INSIGHT: CYBER THREATS

How to build board cyber resilience


by DAVID DUNN AND JORDAN RAE KELLY

Cyber threats are ramping up and boards need to act now to stay ahead, putting in place incident response plans before the worst happens.

Image: FOTOGRIN/Shutterstock.com

Cybersecurity is not just a technology issue. In today's threat landscape of increased geopolitical tension and nation-state activity, cybersecurity is a matter of national security and presents genuine business risk. In contrast with operational incidents, cyber incidents can quickly spread and create lasting reputational damage, requiring a board-level focus on resilience, mitigating disruption and enhancing response, rather than merely prevention.

Sophisticated threat actors exploit supply chain vulnerabilities, steal sensitive information and influence public opinion through targeted attacks—often against the private sector—placing them directly on the front lines. In response, boards should operate as if a cyber incident is inevitable and assess resilience efforts to ensure proper preparation.

Incident response

Cyber-attacks are not necessarily focused solely on profit, as desired threat actor outcomes can include creating disruption and gaining leverage to further the threat actor's agenda. As a result, incident response plans need to be updated to account for evolving risks and the current threat landscape. Planning for what has already happened versus anticipating new attacks may lead to longer downtime and more significant impacts.

Testing plans in advance of an attack is critical in identifying gaps and ensuring all responsible parties are aware of their exact incident response roles, including board members. Boards should also confirm that incident response plans contain clear decision-making protocols, procedures for communicating with key stakeholders and guidance on regulatory reporting obligations.

Data breach management

Threat actors will seek to find exploitable weaknesses to gain access to sensitive information, whether to hold it hostage for ransom payments or to enhance their own capabilities. While many data breach management strategies focus on containment, there is much to be done beyond stopping the spread of an attack.

Threat actors will seek access to sensitive information, whether to hold it hostage for ransom payments or to enhance their own capabilities.

Recent high-profile cyber-attacks highlight the cascading impacts data breaches can have across all business units. Regulatory compliance, customer trust and investor confidence can all be affected, requiring boards to treat these events as enterprise-wide incidents. During post-breach assessments, utilising forensic efforts to determine what went wrong with decision-making can help turn a crisis into an opportunity to learn and transform an organisation's cybersecurity programmes so they are resilient. An organisation that implements this approach can emerge from a data breach with strengthened resolve and a better understanding of its unique risk profile.

Investigations

Following a cyber-attack, especially one launched by a nation-state or with geopolitical implications, an investigation to determine the root cause and the actual impact is needed both for remediation plans and response planning for future attacks. Investigations should determine what was exploited, missteps in escalation and procedural gaps.

Boards can play a vital role in the investigation process by requiring that lessons learned be integrated into governance frameworks, risk management strategies and third-party oversight. Doing so will prevent mistakes from being repeated and help ensure that investigative findings are leveraged to enhance resilience.

Practical insights

Effective stewardship from the board is critical to building cyber resilience. A board should determine the risk appetite that the organisation is comfortable tolerating, including explicitly clarifying the level of tolerable cyber exposure. This will help guide corresponding preparation plans.

Effective stewardship from the board is critical to building cyber resilience.

Readiness and resilience efforts must be tested using real-world simulations, scenario planning and table-top exercises, with active involvement from the board. These trainings offer practical insight into resilience, both from operational and response perspectives, while in a high-stress environment and when decision making is critical.

Post-incident, capturing key metrics helps create reporting that is actionable, and boards should ensure that more than just technical outcomes are recorded. Incorporating elements such as decision-making agility, collaboration effectiveness and lessons learned will help move cyber resilience from aspiration to reality.

Boards focusing on these areas will make cybersecurity a strategic initiative for their organisations, helping them better withstand sophisticated, nation-state-backed cyber-attacks and everyday threats.

The way forward

Today's volatile geopolitical environment and the advancing capabilities of threat actors have turned cyber resilience into a true measure of organisational leadership. Boards that prioritise incident response, data breach management and post-incident investigative findings demonstrate accountability and position their organisations to withstand and quickly recover from a cyber-attack.

Conversely, boards choosing to view cybersecurity as an unimportant concern or remaining stagnant in their cyber risk management efforts potentially leave their organisations vulnerable to significant operational disruption, regulatory penalties and long-term viability concerns. In the most extreme cases, some organisations may even find that their vulnerabilities present a potential threat to national security.

The leadership barometer for boards has been established, and the opportunity to lead from the front is within reach, especially for those who choose to act decisively.

David Dunn is head of cybersecurity, EMEA & APAC, and Jordan Rae Kelly is head of Americas cybersecurity, both at FTI Consulting.