SECURING THE FUTURE

What You Need to Strengthen Cyber Resilience

There is no question that one of the greatest risks organizations face is the constant threat from cybercrime and ransomware. With nearly every organization facing at least one attack every year, it truly is not a question of if you will face a threat, but when. That is why cyber resilience has never been more imperative to businesses of any size or industry. No organization is immune from its reach.

What is Cyber Resilience?

Cyber resilience is the strategic ability of your organization to not only defend against cyber threats, but also to anticipate, withstand, respond to, and rapidly recover from incidents. True cyber resilience ensures business continuity, reduces downtime, and protects the integrity and value of your organization's data and operations.

11:11 Systems brings together decades of expertise and advanced solutions so your enterprise can stay prepared in a rapidly evolving threat landscape.

The Eight Essential Pillars of Cyber Resilience

A robust cyber resilience program is built on a foundation of both preventive and reactive capabilities. Incorporating and strengthening these eight pillars will fortify and enhance your organization's resilience:

PEVENTIVE RISK CONTROLS

Offensive Security

Proactively identify security program gaps and vulnerabilities before attackers do.

Examples may include penetration testing, vulnerability scans, social engineering, cyber tabletop exercises, vulnerability assessments, and red/purple teaming to enhance cybersecurity and resilience.

Threat Intelligence

Equip your team with actionable, real-time insights to anticipate and respond to emerging threats.

Comprehensive threat monitoring includes dark web surveillance, cyber threat profiling, strategic insights on trends and industry-specific risks, IoT vulnerabilities, geopolitical targeting, and indicator-based tracking like IPs and domains are all good examples.

Cyber Hygiene

Foster a culture that reduces the likelihood of users falling victim to phishing and social engineering.

Examples should include fostering a security-first culture with continual cyber training and awareness focused on safe internet and email use, mobile device security, strong password management, multi-factor authentication, and antivirus software.

Defensive Security

Deploy controls and architectures that ensure the confidentiality, integrity, and availability of your data and systems.

Examples cover key cybersecurity solutions, including firewall management, intrusion prevention, identity and privileged access management, antivirus, patch management, network segmentation, and zero trust security architecture.

REACTIVE RISK CONTROLS

Monitor and Detect

Leverage continuous monitoring to quickly identify and act on potential cyber incidents.

Key examples focus on detection, response, automation, and risk management to enhance security across various cybersecurity tools and solutions.

Incident Response

Establish and routinely test protocols to manage, contain, and mitigate the impact of cyber events.

Some tools and services include comprehensive incident response services, 24/7/365 global support, incident preparedness, detection, containment, forensic investigation, remediation, crisis management, cyber insurance support, and threat actor engagement.

Offline Backups

Maintain secure, immutable backups to guarantee data can be restored in a clean state following an incident.

A thorough data protection strategy includes vital data identification, immutable and encrypted backups, robust authentication controls, air-gapped cyber vaults, physically secured sites, and advanced scanning for data validation and anomaly detection.

Incident Recovery

Develop and validate recovery processes to ensure rapid restoration of business operations and data integrity.

Wide-ranging cyber recovery services include clean data identification, forensics analysis, recovery planning, clean hardware setup, and business continuity strategies. Teams manage the full cyber recovery lifecycle, including testing and exercises, to ensure preparedness and resilience.

Why Cyber Resilience Matters

OPERATIONAL CONTINUITY
Minimize disruption and downtime during an attack or incident.

REGULATORY COMPLIANCE
Meet evolving industry and government standards with confidence.

BRAND TRUST
Enhance your reputation with proven preparedness and responsiveness.

FINANCIAL SECURITY
Limit potential losses and improve cost predictability by mitigating the impact of cyber threats.

By adopting a comprehensive approach to cyber resilience, organizations can transform uncertainty into opportunity, turning advanced threats into manageable risks.

Take the Next Step

11:11 Systems has experts, consulting services, and solutions ready to help strengthen your cyber resilience. With the right preventative and reactive risk controls we can provide you with a comprehensive end-to-end cyber resilient approach. For more information, please reach out to an 11:11 representative.

To learn more about your cyber resiliency, please check out our Cybersecurity Recovery and Risk Assessment to gauge your readiness 1111systems.com/cybersecurity-assessment-ph1

To learn more about cyber resilience, please visit 1111systems.com/solutions/cyber-resilience

THE RESILIENT
CLOUD PLATFORM

11:11 SYSTEMS