The Computer & Internet Lawyer

Volume 43 ▲ Number 3 ▲ March 2026

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

When the Lights Go Out: Navigating Leadership in the Face of Cyber Threats

By Charles Waples, Jonathan Kewley and Lucy Cole

Cyber-attacks have shifted from being an IT headache to a board-level existential threat. In today's hyper-connected economy, a single breach can ripple through global supply chains, trigger regulatory investigations and wipe billions off market valuations. Marks & Spencer's e-commerce was offline for 46 days, losing it £300 million in operating profit and a billion pounds in market cap. Jaguar Land Rover's production lines ground to a halt, with revenue losses estimated at £2.2 billion.

The message for boards is clear: cyber risks are no longer a technical issue – they are a strategic, priority with financial and operational consequences.

This article discusses three key issues:

- Anticipating the Incident: Preparation and Planning;
- First Response: Recovery, Communication and Control; and
- Long-Term Response: Resilience, Insurance and Governance

Charles Waples, the head of interim legal services practice at Odgers Interim, may be contacted at charles.waples@odgers.com. Jonathan Kewley and Lucy Cole, attorneys with Clifford Chance, may be contacted at jonathan.kewley@cliffordchance.com and lucy.cole@cliffordchance.com, respectively.

ANTICIPATING THE INCIDENT: PREPARATION AND PLANNING

Recent headlines tell the story: ransomware gangs targeting logistics giants, state-sponsored actors infiltrating critical infrastructure, and AI-driven phishing campaigns exploiting human error at scale. The cost? Beyond the immediate outage, businesses face contractual penalties, regulatory fines and reputational damage that can/may take years to repair. Boards must assume that a major cyber incident is a matter of "when," not "if." Preparation is crucial for resilience and regulatory compliance.

Boards must demand robust, actionable incident response plans, tested and rehearsed with the same rigour as fire drills. These plans should be concise, role-based and intelligible to non-technical directors, with regular tabletop exercises to ensure the board is ready to lead under pressure.

The initial 72 hours are critical, often triggering mandatory notifications to regulators such as the ICO, FCA,

NCSC and, for multinationals, multiple EU authorities under the GDPR and NIS2.

In a direct call to action, the UK government has urged boards of FTSE100, FTSE250 and other leading firms to prioritise cyber resilience. The letter advises directors/boards to treat cyber risk as a strategic issue, adopt the Cyber Governance Code of Practice, and ensure supply chain partners are certified under the Cyber Essentials Scheme. It also recommends signing up to the NCSC's early warning service to detect threats early, and references the Cyber Assessment Framework as a tool for strengthening critical services.

Crucially, analogue resilience cannot be overlooked. A securely stored, hard copy incident pack listing key contacts, regulator templates and recovery codes may be the board's only lifeline if digital systems are paralysed. In a crisis, this simple measure can mean the difference between decisive leadership and organisational chaos.

Action

- Schedule regular incident simulations and update plans for emerging threats (e.g., AI-driven attacks);
- Mandate the creation and periodic review of physical incident packs, with clear crisis access instructions; and
- Adopt government-recommended practices including CAF, Cyber Essentials certification and the Cyber Governance Code of Practice.

FIRST RESPONSE: RECOVERY, COMMUNICATION AND CONTROL

When systems go dark, the immediate focus must be on recovery, communication and maintaining control.

Restoring operations after a cyber incident is anything but straightforward. Boards must insist that recovery begins only from backups that are proven to be both viable and uncompromised. Recent crises have underscored the necessity for rigorously tested offline backups and well-drilled restoration protocols. The temptation to rush systems back online is strong, but doing so without thorough forensic validation risks compounding the damage and inviting secondary breaches.

Supply chains are the hidden fault line in this equation. Modern businesses operate in a web of interdependencies with cloud providers, logistics partners, payment processors and third-party vendors. Be cautious that contractual liabilities may be triggered if service delivery falters. A single compromised supplier can cascade through the network, halting production lines, delaying deliveries and breaching service-level agreements. For manufacturers, this means idle factories and missed deadlines; for retailers, empty shelves and lost sales. The financial fallout can be severe: contractual penalties, regulatory fines and reputational damage that erodes customer trust. In sectors such as automotive or pharmaceuticals, where just-in-time delivery is critical, the impact can stretch across continents, triggering litigation and shareholder scrutiny.

Boards must recognise that cyber resilience is not confined to their own perimeter but extends to every node in their supply chain.

Customer, Stakeholder and Press Engagement

The reality is stark: customers and markets will detect outages within minutes. Boards are on the frontline, balancing strict legal obligations such as prompt notification and fraud monitoring with the imperative to protect the organisation's reputation. The M&S incident is a cautionary tale: delayed or inconsistent messaging not only erodes public trust but also attracts regulatory scrutiny.

Meanwhile, regulatory oversight is only intensifying. Boards must ensure that disclosures to regulators, markets, and the press are co-ordinated and consistent. A fragmented or opaque narrative can result in sanctions and inflict lasting reputational harm. In the glare of public and regulatory attention, transparent and unified communication is not just best practice – it is essential boardroom governance.

Action

- Demand regular backup testing and ensure restoration plans are rehearsed;
- Insist on forensic validation before systems are brought back online;
- Develop a PR-ready playbook for customer and market communications, aligned with legal requirements and peer best practice; and
- Assign responsibility for regulatory notifications and media engagement. Maintain a single incident narrative for all stakeholders.

LONG-TERM RESPONSE: RESILIENCE, INSURANCE AND GOVERNANCE

After the immediate crisis, boards must focus on long-term resilience and accountability. Directors' duties under the Companies Act 2006, as well as the PRA and FCA rules, place the onus squarely on the board to act in good faith, promote the company's long-term success and exercise prudent management. Critical decisions, such as whether to pay a ransom, require independent judgement, weighing long-term consequences, customer impact, regulatory relationships and reputational risk. While operational response may be delegated, ultimate oversight and accountability must remain firmly with the board.

Cyber insurance is no silver bullet. The JLR incident is a stark reminder that, even with cover in place, payouts can be slow and exclusions are rife.

Boards must have a clear grasp of policy limitations, notification requirements and the reality that immediate losses may need to be absorbed. Insurers are tightening terms, routinely excluding "systemic" events and demanding evidence of robust cyber hygiene before paying out.

The pressure to resume trading after an incident is intense, but boards must resist any urge to rush. Systems should only be brought back online following a comprehensive forensic review and full remediation of vulnerabilities. Recent cases have shown that hasty restoration, without addressing root causes, can lead to damaging secondary breaches.

Action

- Review insurance policies for gaps and exclusions. Consider self-insurance strategies and ensure financial headroom for prolonged outages;
- Set clear criteria for system restoration, prioritising security over speed; and
- Document decision rationales, escalate conflicts of interest and ensure directors are briefed on their specific responsibilities under the Senior Managers Regime.

CONCLUSION

Cyber risk is a business risk. Boards that fail to prepare are gambling with shareholder value, customer trust and regulatory compliance. In an era where supply chains are global and digital, resilience is not optional – it is a competitive advantage. The next time the lights go out, the board's actions in the first hours will define not just recovery but reputation and long-term success.