have a role in making sure the organization remains secure.

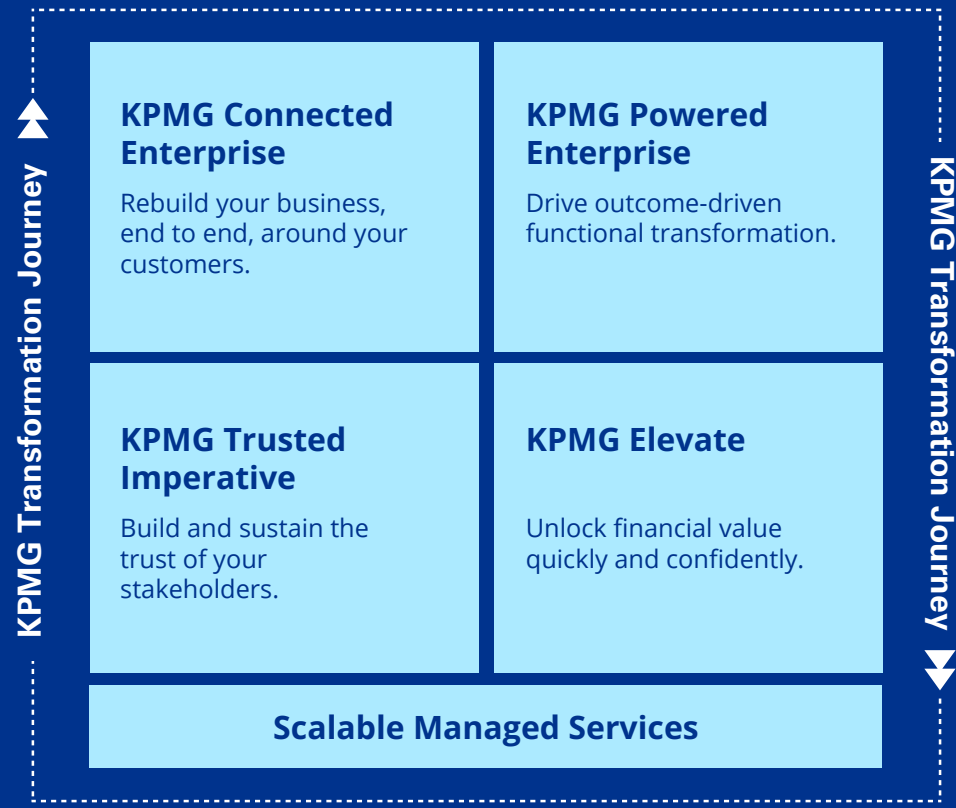
The framework benefits organizations by enhancing their resilience through exercising, testing and simulations. It also, helps minimize the impact of a cyberattack on critical business services and enables recovery and continuity of critical operations. Additionally, it empowers them to use intelligence to adapt quickly to sophisticated cyber threats.

KPMG professionals can help you avoid costly business disruption and remain future-ready by embedding cyber resilience across your organization.

Learn more at: kpmg.com/cybersecurity

In addition, KPMG firms are helping global businesses in every sector embrace a new era of opportunity in the digital economy. From strategy to implementation, KPMG professionals can make all the difference on your transformation journey. Together, we can help transform your current business model to drive future competitiveness, growth and value. KPMG. Make the Difference.

KPMG's Digital Transformation Suite



Meet the author

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG International and Principal
KPMG in the US
jhawardgrau@kpmg.com

Jason is an experienced cybersecurity leader who has been guiding some of the world's most influential organizations through information security transformations. With two decades of experience in industry and IT, cybersecurity and shared services consulting, he has developed a reputation for cultivating world-class teams and maintaining transparency through constant performance measurement.

Over the past five years, Jason has focused on cybersecurity in the industrial or operational technology space, leveraging his expertise to deliver effective cybersecurity strategies in complex manufacturing, refining and energy markets. He is also an experienced Chief Information Security Officer who has successfully implemented risk, compliance, cyber and IT programs across organizations.

Acknowledgements

This report would not be possible without the invaluable contributions of colleagues around the world.

Matt Dri
Partner, Cyber Response and Forensic Technology
KPMG Australia
mattdri@kpmg.com.au

Campbell Logie-Smith
Director, Business Resilience Services Leader
KPMG Australia
clogiesmith@kpmg.com.au

Alexander Rau
Partner, Cyber Security Services
KPMG in Canada
alexanderrau@kpmg.ca

Dani Michaux
EMA Cyber Security Leader and Partner
KPMG in Ireland
dani.michaux@kpmg.ie

Ali Abedi
Senior Manager, Cyber Security Services
KPMG International
ali.abedi@kpmg.co.uk

Contacts

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG International and Principal
KPMG in the US
jhawardgrau@kpmg.com

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

Dani Michaux
EMA Cyber Security Leader and Partner
KPMG in Ireland
dani.michaux@kpmg.ie

Prasad Jayaraman
Americas Cyber Security Leader and Principal
KPMG in the US
prasadjayaraman@kpmg.com

Matt O'Keefe
ASPAC Cyber Security Leader and Partner
KPMG Australia
mokeefe@kpmg.com.au

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

kpmg.com/cybersecurity

Designed by Evalueserve.
Publication name: Maintaining cyber vigilance and staying resilient
Publication number: 139036-G
Publication date: October 2023