FT LONGITUDE

CMS
law·tax·future

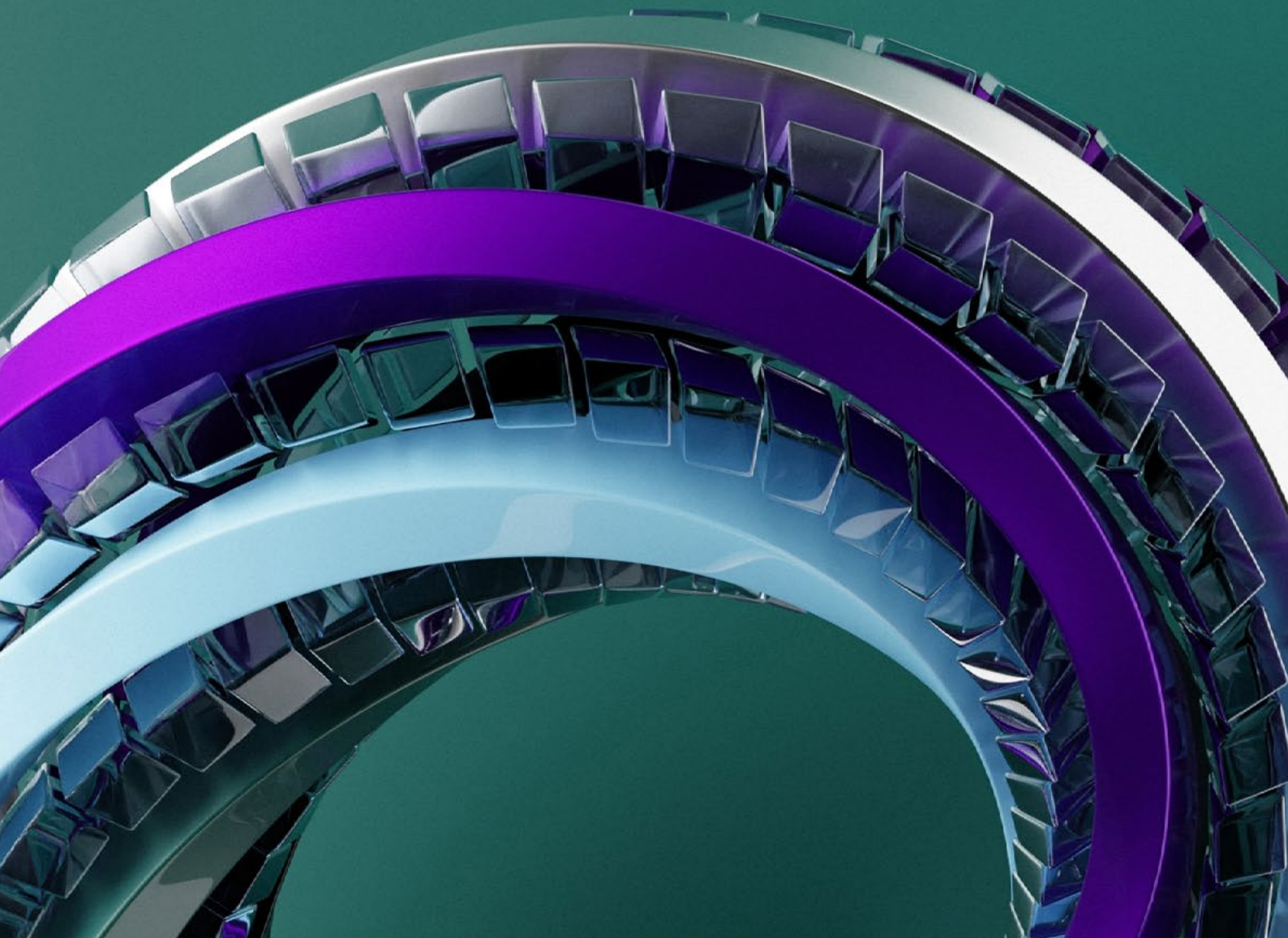
The Cyber Continuum

Ready, resilient, recovered

May 2026

DATA DRIVEN DISPUTES

Contents



Executive summary

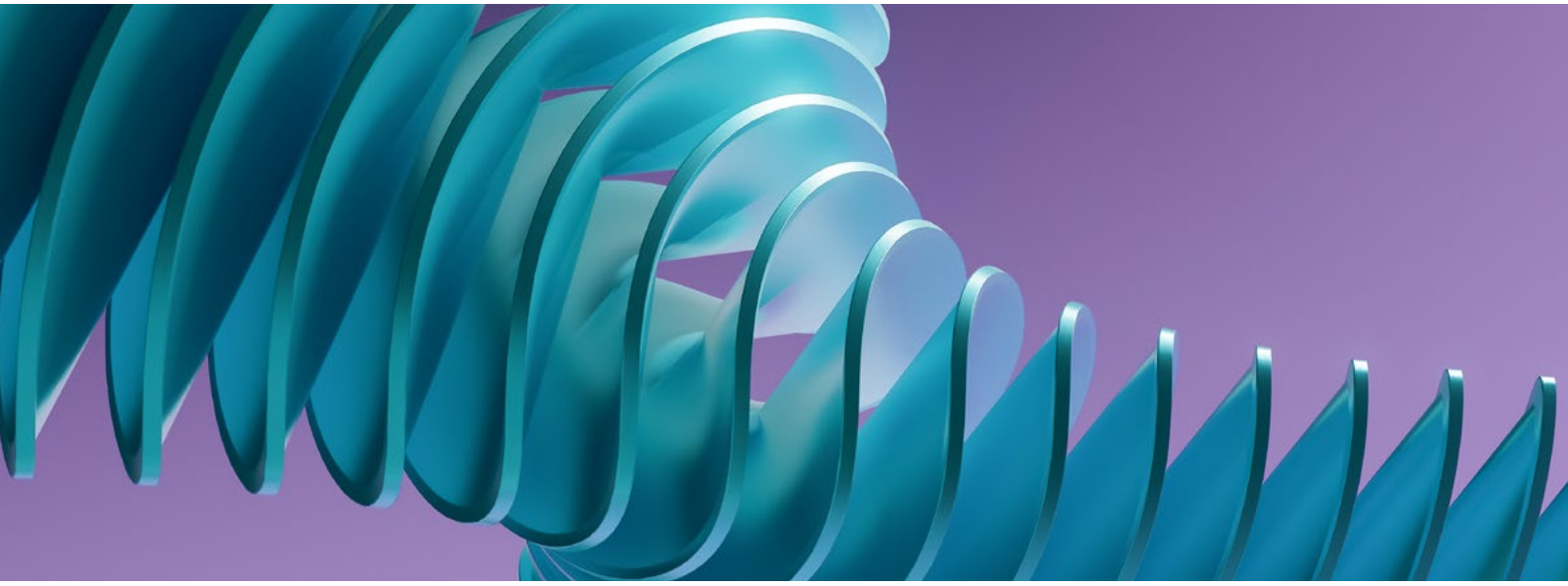
Are you confident or is it complacency?

The first crewed Apollo mission was scheduled for February 1967. After years of preparation and rapid technical development, NASA was confident it was ready. But during a preflight test just weeks before the intended launch, **a devastating fire** broke out in the crew cabin, halting all missions.

NASA responded by redesigning critical systems, more rigorously focusing on risk and overhauling its approach to testing and preparation. Entire systems were tested rather than individual components. And training simulations were made more realistic, conducted when astronauts were tired and with supervisors inserting unexpected failures into exercises. Two years later, Apollo 11 landed on the Moon.

Businesses' approach to cybersecurity must follow a similar pattern. Preparation must be robust. Should a breach happen, the response must be coordinated and rehearsed. And lessons from incidents should be applied to improve preparation for future events. This is the cyber continuum: cyber defence implemented throughout the organisation – always on and always improving.

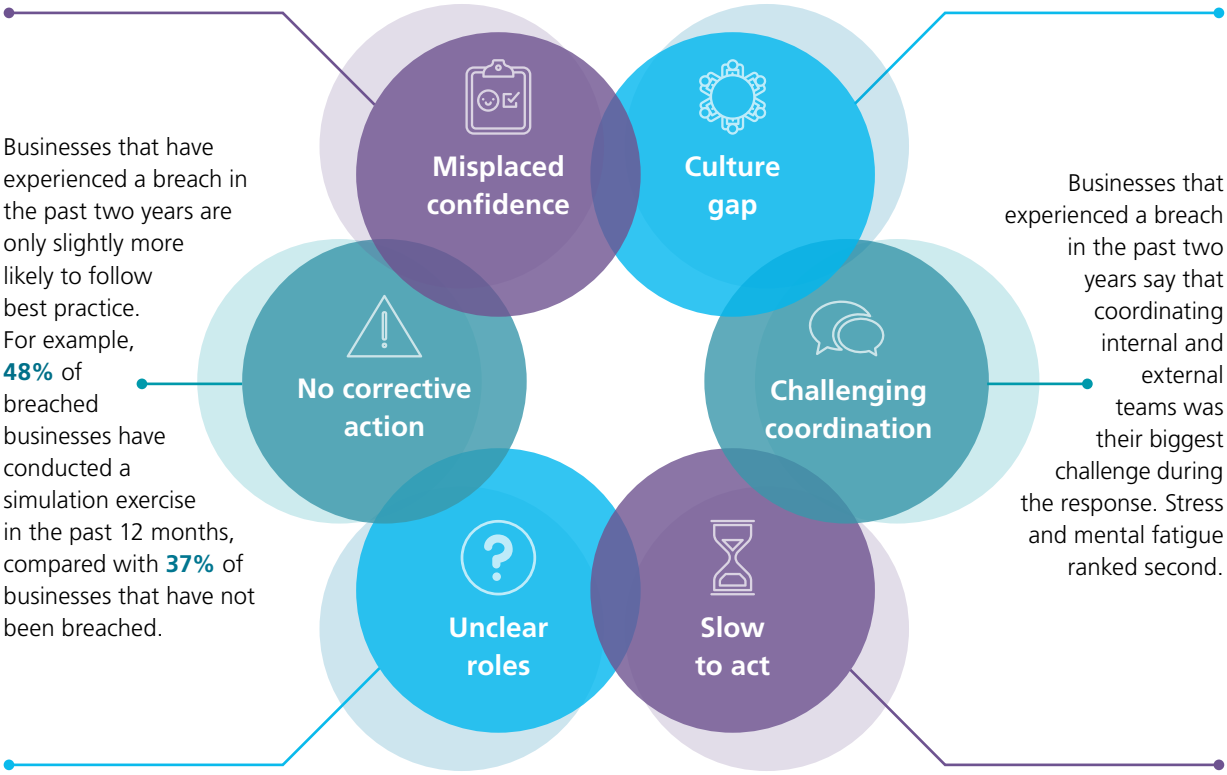
Most of the 400 business executives in our new survey say they are very confident about their ability to prepare for, respond to and recover from a cybersecurity breach. Is their confidence justified? Or is there more that should be done, as NASA found?



What the research tells us

64% of executives say they are very confident about their preparation for a potential cyber breach, but only **40%** have simulated a cyber breach in the past 12 months and only **37%** have audited the cyber credentials of key suppliers.

99% of executives believe they have a strong cybersecurity culture, but only **48%** have departmental cyber ambassadors and just **41%** have employee incentives to promote a cybersecurity culture.



Businesses that have experienced a breach in the past two years are only slightly more likely to follow best practice. For example, **48%** of breached businesses have conducted a simulation exercise in the past 12 months, compared with **37%** of businesses that have not been breached.

Businesses that experienced a breach in the past two years say that coordinating internal and external teams was their biggest challenge during the response. Stress and mental fatigue ranked second.

Non-technical executives are not certain about their personal role in the event of a breach. Just **43%** of legal executives and only **24%** of finance leaders say they are very clear about their remits.

60% of businesses with recent breach experience say they would act faster if a similar event happened tomorrow. This means making consequential decisions with imperfect information. General counsel find this more challenging than other functional heads.

Cyber attacks are rising

In the UK alone, the number of nationally significant incidents more than doubled in the first nine months of 2025 from the same period a year earlier. IBM puts the average business cost of a single breach at USD 4.44m, rising to USD 10.22m in the US. Just five years ago, the global average cost was USD 3.86m.

"The threat environment is going through the roof," says Berin Lautenbach, CISO at international logistics company Toll Group. "Bad actors are ramping up their efforts because there is money to be made from cybercrime. And state-sponsored, geopolitically-driven attacks are becoming more common because they severely disrupt operations. This makes businesses such as ours, which operates critical infrastructure for citizens, much more of a target."

Cyber attacks are not just more common, they are also more intricate and realistic. AI means that phishing emails no longer contain the telltale signs of obvious spelling errors or obscure language. And bad actors can use AI to create deepfakes of executives' voices and images, which makes it harder to identify phishing attempts. They can also deploy AI to identify cyber vulnerabilities and even execute attacks. For example, although not available to the public, Anthropic's Mythos tool can identify high-severity vulnerabilities in major operating systems and web browsers.

How can you prepare for and respond to these threats? In this report, we explain why businesses should treat cyber attacks like other major events such as natural disasters and supply chain collapses. And we show that the response to a cyber incident can no longer be siloed, improvised or overly technical. Instead, it must be embedded into enterprise-wide crisis management frameworks and viewed as a continuous process.

In this report, we explain why businesses should treat cyber attacks like other major events such as natural disasters and supply chain collapses.

This report contains 11 recommendations for businesses to improve the preparation for, response to and recovery from a cyber incident. They are:

Breach preparedness

1. Audit and support important suppliers
2. Take culture beyond communication
3. Prepare with simulation and training
4. Use cyber insurance for more than financial support

Breach response

1. Remember the human dimension
2. Act quickly, even when the situation is evolving
3. Orchestrate external experts
4. Clarify breach roles and responsibilities
5. Preserve trust with a decisive legal response

Breach recovery

1. Intervene early to improve the chance of recovering losses
2. Form a claims defence strategy based on an objective assessment of liability

Breach preparedness

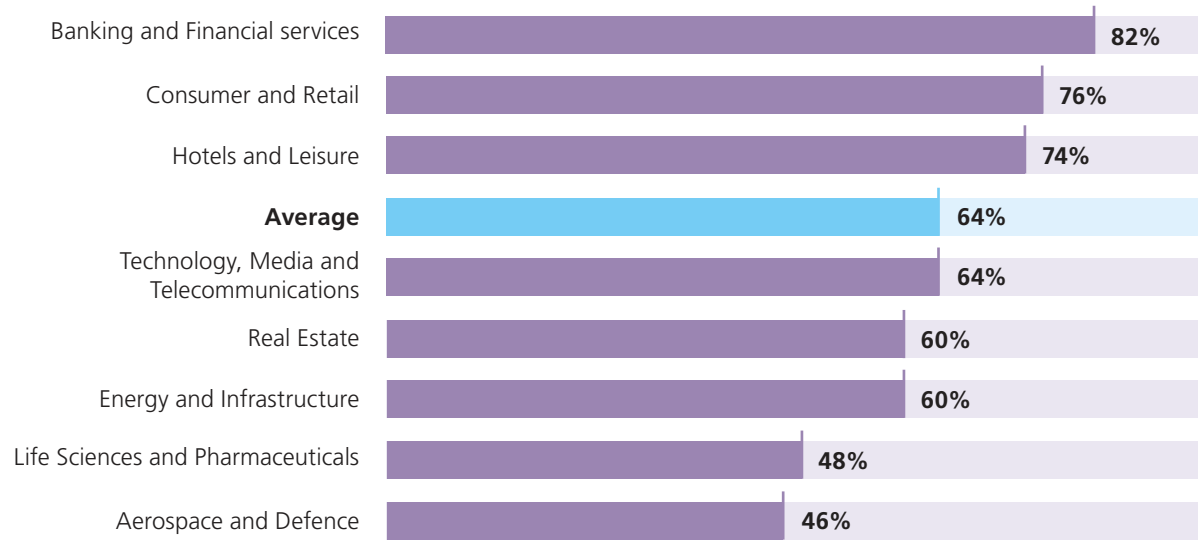
From assumptions to action: how to close the cyber preparedness gap

Our survey shows there is a gap between business executives' confidence in their preparedness for a cyber breach and their practical readiness. Almost two-thirds are very confident, although this figure varies according to business size, sector and whether the business has specific vulnerabilities such as a highly complex supply chain.

Businesses are more likely to be confident about cyber preparedness if they are a larger organisation, operate in banking and financial services or have recent breach experience

(Percentages of businesses that are very confident about their ability to prepare for a potential cybersecurity breach)

By sector

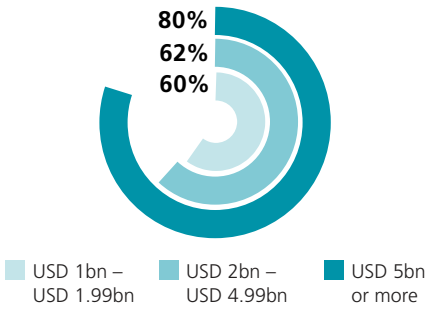


By breach status

Businesses that have not experienced an incident in the past two years

Businesses that have experienced an incident in the past two years

By revenue

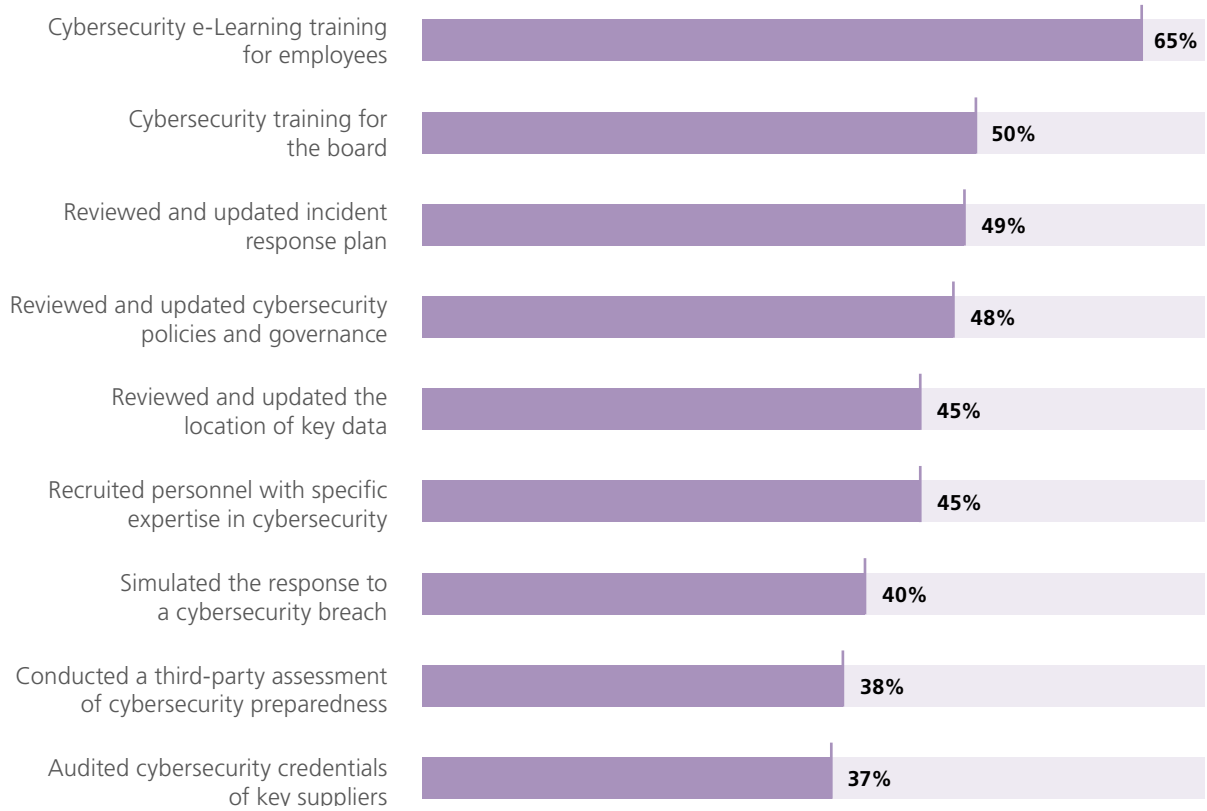


This confidence can, in certain cases, be misplaced. There are some cyber initiatives that businesses should carry out annually, but in the past 12 months only:

— **50%** did board-level cyber training
— **40%** simulated a response to a breach
— **38%** conducted a third-party assessment of cyber preparedness

Many businesses are not as prepared for a cyber attack as they think

(Percentages of businesses that have done each of the following in the past 12 months to prepare for a cybersecurity breach)



Many businesses are simply unaware of cyber best practice and legal requirements, which creates a comfortable but false sense of preparedness. One-fifth of executives admit to not having the expertise to make decisions relating to cybersecurity, and this increases to one-third of executive board members. Others are constrained by budget or time, or just do not expect to be attacked.

Strikingly, recent experience of a breach does not always prompt immediate corrective action. Businesses that have suffered a breach in the past two years are only slightly more likely than others to have taken critical actions: 42% have conducted a third-party assessment of preparedness in the past 12 months, compared with 36% of businesses that have not experienced a recent breach.

Rising threat levels make this approach unsustainable. Poor preparation increases the likelihood and severity of a potential breach. It also means that businesses are less likely to meet their regulatory obligations, such as the need to inform affected parties or regulators in a timely way, which can lead to fines and civil claims.

Recent experience of a breach does not always prompt immediate corrective action.

ACTION 1

Audit and support important suppliers

Suppliers are a growing cyber vulnerability: 30% of breaches in 2025 were linked to third-party involvement, which was twice the proportion just one year earlier.

Nearly all the businesses in our survey (99%) say they actively manage suppliers in relation to cyber risk. For most, this involves conducting compliance checks when new, strategically important suppliers are onboarded. Far fewer (37%) have audited the cyber credentials of key suppliers in the past 12 months.

This needs remedying. "There are a number of low-cost or even free tools from the NCSC (National Cyber Security Centre) that provide proactive monitoring tools to help organisations, but uptake is often miniscule," says Emma Burnett, Head of Data Protection at CMS. "Businesses often suspect that information shared with the NCSC will be passed to the regulator, but this is not the case. They are highly beneficial and those that actively involve national security services in incidents tend to recover faster from a breach."

Today's high threat level means that businesses should not only audit their suppliers, but also proactively improve their cyber credentials. Suppliers benefit from constructive dialogue about the threat landscape and best practice. But just 56% of businesses in our survey have helped more than half of their critical suppliers to improve their cybersecurity in the past 12 months. The rise of shadow AI, the unauthorised use of AI tools without knowledge of a business' IT team, adds a layer of complexity when assessing suppliers as it creates a number of new risks. Employees may inadvertently upload sensitive data to public AI tools, creating confidentiality and privacy concerns. Outputs generated by AI tools may incorporate third-party intellectual property, exposing the business to IP infringement claims. And the use of unsanctioned tools may result in breaches of contractual obligations with clients or other counterparties.

There is also a cybersecurity dimension, as AI solutions adopted outside of formal procurement channels may not meet the organisation's security standards. In addition to ensuring their own employees do not use unauthorised AI tools, businesses must check that their suppliers have robust measures to prevent unsanctioned AI use and to manage the associated risks across their supply chain.

"You can no longer treat vendors as a procurement exercise — in the age of AI, your fourth-party risk extends well beyond direct suppliers to the models they use and why," says Jason Lau, CISO at crypto exchange platform Crypto.com. "I engage at the executive level to surface concerns and build a feedback loop that meaningfully strengthens their solutions."

ACTION 2

Take culture beyond communication

In 2025, 60% of breaches involved a human element. Recognising this, businesses have tried for many years to create a strong cybersecurity culture in which employees at every level are alert to cyber threats and feel empowered to report suspicious activity.

Nearly every business in our survey (99%) claims to have achieved a strong cybersecurity culture. In practice, most are only doing the basics:

76%
have clear and frequent communication from senior management about cybersecurity best practice

68%
have clear and accessible employee guidelines

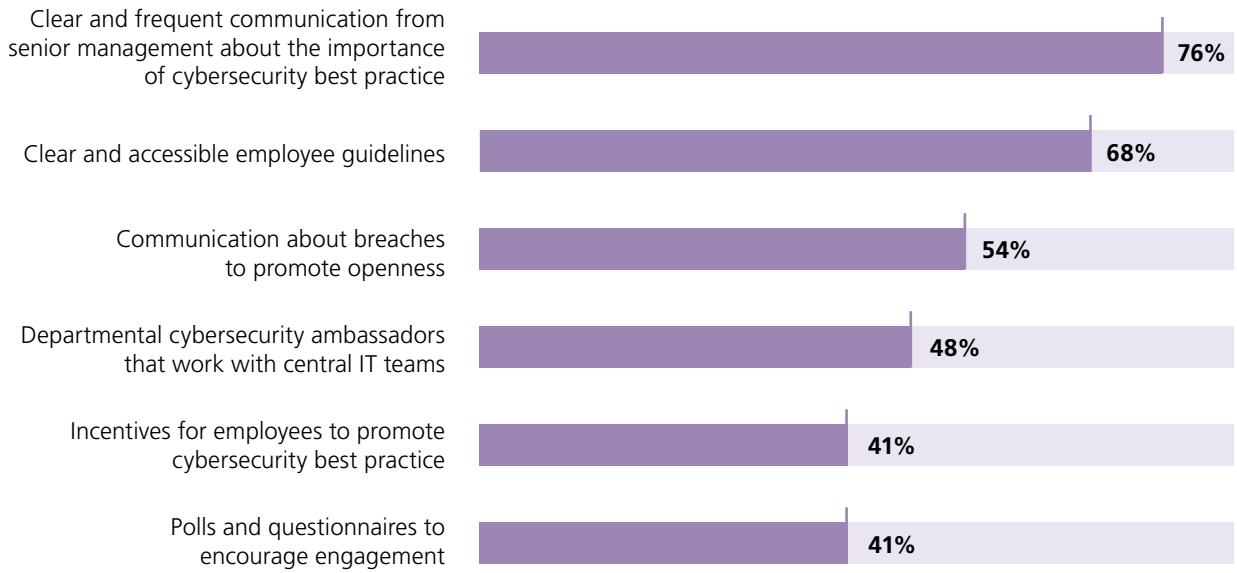
Far fewer are going any further:

48%
have departmental cybersecurity ambassadors that work with central IT teams

41%
have incentives for employees to promote cybersecurity best practice

Businesses are neglecting important parts of a cybersecurity culture

(Percentages indicate those that have each in place)



"The crux of culture is that your employees do the right thing when it comes to reporting suspicious activity while no one is watching," explains Julian Doak, CISO at the Australian National University. "It's critical to adopt different approaches to engaging stakeholders. We have about nineteen thousand students and it's very unlikely they'll read an email from us, so we reach them through social media instead."

Employees who are aware of the cyber threat are much less likely to fall for initial access attempts. Raising cyber awareness is a low-cost exercise, but the benefits can be significant.

"The crux of culture is that your employees do the right thing when it comes to reporting suspicious activity while no one is watching," explains Julian Doak, CISO at the Australian National University.

ACTION 3

Prepare with simulation and training

Simulating a major cybersecurity incident can find gaps in anything from escalation protocols to requirements to notify regulators.

More generally, it is a way to practise your response: it builds muscle memory and helps the people in charge of the response to stay calm in the event of a real breach.

Businesses that are large, have recently suffered a breach or are especially vulnerable are more likely to have simulated an attack, but it is still a low proportion.

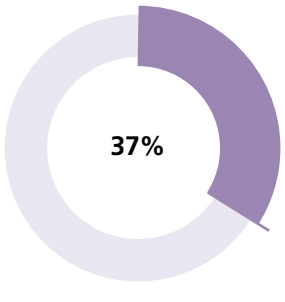
Simulations can be costly and time consuming, but businesses that are not routinely running them are more likely to be unprepared for an attack.

Only 40% of businesses in our survey have simulated a cybersecurity breach in the past 12 months.

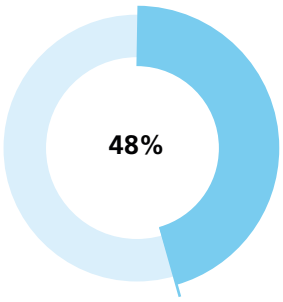
Size, vulnerability and breach history affect the likelihood of a business conducting breach simulations

(Percentages of businesses that have simulated a response to a cybersecurity breach in the past 12 months)

By breach status

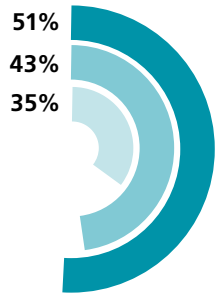


Businesses that have not experienced an incident in the past two years



Businesses that experienced an incident in the past two years

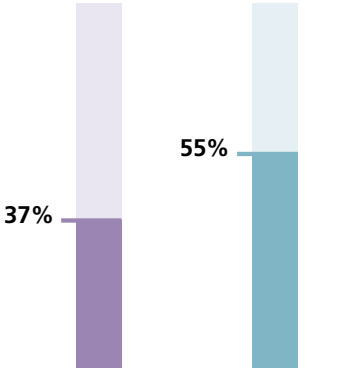
By revenue



USD 1bn – USD 1.99bn

USD 2bn – USD 4.99bn

USD 5bn or more



Note. Survey participants were asked whether their business is vulnerable to cyber attack in any of the following ways. Most (79%) had either one or two vulnerabilities. 12% had 3-4.

1. Operating a highly complex supply chain
2. Handling significant amounts of personal data
3. Owning, operating, or interacting with national critical infrastructure (essential physical and digital assets relating to energy, water, transport, defence and health services)
4. Having a significant proportion of their workforce work remotely
5. Providing online search engines/marketplaces and/or cloud computing services
6. Provide IT infrastructure and/or security managed services

CASE STUDY

How to run an effective cybersecurity simulation

North American natural gas company Énergir frequently simulates cyber breaches with different teams. Once every three years it conducts a full-scale crisis incident for 12 hours starting at 7am, and it is working. "Our last full-scale simulation jumpstarted a lot of our cybersecurity efforts," says Martin Laberge, Énergir's CISO.

Laberge says it is crucial that simulation exercises genuinely challenge everyone involved and closely reflect how a real crisis might unfold. "You can't make it easy," he says. "Executives need to be confronted with difficult decisions – are they willing to pay a ransom or spend two weeks offline while systems are brought back online?"

The scenario needs to be real enough that executives take it seriously. "Sometimes, businesses rely on generic simulation scenarios, but these don't engage the response team," says Laberge. "The worst thing that can happen is for an executive to say that your scenario will never happen. You immediately lose the room. We work with consultants to help design these scenarios to make them as real as possible."

Small tactics such as removing executives' laptops, which would inevitably be compromised in a major breach, create urgency and pressure. "I convinced the president of our largest customer to call up our president in our most recent simulation exercise," says Laberge. "He wasn't expecting that."

ACTION 4

Use cyber insurance for more than financial support

Eight in ten of the businesses in our survey (82%) have cybersecurity insurance coverage. Coverage levels are likely to be lower among smaller businesses that generate less than USD 1bn in annual revenue; these were not included in our survey.

"There can be tendency to either spend money on internal security or on insurance, but the reality is that you have to do both," says Tristan Hall, Co-Head of the CMS Insurance Sector Group. "Some businesses are sceptical that it won't pay out, but it does in the vast majority of cases."

Insurers typically provide a suite of technical and legal experts that can assist in the event of a breach. Many insist that businesses use their pre-agreed panel of experts, but some allow them to appoint their own.

Just 52% of businesses say they have designated external cybersecurity breach legal counsel in place. Designated legal counsel is typically provided alongside a cyber insurance policy, so many more will have this in place without realising it. This is a problem, because external legal counsel should participate in breach simulation exercises to establish ways of collaborating. If the business does not know it has access to them, they will not be invited.

Purchasing cybersecurity insurance also forces businesses to be disciplined in the way they establish their defensive measures. "The conditions of obtaining insurance have become stricter in recent years, and you have to provide evidence of your preparedness," explains the Australian National University's Julian Doak. "It's a useful discipline mechanism. Premiums are lower if you follow best practice, which can be useful in unlocking budget for cyber initiatives."

"There can be tendency to either spend money on internal security or on insurance, but the reality is that you have to do both," says Tristan Hall, Co-Head of the CMS Insurance Sector Group. "Some businesses are sceptical that it won't pay out, but it does in the vast majority of cases."

Breach response

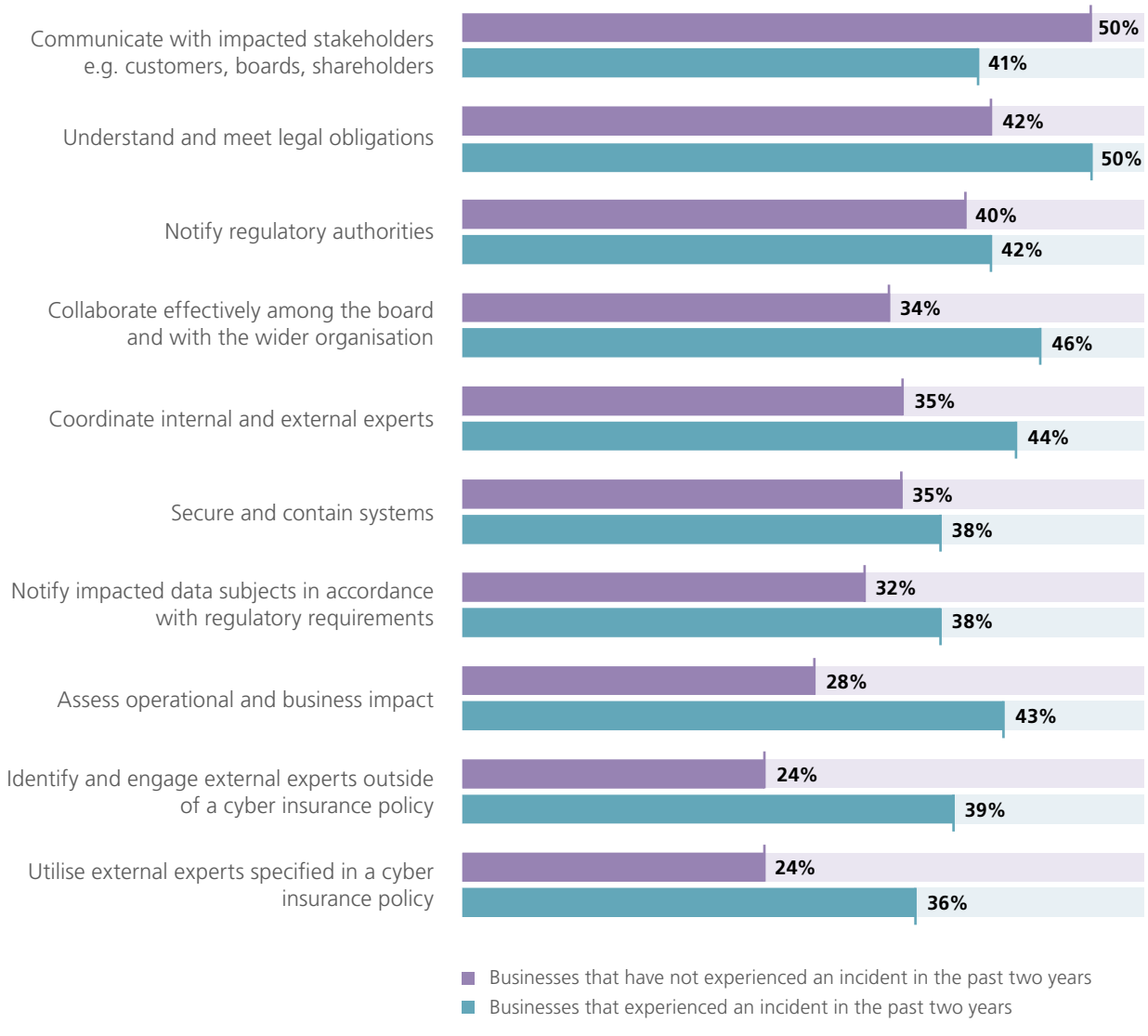
Speed, clarity and composure: a better approach to incident response

Businesses are almost as confident about their ability to respond to a cybersecurity breach in the days following an incident as they are about their preparedness: 59% say they are very confident.

Again, their confidence might not be entirely justified. No more than half of businesses without recent breach experience said they could execute various key aspects of breach response very effectively if attacked tomorrow. We also asked businesses with recent experience of a cyber incident how effectively they carried out the same initiatives during their incident, and again it was only a minority that said they did any of them very effectively.

Incident response is often not good enough

***(Businesses with recent breach experience:** Percentages show the proportion that did each of the following very effectively in their most recent breach. **Businesses without recent breach experience:** Percentages show the proportion that think they could do each group)*



ACTION 1

Remember the human dimension

There is immense pressure on the people who lead their business's response to a major cybersecurity event. Every decision could have significant operational, financial and reputational consequences, and for the individual it can be career defining.

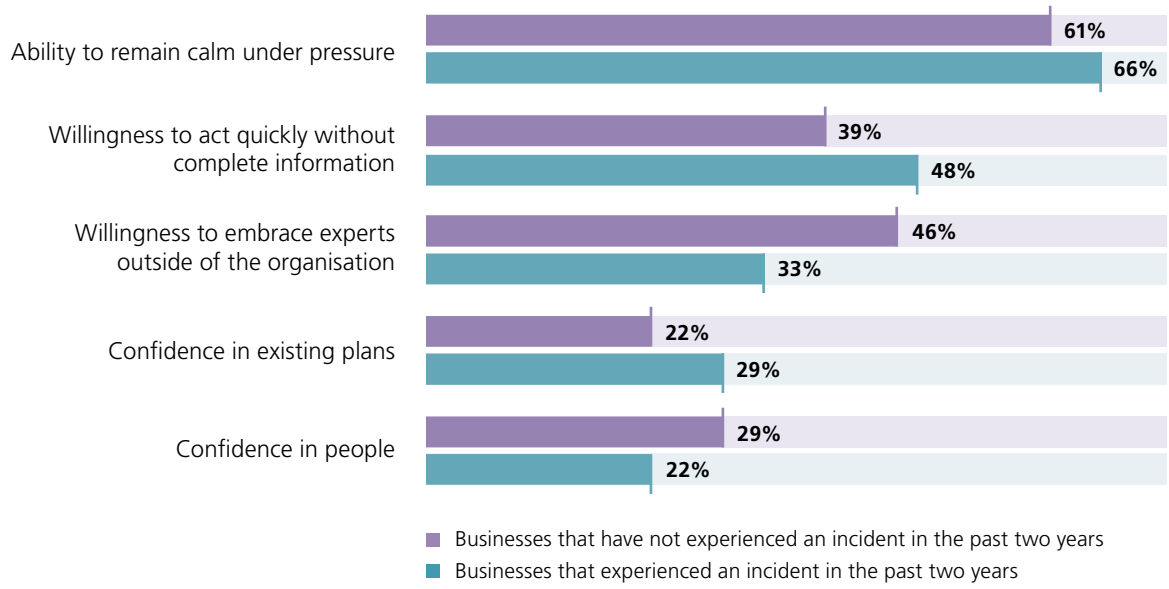
When we asked businesses with recent experience of a breach about their greatest challenge in responding, stress and mental fatigue were second only to coordination across internal and external teams.

"I've known people that went through a major incident and were never the same after," says Énergir's Martin Laberge. "Some CISOs and technical people have resigned after the incident because they never want to endure it again. These are relatively small teams, so you have to work 20 hours a day every day for three or four weeks after the incident to return the business to an operational state."

Teams working on a major incident are less likely to experience high stress levels if the people leading the response do not appear to be stressed. We asked businesses about the leadership mindsets that are most important to effectively responding to an incident, and the ability to remain calm under pressure came out on top.

Composure is crucial to an effective response

(Percentages of businesses that rank each leadership mindset as the most or second-most important during a breach)

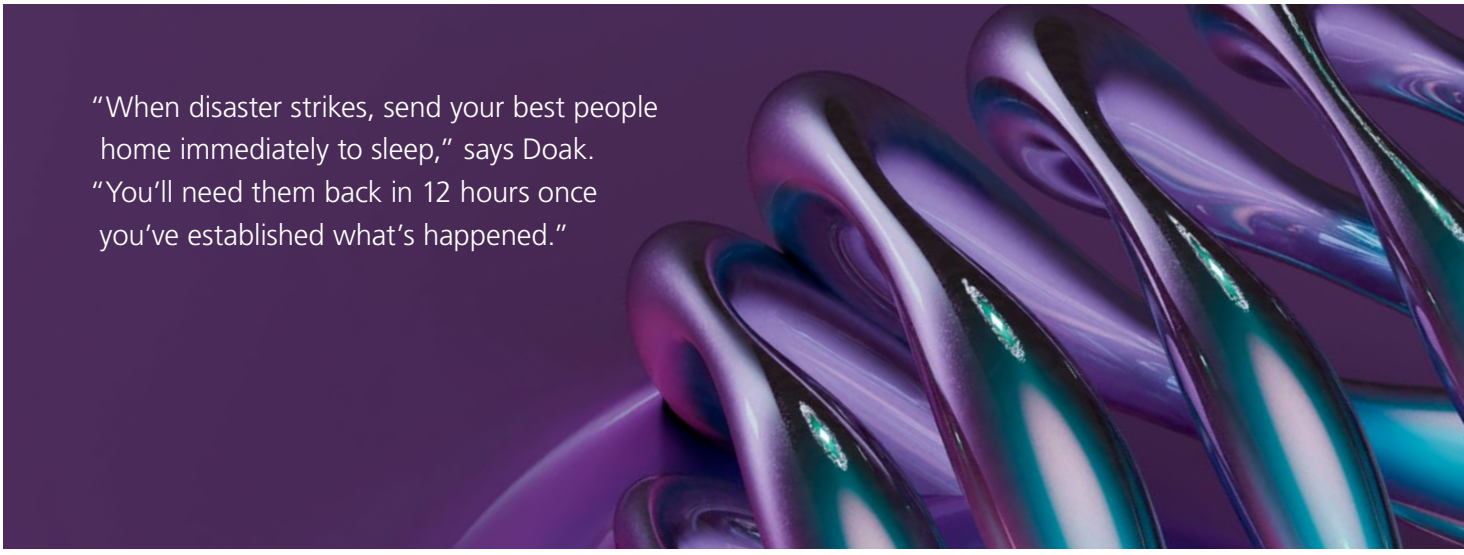


It's really difficult not to burn out, but you need to exercise where possible and eat properly. Look after yourself so you're able to make the best decisions."

Strict shift patterns help teams to switch off and not burn out. "When disaster strikes, send your best people home immediately to sleep," says Doak. "You'll need them back in 12 hours once you've established what's happened. The response needs to be 24/7, so set up two 12-hour shift patterns, going down to a three eight-hour schedule when things calm down a little."

Establish strict reporting protocols to relieve pressure on the response team. In the height of a crisis, leadership might ask for updates every 15 minutes. This takes up valuable time, and in reality, there is relatively little to update management about this frequently. Setting a two-hour reporting cadence frees up the team to focus on identifying and mitigating the issue.

"When disaster strikes, send your best people home immediately to sleep," says Doak. "You'll need them back in 12 hours once you've established what's happened."



ACTION 2

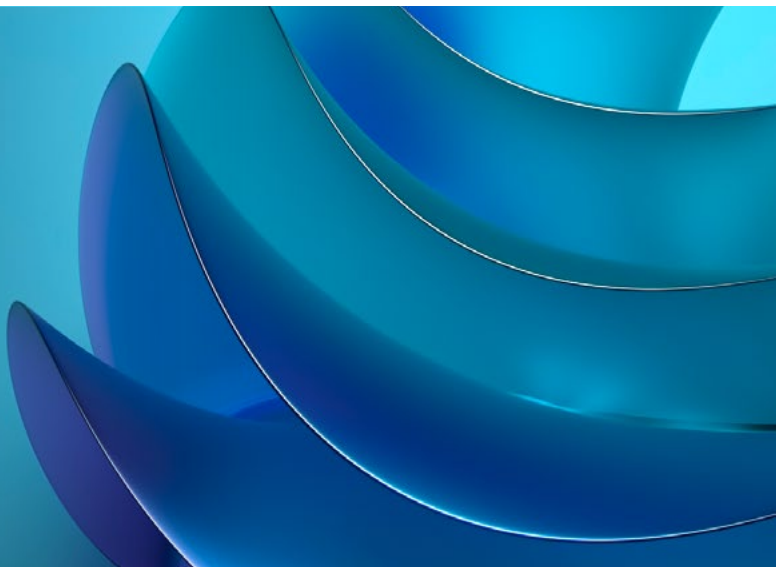
Act quickly, even when the situation is evolving

In a major incident, quick and decisive action is critical. Six in ten businesses that have experienced a significant breach in the past two years say they would act more quickly if a similar event happened tomorrow: faster activation of the incident response plan, quicker engagement of experts and a more rapid shutdown of systems.

This means making consequential decisions without knowing the exact nature of the breach, which will feel unnatural when you are used to making evidence-based decisions.

Acting quickly is essential. When we asked which leadership mindsets are most important to effectively responding to a breach, businesses with recent breach experience ranked a willingness to act quickly without complete information second. Businesses without recent experience of a breach ranked it third.

"Once you've been through a few of these incidents, you realise that you always have to act on imperfect information," says Matthew Bennett, Co-Head of TMT at CMS. "There's a tendency to delay decisions in the hope that clearer information will emerge, but it rarely does."



Empowered people support rapid decision-making

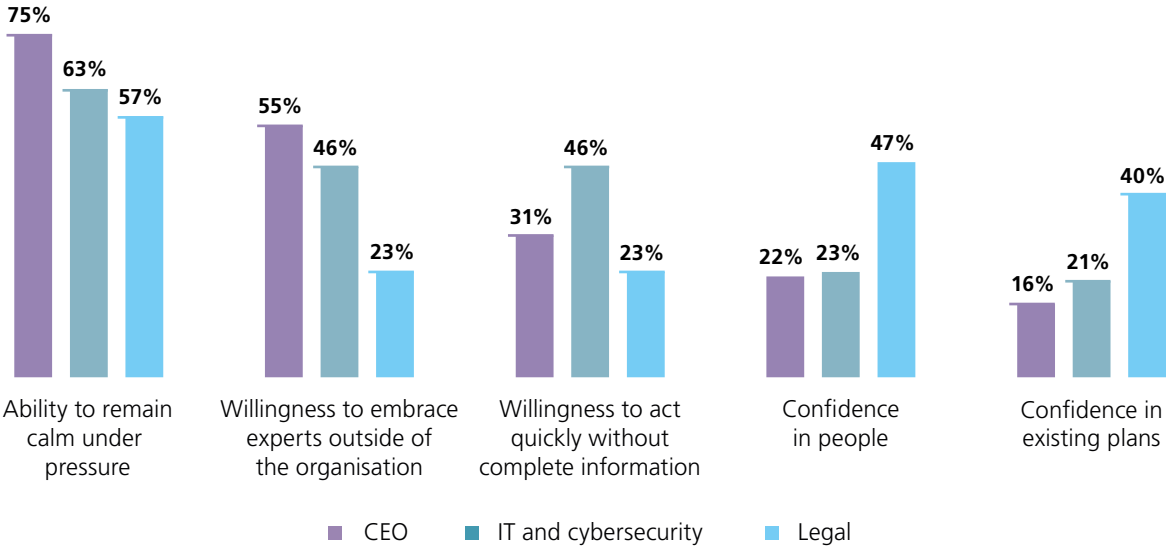
But willingness to make swift decisions is not enough. Businesses should give key individuals the autonomy to make operational decisions in the early stages of a breach as soon as they need to, even if that means not consulting more senior colleagues.

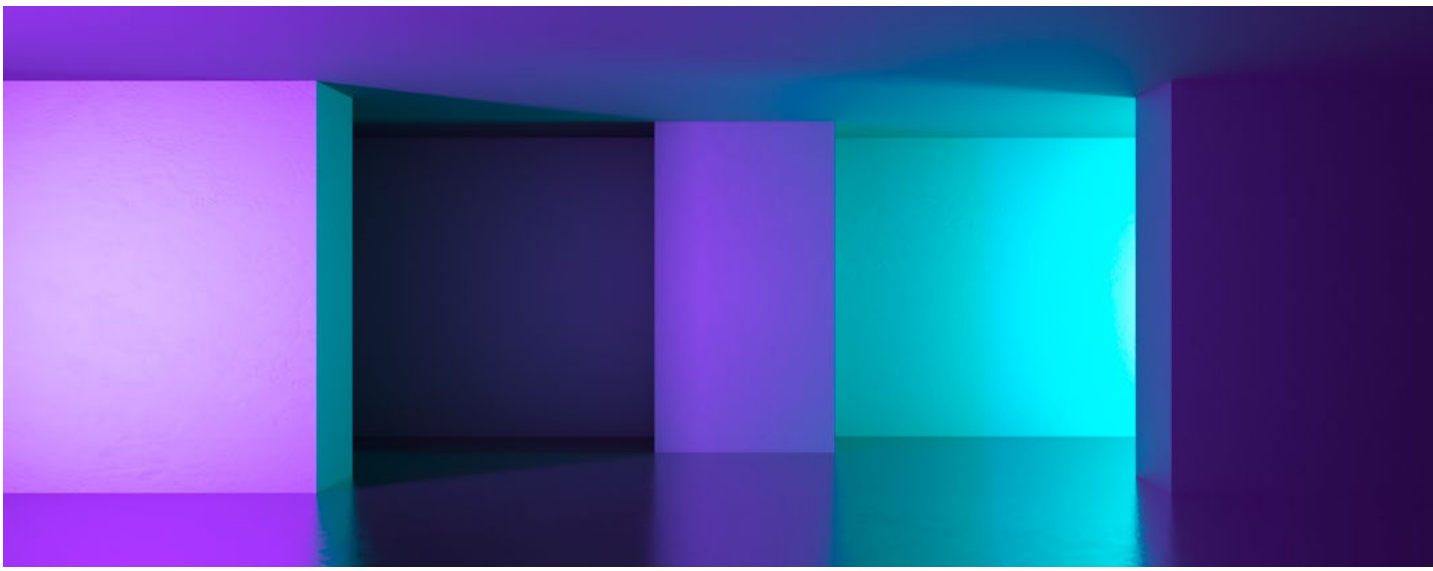
"There are times when the CIO or CISO has to make a unilateral decision on the spot at 2am in the morning to take the business's most critical system offline because there's good reason to believe it's been compromised or is under attack," says Berin Lautenbach, CISO at international logistics company Toll Group. "It's crucial to have these conversations with the CEO and senior leadership team in advance so you feel empowered to act decisively and so they are not surprised if this happens."

Our survey finds that general counsel and heads of legal are less inclined to act decisively in times of crisis. Just 23% of legal leadership identify a willingness to act quickly without complete information as an important leadership mindset, which is half the proportion of IT and cybersecurity leaders (46%). In contrast, legal leaders say that confidence in existing plans and confidence in people are critical leadership mindsets.

Legal leaders are more cautious about acting decisively

(Percentages of functions that rank each leadership mindset as the most or second-most important during a breach)





ACTION 3

Orchestrate external experts

Businesses will call on multiple external experts for assistance in the event of a breach: law firms, IT specialists, PR agencies and potentially others. They will also need a large number of experts within the business, spanning multiple functions, to participate in the response.

Our survey reveals that businesses are struggling to coordinate these different parties. The ones with recent breach experience say their number one challenge was coordinating internal and external teams. Only 44% say they coordinated internal and external experts very effectively, and less than 40% identified, engaged and utilised external experts very effectively, including the experts specified in cyber insurance policies.

Involving crucial third parties in simulation exercises can help businesses to establish ways of working together. "The first step is to get the right experts on retainer," says Énergir's Martin Laberge. "As part of this, include them in simulations and in designing the simulation itself. It helps the internal response team to build trust with outside parties."

Some external experts, such as law firms, can take on the role of coordinating the response, including managing internal and external experts. One tactic that has proved effective is to avoid large meetings that include every internal and external expert involved in the response, which can be difficult to organise and are often unnecessary.

"Many organisations already have strong cyber foundations," says Amit Tyagi, Partner and Solicitor Advocate at CMS. "The real challenge is coordinating people, processes and technology so those measures work together when it counts. It may not be glamorous, but practice really makes perfect."

> The ones with recent breach experience say their number one challenge was coordinating internal and external teams.

ACTION 4

Clarify breach roles and responsibilities

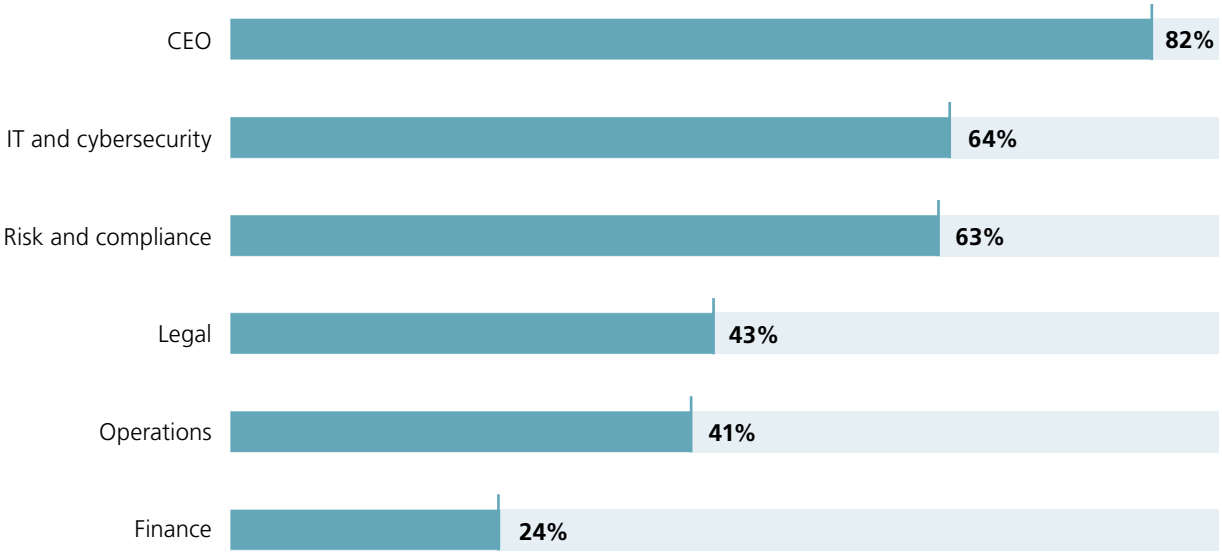
In a fast-moving, high-pressure breach situation, everyone needs to understand their role so that every part of the response is carried out. Alarmingly, our survey shows that this is not always the case.

The good news is that 82% of CEOs are very clear about their personal role and responsibility during a breach, and so are 64% of IT and risk and compliance personnel. But less than half of senior leaders in the legal, operations and finance function say the same, and 60% say that individual responsibilities overlap.

Exactly who is responsible for the regulatory response to a breach can be ambiguous. This includes responsibility for informing regulators and affected parties, and documenting the steps taken during an incident. Some businesses allocate this responsibility to the legal team. Others give it to the risk and compliance or data privacy team.

The finance function is the least clear about its role during a breach

(Percentages of business roles that are very clear about their personal roles and responsibilities if a breach occurred tomorrow)



"Your incident response team must operate like a Formula 1 pit crew — everyone knows their role, their lane, and who makes the call," says Jason Lau of Crypto.com. "Speed is everything in a breach, but you can only move fast when the structure is already in place long before the crisis hits."

At best, unclear responsibilities lead to duplicated effort. At worst, they cause costly delays to the escalation of vital information. Or they cause activities required by law, such as informing regulators or affected individuals, to be rushed or overlooked entirely.

Businesses need to address this by clearly documenting the roles of individuals in the event of a major incident. Simulation exercises help because they expose any ambiguity and instances where responsibility overlaps across individuals or teams. They are a way to instil responsibilities: executives that have recent breach experience are clearer about their personal role in responding to a breach (77%) than executives without breach experience (53%).

ACTION 5

Preserve trust with a decisive legal response

Our survey reveals that only a minority of the businesses that recently suffered a breach executed legal and regulatory initiatives very effectively. These initiatives include:

50%

Understanding and meeting legal obligations

42%

Notifying regulatory authorities

41%

Communicating with affected stakeholders

38%

Notifying affected data subjects in accordance with regulatory requirements

Businesses need to address this urgently. Swift and coordinated action from the legal team will not only manage liability but will also preserve trust and help to shield the business from regulatory action or civil claims. For example, conducting investigations under legal privilege protects sensitive findings from disclosure during potential litigation. Tools such as injunctions against persons unknown can help to freeze assets and trace funds even before the attacker is identified.

Legal teams are also vital in shaping coherent public communications about the breach as well as notifications to affected parties. "It's critical to clearly establish the thresholds at which you need to inform the regulator and data subjects about a breach, but you may want to notify even if this threshold isn't met if it makes practical sense to do so and helps mitigate risk," explains CMS's Emma Burnett. "Communications to stakeholders can build trust if done well, but they undermine credibility if they are unclear or inconsistent."

Breach recovery

Beyond the breach: how to manage the long tail of cyber recovery

Businesses' work does not stop when their systems come back online after a breach. Regulatory investigations and civil claims can last for years. Scrutiny into what went wrong can be protracted. And businesses need to learn lessons and make any necessary changes once the incident is resolved.

But in our survey just 46% of businesses are very confident about their ability to recover from a cybersecurity breach in the longer term. This is significantly lower than the proportion that express the same level of confidence in their ability to prepare for an incident (64%) and handle the immediate breach response (59%).

This is important because the recovery phase of an incident is when legal and reputational risk is highest. It is also when the board must actively determine what the business needs to change to improve future preparedness.

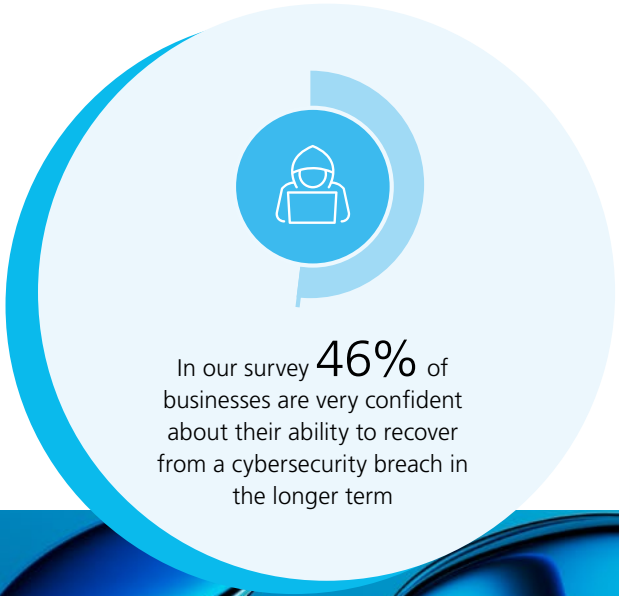
Confidence levels might be low overall, but businesses with recent breach experience say they executed some longer-term technical recovery initiatives effectively.

For example:

— **67%** are very confident that they effectively diagnosed the cause of an incident
— **65%** effectively recorded actions to improve their cybersecurity preparedness
— **63%** effectively learned lessons and made necessary long-term changes

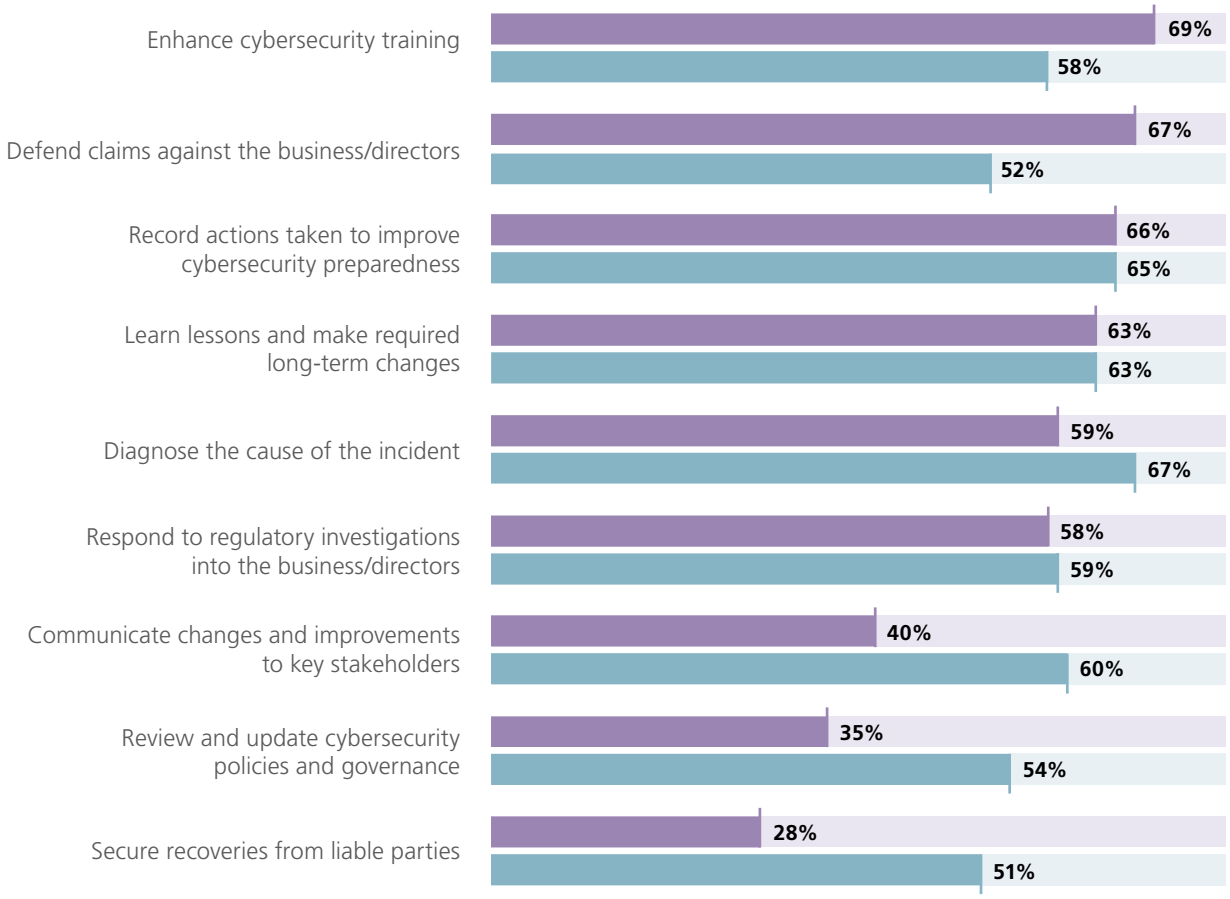
Legal, cybersecurity and IT leadership might struggle to devote enough time to these longer-term recovery initiatives. Establishing a dedicated incident recovery team would help them to deal with the workload.

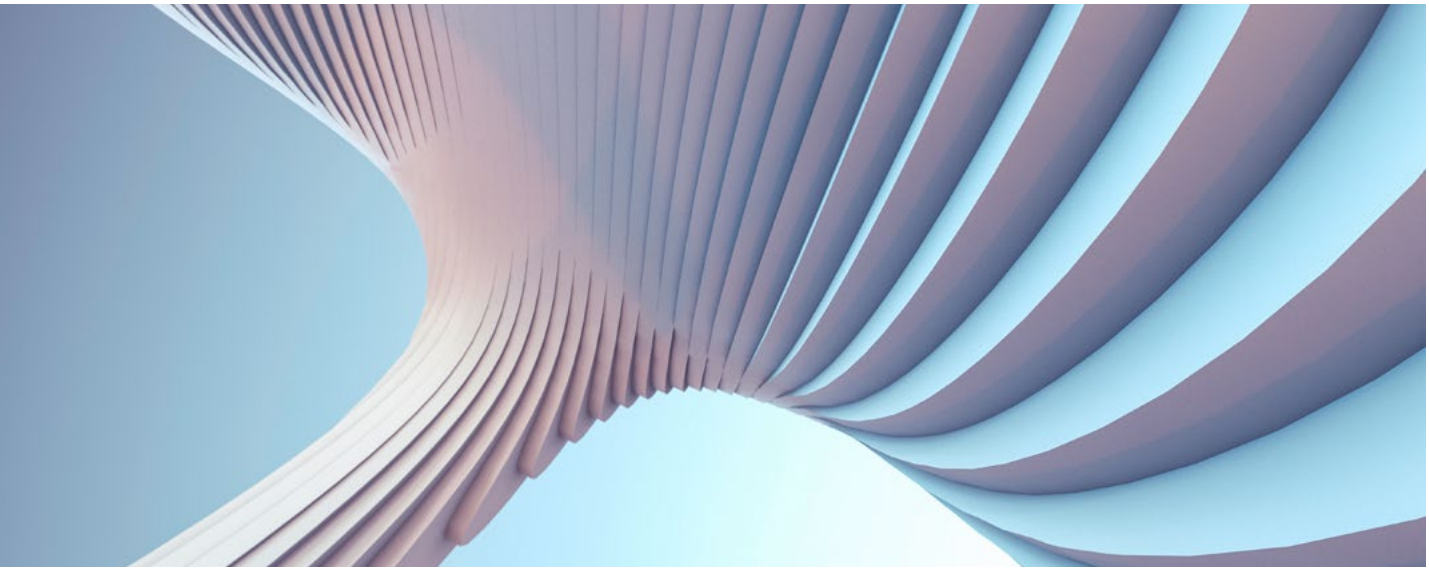
Far fewer businesses say they conducted important legal and regulatory actions effectively, including securing recoveries from liable parties and defending potential claims against the business and its directors.



Recovery from a cyber incident is often not effective enough

***(Businesses with recent breach experience:** Percentages show the proportion that did each of the following very effectively in their most recent breach. **Businesses without recent breach experience:** Percentages show the proportion that think they could do each group)*





ACTION 1

Intervene early to improve the chance of recovering losses

Only about half of businesses with recent experience of a breach (51%) say they are confident that they can effectively conduct the processes necessary to secure recoveries from liable parties. This suggests that a significant proportion of businesses that have experienced a breach, lack confidence in their ability to pursue and obtain recoveries.

It is rarely possible to recover losses from the perpetrator of an attack, because their identity and whereabouts will be unknown. However, it may be possible to secure recoveries from a supplier if it can be determined that the cyber incident would not have happened if it had complied with its contractual obligations.

In many cases businesses do not attempt to seek recovery from their suppliers. Either they do not want to damage their relationship with a supplier of business-critical services, or they know they are unlikely to establish liability, or will be unable to make any meaningful recovery, for example due to contractual limitation of liability. Securing recoveries is even less likely when the provider is small or facing multiple claims, which will affect its ability to pay.

A business can best position itself to secure recoveries in the event of a cyber attack by conducting effective due diligence of its suppliers and careful contract negotiations. Instead of accepting the supplier's standard terms, try to negotiate contract language that appropriately reflects the risk to both parties. For example, it may be possible to negotiate limitations of liability which adequately address the risks and to mandate that the supplier follows best practice relating to software updates. This may make it easier to establish that the supplier was in breach of its contractual obligations if a vulnerability in its software enabled the threat actor to access the systems.

"In my experience, no more than 20% of businesses which suffer a breach attempt to secure recoveries, and about half of these are successful," says Lee Gluyas, Partner in the Litigation and Arbitration team at CMS. "Your chance of success improves if legal teams review contracts and negotiate a fair and balanced allocation of risk during contract negotiation or audit. You are never going to get exactly what you want or persuade a huge supplier to change its terms, but you can often secure terms that will make a significant difference if you need to advance a claim."

ACTION 2

Form a claims defence strategy based on an objective assessment of liability

The number of claims by individuals whose data has been accessed during a cyber breach is increasing, and generative AI tools make it easier for affected individuals to submit claims.

Formalising a strategy to deal with these claims is challenging because it has to be tailored to the circumstances of the breach. The first step is to formally investigate whether there has been any non-compliance.

"Investigations can be tricky, because they usually involve employees who may have been involved in the implementation or monitoring of the compromised security measures," explains Wout Olieslagers, Counsel and Head of the IT and Data Protection practice at CMS Netherlands. "It's therefore important to ensure that the investigation is truly objective. Leadership teams should focus on fact-finding and not point any fingers."

Once it has established the degree of non-compliance, the business needs to determine whether it should pay courtesy compensation to individuals who make a claim. This is where compensation is paid without acknowledging non-compliance.

Timing is vital. Offer compensation too soon, and claimants are likely to demand higher payment and may inform others about the likelihood of securing a payout, and law firms which make a business out of advancing class actions may become more interested. But offering compensation too late causes legal costs to build up.

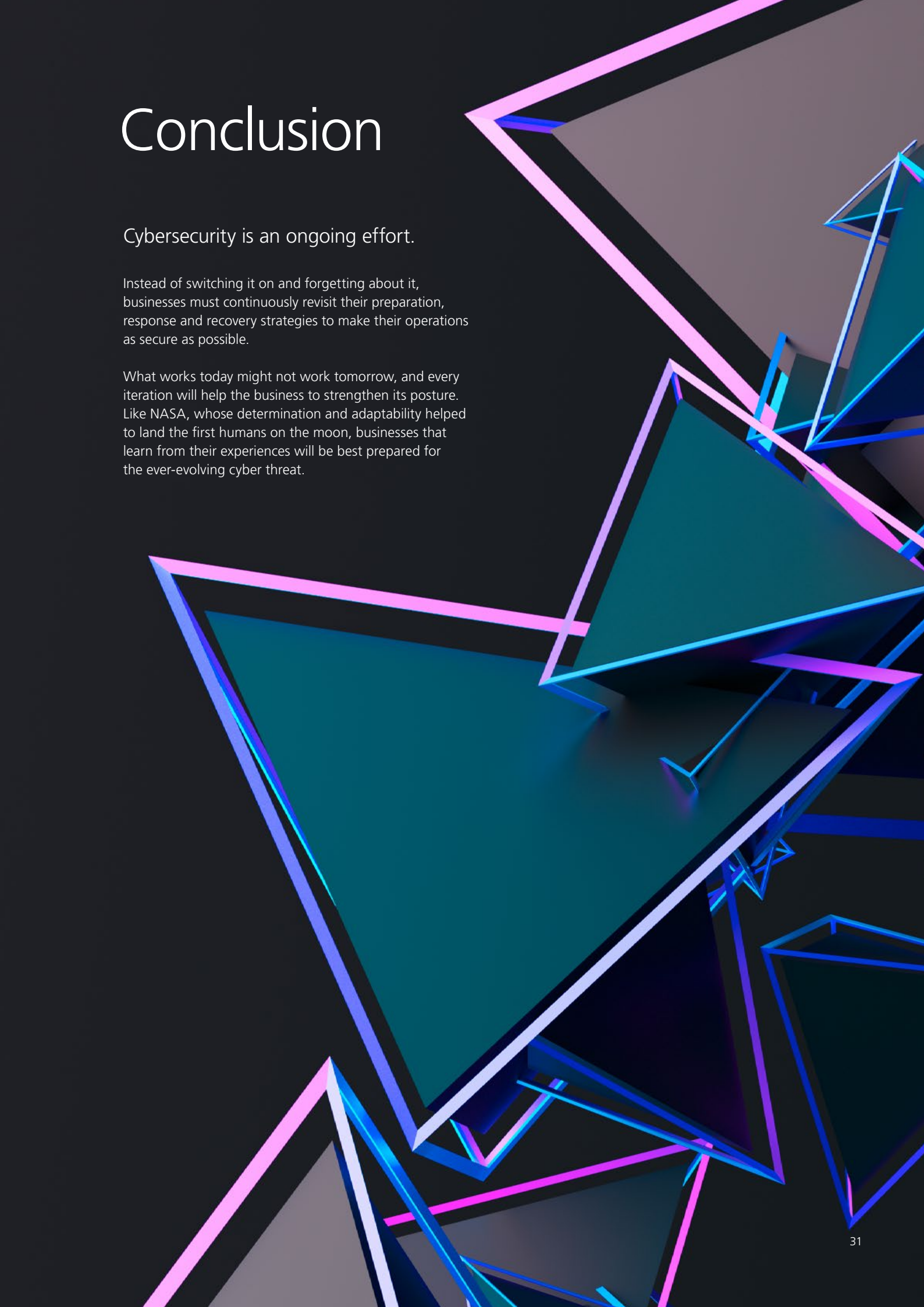
For large claims involving potentially tens of thousands of claimants, the business will need to work closely with PR teams on how it communicates with potential claimants. Whether this is by email or phone, its tone should be sensitive and understanding instead of combative. Offering free annual subscriptions to fraud detection services will demonstrate goodwill and may discourage some potential claimants from advancing claims.

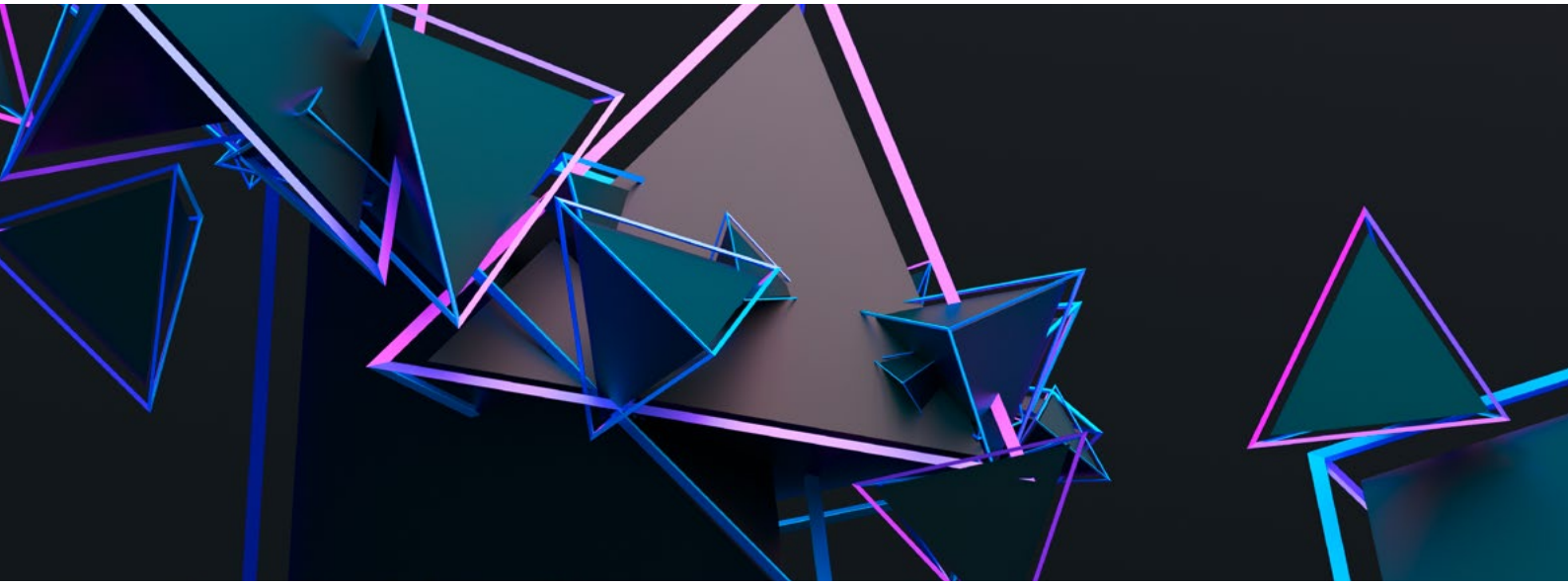
Conclusion

Cybersecurity is an ongoing effort.

Instead of switching it on and forgetting about it, businesses must continuously revisit their preparation, response and recovery strategies to make their operations as secure as possible.

What works today might not work tomorrow, and every iteration will help the business to strengthen its posture. Like NASA, whose determination and adaptability helped to land the first humans on the moon, businesses that learn from their experiences will be best prepared for the ever-evolving cyber threat.





About the research

In February and March 2026, CMS surveyed 400 business leaders in Europe, Asia Pacific and the Middle East. Respondents were C-suite and business executives in the finance, IT, cybersecurity, legal, risk and compliance, and operations functions. Every surveyed respondent works for a business generating at least USD 1bn in annual revenue in one of the following sectors:

- Aerospace and defence
- Banking and financial services
- Consumer and retail
- Energy and infrastructure
- Hotels and leisure
- Life sciences and pharmaceuticals
- Technology, media and telecommunications
- Real estate

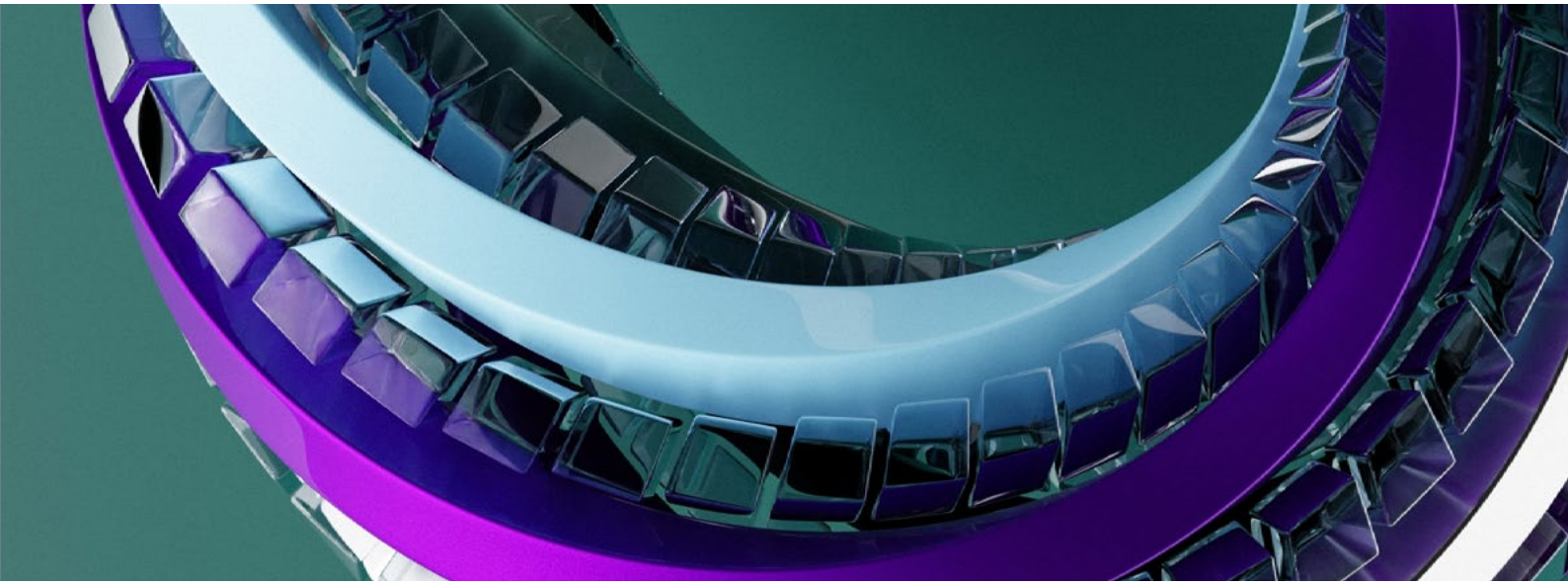
FT LONGITUDE

At FT Longitude, we harness the power of intelligence with influence to leave a lasting impression on the world of business.

With a focus on pioneering thought leadership strategies, we create high-impact campaigns that transform perceptions. We craft powerful insights that engage key decision-makers, and using creative storytelling techniques, we imprint brands with unforgettable messages that resonate.

Part of the Financial Times Group, we help brands reach and connect with the world's most influential people, through the FT's 21 million monthly global readers.

Visit longitude.ft.com and find us on social media.



CMS – your partner in protecting your business against a cyber incident

Cyber threats continue to grow at pace for organisations of all sizes, and across all sectors. Those businesses that prepare for the worst are best placed to respond. CMS can be your partner in protecting your business.

CMS has been advising businesses on cyber issues for over a decade. With experience of over 1,000 breaches, we build robust defences, respond swiftly to incidents, and minimise the risk of financial loss, regulatory penalties, and reputational harm.

- **24/7/365** cyber breach coverage
- **1,000+** cyber incidents to date
- **70+** jurisdictions covered as part of our global cyber network

Key contacts

Emma Burnett
Partner
T +44 20 7367 3565
E emma.burnett@cms-cmno.com

Tristan Hall
Partner
T +44 20 7367 3105
E tristan.hall@cms-cmno.com

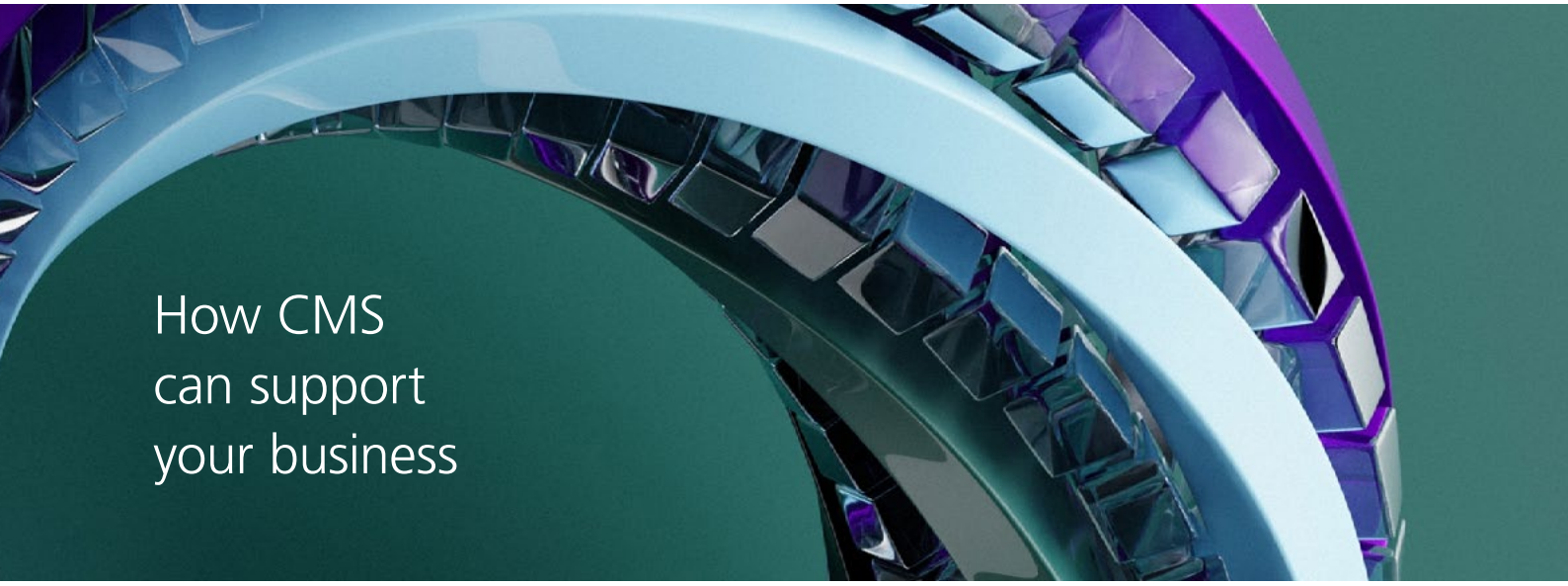
Dora Petranyi
Partner
T +36 1 483 4820
E dora.petranyi@cms-cmno.com

Amit Tyagi
Partner
T +44 20 7367 3578
E amit.tyagi@cms-cmno.com

Lee Gluyas
Partner
T +44 20 7524 6283
E lee.gluyas@cms-cmno.com

Leonard Böhmer
Advocaat
T +31 20 301 62 48
E leonard.bohmer@cms-dsb.com

Wout Olieslagers
Advocaat
T +31 20 259 33 16
E wout.olieslagers@cms-dsb.com



How CMS can support your business

Prepare

- Incident response plan development
- Cyber incident simulation workshops – bespoke simulations tailored to your risk profile
- Risk and preparedness assessment for businesses and directors – evaluating the current compliance state and recommend improvements
- Policy and governance – review cybersecurity policy/governance structures and/or develop a new policy. Ensure policies remain compliant as the law changes
- Cybersecurity training (including CMS e-Learning modules) – to help the workforce understand their role.
- Legal and regulatory advice – guidance on legal requirements and potential consequences of a cyber incident
- Contractual advice to manage and mitigate supply chain cyber risk.
- Data protection registration

Respond

- 24/7/365 breach response hotline with guaranteed response times
- Incident management support including the introduction and management of key vendors e.g., technical incident responders, crisis communications experts, ransomware negotiators
- Legal and contractual obligations advice
- Breach notifications to the appropriate regulatory authorities and data subjects
- Supporting coordination with the relevant criminal and counterintelligence authorities

Recover

- Regulatory investigations – formulate response to investigations into the business and/or its directors
- Defending civil claims against the business and/or its directors
- Defending data litigation claims against the business
- Policy and governance – review and update as required
- Securing recoveries from IT providers or other parties that bear liability for losses
- Assisting with lessons learned exercises

CMS global offices

The Americas

Bogotá
Lima
Mexico City
Rio de Janeiro
Santiago de Chile
São Paulo
Silicon Valley*

Europe

Aberdeen
Amsterdam
Antwerp
Barcelona
Belgrade
Bergen
Berlin
Bratislava
Bristol
Brussels
Bucharest
Budapest
Cologne
Dublin
Duesseldorf
Edinburgh
Frankfurt
Funchal
Geneva
Glasgow
Gothenburg
Hamburg
Istanbul
Kyiv
Leipzig
Lisbon
Liverpool
Ljubljana
London
Luxembourg
Lyon
Madrid
Manchester
Milan
Monaco
Munich
Oslo
Paris
Podgorica
Poznan
Prague
Reading
Rome
Sarajevo
Sheffield
Skopje
Sofia
Stavanger
Stockholm
Strasbourg
Stuttgart
Tirana
Vienna
Warsaw
Zagreb
Zurich

Africa

Casablanca
Ebene
Johannesburg
Luanda
Maputo
Mombasa
Nairobi

Middle East

Abu Dhabi
Dubai
Muscat
Riyadh
Tel Aviv

Asia-Pacific

Beijing
Bengaluru
Brisbane
Chennai
Gurugram
Hong Kong
Hyderabad
Mumbai
New Delhi
Shanghai
Singapore
Sydney

*Representative Office

CMS Legal Updates subscription service

Sign up now for the free online email alert service delivering commentary, analyses and insights from CMS experts on the legal issues affecting your business, directly to your inbox.
cms.law/subscription

CMS locations:
Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bengaluru, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Chennai, Cologne, Dubai, Dublin, Duesseldorf, Ebene, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Gurugram, Hamburg, Hong Kong, Hyderabad, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Mumbai, Munich, Muscat, Nairobi, New Delhi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Silicon Valley, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Sydney, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**