Nortal

Cybersecurity

Cyber Incident Readiness and Response

Maintaining strong cybersecurity posture demonstrates commitment to protecting sensitive data, safeguarding privacy and protecting shareholder value. It is critical that the leadership must actively engage in understanding the company's cybersecurity posture, risk mitigation strategies, and compliance efforts.

NIST

With the steady escalation of cybersecurity incidents, organizations find themselves grappling with heightened concerns and dwindling confidence in their security measures among board members and executives. Compounding this challenge are new regulatory frameworks such as SEC disclosure and CIRCIA, demanding more rigorous controls and operational readiness against potential breaches.

Nortal has been helping government agencies and enterprises across the globe in their cyber incident preparedness for 25 years. Our Incident Readiness and Response Services build confidence by continuously stress testing the security posture and the incident response processes of the organization.

Incident Response Planning

Minimize financial and reputational risk by comprehensive and effective planning that drives decisive action during a cyber attack

Cyber Incident Simulations, Exercises, & Capability Development

Elevate your organizations preparedness with realistic simulations coupled with capability development activities

Regulatory Compliance

Assess and enhance reporting infrastructure and processes to ensure accurate and timely regulatory action

Prioritizing information security and compliance isn't just a smart move—it's a strategic imperative that pays dividends in both financial stability and long-term success.

73%

Percent of organizations reported at least one ransomware attack in 2023

Fortinet

65%

Percent of organizations that could not fully recover their data after a ransomware attack

Fortinet

$9.5M

Average financial impact of a data breach

IBM

Nortal

Timelines are shorter and the consequences of failure to collaborate are greater when a significant cyber incident unfolds. Nortal Incident Readiness and Response Services, leveraging NIST CSF 2.0, ensures that your organization's incident response plan is effective by validating the accuracy of procedures and identifying weaknesses and the areas for improvement.

Incident Plan Review

Evaluate operational realities against existing incident response processes

Align IR plan to organizational structure, priorities, and risk landscape

Hardened IR processes with NIST recommendations, industry best practices, standards and regulatory compliance requirements

Stress-test IR plan with likely risk scenarios

Attack Simulation

Develop exercises based on MITRE ATT&CK framework to simulate likely cyber-attack campaigns

Practice handling real-world scenarios, train teams and individuals, and test IT & OT solutions in realistic conditions with complex simulation environments

Assess escalation and disclosure processes against regulatory compliance requirements

Learn and Improve

Develop gap analysis, hardening recommendations, and a tactical roadmap

Disseminate learnings from exercises directly into team environments and throughout the organization

Continuous Readiness

IR is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action

Regular cadence of Readiness and Compliance reviews and exercises provide the mechanism for the leadership to regularly assess the incident and compliance readiness of the organization

Nortal

The opportunity to redesign your future is now

Your frictions and frustrations are our insights and inspirations.

Let’s discuss!