KEY TAKEAWAYS ›

# Incident Planning, Response and Recovery

Cyber security incidents can have a huge impact on an organisation in terms of cost, productivity, reputation, loss of customers and legal implications. This understanding will provide Boards with the oversight needed to ensure effective planning, response, and recovery processes are in place, strengthening resilience and building confidence in the organisation's ability to manage threats and maintain continuity.

## 1. Incident Response Plan (IRP)

The Board must gain assurance that a Cyber Incident Response Plan (IRP) is in place. This ensures that all stakeholders are prepared, key decisions can be made effectively, and resources are readily available. Strategic decisions, such as whether to pay a ransomware demand, should be agreed upon in advance to ensure swift action during an incident.

## 2. Regular testing of the plan

Regular testing ensures the Incident Response Plan remains effective, identifies gaps, and drives improvement. Testing should occur whenever there are changes, such as new technology, organisational shifts, or emerging threats. The Board should seek evidence of thorough testing, at least annually, and ensure that lessons learned are applied to improve future responses and maintain preparedness.

## 3. Legal and regulatory requirements

Boards should familiarise themselves with the legal and regulatory requirements related to cyber incidents, including data protection laws and industry-specific standards. They should also gain assurance that Executives have considered these regulations and how compliance might be affected, as well as a plan for resuming compliance in the aftermath of an attack.

## 4. Adopt a supportive oversight role during crises

During an incident, the Board provides strategic oversight and supports the Executive team, unless assigned a role in the IRP. The Chair of the Board ensures timely communication with the Board, while the appointed spokesperson keeps stakeholders informed. This approach ensures clear messaging, strengthens trust, and empowers the Executive team to focus on managing the situation, ensuring a coordinated and confident response.

## Remember

Good incident management and planning can reduce the financial, operational, and reputational impact of an incident, as well as limit the impact on suppliers and customers. It's critical for cyber resilience and minimising material harm within your business and across your supply chain.

## Question for the Board

**Does your organisation have an incident response plan in place that is regularly tested?** *Board members should expect direct sight of the plan. Exercises identify improvements and are a far better way to ensure people know what they are expected to do, rather than reading documents. The board should expect to see reporting on the exercise conducted and lessons learned.*