Clifford Chance

BRIEFING

Cyber survival strategies for boards

13 January 2026

Cyber-attacks on global businesses have caused severe business disruption, substantial financial losses and significant negative brand impact. Criticism is increasingly being directed at the board and other senior personnel, with growing numbers of regulatory bodies across the globe placing direct legal obligations on boards and senior management to ensure cyber resilience in conjunction with establishing personal liability risk in certain circumstances.

This briefing considers senior management accountability in the face of new regulations and geopolitical risk and looks at right-sizing strategies. We set out some suggested steps to immediately take in relation to incident response and litigation and well as helping you to benchmark your business's preparedness and know what to do before, during and after an attack.

"In the past six months the cyber landscape has changed for every business, forever," says Jonathan Kewley, a Partner and Co-Chair of the Global Tech Group at Clifford Chance. "High profile breaches in the retail sector, automotive and elsewhere have spotlighted the huge impact of cyber-attacks on operations, operating profit and market cap. Add into the mix, national security threats from state actors and the rise of AI, and you have the perfect storm."

Key takeaways

1. Boards and senior management are increasingly being held accountable (both at a legislative and business/PR level) for cyber resilience and are facing rapidly accelerating regulatory and litigation risk across the globe. It is imperative, for c-suite and senior management to understand their legal and company obligations before, during and after a cyber incident and for them to be prepared to step up and take action.

2. Effective incident response management requires clear planning and testing, cross-functional coordination and rapid escalation protocols,

together with legal review of processes to manage multi-country statutory reporting obligations, tested procedures and secure communication channels.

3 The evolving threat landscape, including AI-driven attacks and stricter regulations, demands ongoing vigilance and proactive board-level engagement.

Why this matters for boards now

Cyber incidents are no longer assessed solely by reference to technical controls or post-incident remediation. Regulators, courts, shareholders and the media increasingly examine how boards anticipated cyber risk, how decisions were taken under pressure, and whether governance frameworks functioned as intended. In recent cases, scrutiny has extended to whether directors received adequate information, challenged management assumptions, ensured appropriate escalation and documented the rationale for critical decisions such as disclosure timing, operational shutdowns or ransom response.

For boards, the issue is therefore not simply whether an organisation was attacked, but whether it can demonstrate reasonable, informed and timely oversight before, during and after the incident. Failures in governance, coordination or decision-making are now as likely to drive regulatory enforcement, litigation exposure and reputational damage as the underlying cyber event itself.

Common pitfalls and how to avoid them

"One of the biggest challenges for businesses is reliance on legacy systems and slow recovery processes, coupled with a lack of readiness to engage specialists. These gaps often lead to criticism of poor transparency and insufficient detail about compromised data," says Partner Megan Gordon. This stems from inadequate planning, including:

- Not having a formal incident response plan (IRP) leading to a lack of preparedness, panic and disorganised decision-making when a cyber-attack occurs.
- Failing to test the IRP to identify weaknesses and train the team in stress scenarios.
- Using outdated plans and contact lists that don't reflect current infrastructure or personnel.
- Neglecting the basics such as timely patching and backups, leaving known vulnerabilities open to exploitation.

"Teams operating in silos is a big mistake," says Patrice Navarro, a Clifford Chance Tech/Digital Partner. "At times we see IT looking at the technical realities, the legal team looking at the contracts, and comms drafting a press release. They are often all working off different versions of the truth." The result is inconsistent notifications to data protection authorities and other regulators as well as to employees and customers. "When those narratives don't match, you lose credibility with regulators and hand ammunition to future litigants," he says. Companies need to establish a "Master Storyline"– a single centralised document and version of the truth that records only verified facts and is updated in real time.

Defining a chain of command is crucial. Samantha Ward, a Clifford Chance Partner specialising in Litigation and Dispute Resolution, says: "We had a case where a significant ransom was demanded, or the company would lose access to its systems. A team of specialists was assembled but nobody knew where the buck stopped or who could authorise a significant payment of that kind. It is important to have well-defined and rehearsed decision-making processes in place rather than having to implement and design these in the middle of an incident."

A common mistake is delayed escalation of early warning signs. "IT teams are often the first to detect anomalies, but if their reports are not acted upon promptly the containment window closes rapidly," says David Olds, a Counsel in the Tech/Digital team based in Hong Kong. The SingHealth cyber-attack, which took place in 2018, is a stark example. IT staff noticed suspicious activity and reported it internally, but middle management failed to escalate it or to respond decisively. The delay allowed attackers to exfiltrate the personal data of 1.5 million patients. "If you don't have a culture of compliance and reporting that moves these things quickly upwards, then you're heading for trouble," he says.

A common global challenge

While cybersecurity regulation differs significantly across jurisdictions, recent incidents reveal a common challenge for multinational organisations: a single cyber event can trigger multiple, overlapping and time-critical obligations at the same time. Data protection authorities, sectoral regulators, financial markets supervisors, law-enforcement bodies and civil litigants may all become engaged within hours or days of the same incident, often applying different legal tests, disclosure thresholds and reporting timelines.

For boards, the complexity lies not only in complying with each regime individually, but in coordinating decisions and disclosures across jurisdictions in a way that is consistent, defensible and aligned with fiduciary and governance duties.

Cybersecurity regulation in the US – enforcement and accountability on the rise

"The US has a multilayered approach with a mix of federal and state laws that results in a fragmented, yet strict, regulatory landscape," says Megan Gordon. "The focus is currently shifting from policy to practice, with a strong emphasis on enforcement actions and individual accountability." State-level privacy laws, such as California's CCPA and CPRA and new rules in Colorado and New York, are expanding protections for consumer data and biometric information and placing more obligations on companies.

The most significant recent case involving an individual was the U.S. Securities and Exchange Commission (SEC) lawsuit against SolarWinds and its CISO, Timothy Brown. Filed in 2023, the SEC alleged that Brown and the company committed fraud by misrepresenting cybersecurity practices to investors prior to the 2020 "Sunburst" cyber-attack. However, in November 2025, the SEC voluntarily dismissed all remaining claims against both SolarWinds and the CISO. "This has sparked considerable debate about the future of individual accountability in cybersecurity governance in the US," says Gordon.

The Federal Trade Commission (FTC) has taken action against CEOs of companies in specific cases where such companies were directly involved in the unlawful collection of personal data, particularly from children.

Since January 2025, the Department of Justice has been active in holding federal contractors accountable for cybersecurity violations under the False Claims Act, indicating a focus on companies that fail to meet security standards stated in government contracts.

"We are also seeing a lot of private lawsuits in the wake of the 2024 incident when cybersecurity firm CrowdStrike issued a security software update to one of its products and caused a widespread IT outage that affected a wide range of industries. As a trend, we have noted that plaintiff attorneys are bringing cases any time there is a cybersecurity breach," Gordon says.

European cybersecurity regulation increases

"There is a 'tsunami' of regulation in Europe, and we are moving from 'guidance' to 'hard law' very quickly," says Patrice Navarro. Regulators are increasingly active and there are three key EU laws driving change: NIS2 – aimed at strengthening the security of critical infrastructure across all member states; the Digital Operational Resilience Act (DORA) which focuses on security and resilience for financial entities; and the Cyber Resilience Act which introduces mandatory cybersecurity requirements for hardware and software products. The EU AI Act also brings in breach notification obligations for certain types of high-risk AI.

"This is a huge new burden for businesses. It's not just an IT issue anymore. It's about board accountability. Under NIS2, for example, members of management bodies can be held personally liable for non-compliance."

Companies also face a new threat – cyber litigation. "Historically, companies worried about GDPR fines. Now a US-style class action is a risk with mass claims for data breaches in Germany and the Netherlands, for example, having already been seen. Boards now need to prepare not only for regulators but for lawsuits."

The UK takes a tougher stance

There are a number of cybersecurity trends in the UK including a rise in group litigation. The recent case of *Farley v Paymaster* confirmed that there is no "threshold of seriousness" that claimants must overcome in order to be entitled to compensation arising from breaches of data protection law in cases of cyber breach.

"Another important trend is an increase in the prevalence of "stock drop" claims where a company's shareholders pursue the company (and potentially individual directors) for losses associated with a decline in share price due to decisions taken by those directors," says Samantha Ward. "We are seeing these claims arise in various contexts, and it is possible that these types of claims could arise following significant cyber incidents - that is something we are already seeing in the U.S"."

In terms of regulatory enforcement, the UK is getting tougher. The Information Commissioner's Office (ICO) is armed with new powers – including the ability to impose penalties under the Data (Use and Access) Act 2025. The Financial Conduct Authority (FCA), while scaling back on

enforcement cases in other areas, remains committed to cyber resilience – periodic fines in the tens of millions of pounds are likely to continue.

The UK Government is also consulting on significant changes to legislation concerning ransomware, including a ban on ransomware payments by public sector bodies and the owners/operators of critical infrastructure. "This is the beginning of a shift away from agencies blindly accepting that a ransom demand should be settled without any implications," says Ward. Jonathan Kewley adds: "Around 80% of our clients say they would pay a ransomware demand so it's interesting that the UK government is looking to push against it. Could it make things worse for businesses? Every company needs to have a ransomware strategy as a means to keep the lights on in a worse case breach scenario – including who is going to pay it? How are they going to pay it?"

With an impending update to laws on cyber in the UK coming too, the UK Government is now urging businesses to prepare for cyber-attacks and to ensure that cyber security is a standing item on the board agenda. And has done this by writing to 250 of the top UK companies.

"Every company needs to have a ransomware strategy as a means to keep the lights on in a worse case breach scenario, including approach to payment decisions, and addressing practicalities – who is going to pay it? How are they going to pay it?" says Jonathan Kewley

Asia-Pacific – direct accountability and stringent reporting requirements

"Cybersecurity regulation in Asia-Pacific is evolving rapidly, and boards and senior managers are now under direct accountability for timely and accurate incident reporting. This is no longer just an IT issue; it is a governance and compliance priority that requires immediate attention," says David Olds.

More jurisdictions in the region are introducing mandatory breach notification requirements and the timelines for reporting are becoming increasingly stringent. In China, for example, cybersecurity incidents may need to be reported within one hour depending on the type of operator and the incident severity. In South Korea, organisations may need to notify regulators and affected individuals within 72 hours of a data breach. "This creates significant challenges for multinational organisations given the variance of reporting requirements across jurisdictions. Boards must ensure that incident response plans include clear escalation protocols and legal review processes to manage multi-country reporting obligations effectively," he says.

Regulators are also making it clear that cybersecurity is a board-level responsibility. In Australia, for example, various governance guidelines have emphasised that proper handling cybersecurity threats is one of a director's duties.

How to prepare for a cybersecurity incident

- **Map regulatory notifications.** Who do you have to contact and when? Companies operating in sectors which are separately regulated on a sector basis (for example, in the UK, by the FCA) will have to co-ordinate their notifications to such sectoral regulators with those to other regulators such as data protection authorities. And these will need to be consistent in messaging.
- **Have a pre-prepared communications plan with decision trees.** "*"It is of course difficult to plan precisely your communications before a crisis happens. However, it does pay to scope in high level terms how you would approach communications, which stakeholders may require engagement and some of the practical challenges that flow from crisis response such as whether you have enough resource to respond to multiple queries on a daily basis, whether onboarding additional PR assistance is prudent and critically, the types of messages you are likely or unlikely to convey to individuals or clients that will ultimately be demanding, emotional and potentially challenging to handle,*" says Samantha Ward.
- **Create an offline "digital safe" for all your key documents, digital response plan and contacts.** When ransomware hits, your corporate network and key apps are often the first thing to go down or be locked. Boards must ensure they have an offline "Digital Safe**"** or separate computer that is *not* connected to the main network.
- **Review supplier contracts.** When you are negotiating contracts, prepare for the worst-case scenario. "If your IT provider goes down, an indemnity clause doesn't get your factory running again. You need operational continuity rights. Do you have "step-in" rights to take over the service? Do you have immediate notification rights (not 72 hours but immediately, so you can lock your own gates)? Can you audit their security now, before the breach happens? And will your supply chain help, in the event of breach, in terms of necessary information and assistance for regulators?" says Patrice Navarro.
- **Assess insurance cover.** Cyber insurance is not a silver bullet, and it is increasingly harder to procure. "Insurance helps, but it is slow. There is a massive gap between the incident and the payout. You need enough liquidity to survive the "burn" of the first three months or so (forensics, PR, lost revenue) before the cheque arrives," Navarro says. Insurers are getting tougher. If you didn't have MFA (Multi-Factor Authentication) on the specific server that was hacked, they might deny the claim, for example. Boards must check if their current security reality matches what they told the insurer. Confirm which technical and legal experts the policy appoints or allows you to appoint – these may not be your preferred choices, so negotiate upfront. Check if the policy covers recovery of stolen or diverted funds and the expected timelines for reimbursement. Failure to clarify these terms can lead to coverage disputes and costly litigation after an incident.

Incident response – key steps in the crucial initial hours

"Most organisations will already have in place a policy on how to deal with a cyber incident, but it is important that those policies be tested and evaluated on a regular basis. In practice, this includes reviewing incident response playbooks at least annually, ensuring there is board-level visibility of cyber risk metrics rather than relying solely on IT dashboards, and having a clear escalation trigger for when management must inform the board so that senior management has visibility of cyber security issues and threat management plans before any crisis hits," says David Olds. When an incident does occur, the tested and validated plan should see the organisation:

- Follow a documented incident response plan (IRP).
- Activate the Incident Response Team (IRT): immediately convene the designated IRT, which should include members from IT, security, legal, human resources, risk management, and communications.
- Confirm and assess the incident: verify that an actual incident has occurred (ruling out false positives) and begin initial data collection to understand its nature, scope, and severity.
- Contain the threat: take immediate action to stop the spread of the attack. This might involve isolating affected systems or networks, disabling compromised accounts, and stopping non-critical traffic to prevent further damage. The goal is to limit the impact without destroying valuable forensic evidence.
- Preserve evidence: document all actions taken and collect system logs and other potential evidence for a future forensic investigation or legal proceedings.
- Establish a secure communication channel: do not use potentially compromised systems (such as internal email) for sensitive incident communications. Have an out-of-band / independent communication channel ready.
- Notify key stakeholders: inform internal leadership, legal counsel, and the cyber insurance provider immediately. Additionally, most cyber insurance policies have specific protocols for engaging approved forensic and legal experts which must be followed.

Obligations on board and senior managers

- The primary role of senior leadership is oversight and readiness to act in the event of a breach, not day-to-day incident management.
- Test the plan at board level. And ensure the plan is followed if needed: the role of the board and senior managers is to then ensure management is executing such a predefined and tested IRP effectively if it is needed in the event of an incident.
- Provide adequate resources: ensure the IRT has the necessary budget, tools, and access to internal and external experts (for example, forensic firms, outside counsel, crisis PR) to manage the crisis effectively.
- Oversee materiality determination: for public companies in certain jurisdictions, senior management and the board must work together to determine if the incident is "material" and thus requires public

disclosure – for example, in the US, this would be through a Form 8-K within four business days of this determination under SEC rules.

- Oversee disclosure and compliance: Be ready to discharge your responsibilities for overseeing external communications. This includes messaging that allows your business to comply with various laws and regulations and to communicate to customers and to the public. There may be a need for nuance between these stakeholders, but the messaging must be consistent.
- Ask probing questions: the board should be proactively armed with up-to-date information, which will mean asking questions about and understanding the nature and scope of the incident, the response plan and potential impacts on business operations, finances and reputation.
- Document the process: regulators and courts will scrutinise the response process. Boards should ensure that both their involvement and the company's response are appropriately documented to demonstrate due diligence and good-faith efforts, while also being mindful of the communications for which privilege protections should be sought.
- Approve key decisions (if necessary): For critical decisions, such as whether to pay a ransom, management may need to seek board approval. The decision pathways for important decisions should be pre-agreed. It is also important to track the legality of paying such ransoms as the legislative landscape develops.

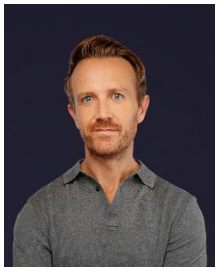
Future risks

Cybersecurity is becoming more complex as AI is increasingly used in cyber-attacks. In 2024, fraudsters targeted the engineering group Arup using a digitally cloned deepfake of a senior manager to induce a transfer of US$25 million. These techniques challenge traditional assumptions about identity, trust and authorisation.

"All response plans should now have an AI dimension embedded in them," says Jonathan Kewley, a Partner and Co-Chair of the Global Tech Group at Clifford Chance, "including how organisations respond to deepfakes, data poisoning or compromise of AI-driven systems. Threats are evolving rapidly – and in the coming years we may face risks that today still feel theoretical, including those linked to quantum computing."

See our latest publication:

- When the lights go out: Navigating leadership in the face of cyber threats



Jonathan Kewley
Partner, Co-Chair of the Global Tech Group, London

jonathan.kewley@cliffordchance.com
+44 207006 3629

Samantha Ward
Partner, London

samantha.ward@cliffordchance.com
+44 207006 8546

Patrice Navarro
Partner, Paris

patrice.navarro@cliffordchance.com
+33 1 4405 5371

Megan Gordon
Partner, Washington DC

megan.gordon@cliffordchance.com
+1 202 912 5021

David Olds
Counsel, Hong Kong

david.olds@cliffordchance.com
+852 2825 8996