SUPPORT MAX

Cyber resilience checklist

The following cyber resilience checklist draws on the U.S. National Institute of Standards and Technologies (NIST) Cybersecurity Framework.

GOAL	STRATEGIC FOCUS FOR BUSINESS LEADERS — WHAT YOU NEED TO KNOW	PROGRESS
PREPARE	**Organize** • Regulatory compliance What are your legislation and compliance obligations in each of the markets you operate in? • Management involvement and remit Who in the leadership team needs to be involved in cyber resilience and risk decisions? • Cyber insurance What kind of insurance do you need/are you willing or able to invest in?	□ □ □
	Identify • Asset management What assets do you have, where are they, who has access to them? What are your most important assets for maintaining business continuity and operations? • Risk management and strategy What are your most exposed assets? What risks do they face? What is the potential impact of an attack in terms of damage, disruption, or loss?	□ □
WITHSTAND	**Protect** • Security processes, policies, and technologies How can you best protect assets, infrastructure, and people within your available resources? • Cybersecurity awareness training How do you train and support employees? • Maintenance and control — patching, etc. Are your security basics in place? Patching, robust authentication, and access controls (multifactor authentication/Zero Trust), etc.?	□ □ □
	Detect • Detection technologies and processes Can your security systems detect and block new and emerging threats? • Security operations center Is your security monitoring reliable and continuous? Can you oversee and manage the entire IT estate 24/7? Do you have access to the tools, skills, and staffing to investigate red flags and anomalies?	□ □
RESPOND	**Mitigate** • Incident response planning and process Do you have an incident response plan that applies across the business? Is it regularly tested and up to date? How do you contain and neutralize incidents? How much downtime can your critical systems sustain? Can you revert to manual processes if needed? If your customers will be impacted, what is the service level that has been agreed to? Is your system on premises or in the cloud? (Is it a security-as-a-service (SaaS) enterprise, business system, etc.) In terms of regulatory compliance, who do you need to inform, and when? • Internal and external communications • Incident analysis and mitigation	□ □ □
RECOVER	**Restore** • Recovery planning Do you have a business continuity plan/disaster recovery plan? Do you have a 'high availability' set up with your cloud provider? Do you need third-party support to uncover and close all gaps? • Internal and external communications • Improvements What lessons did you learn? What steps are you taking/should you take to harden your security?	□ □ □