CYBER RESILIENCE

WHAT IS CYBER RESILIENCE?

Cyber resilience refers to an organization's ability to withstand, adapt to, and recover from cyber threats and incidents while maintaining the essential functions of its business and protecting its assets. It is a crucial aspect of cybersecurity that goes beyond just preventing cyberattacks. Cyber resilience recognises that despite best efforts to prevent breaches, cyber incidents can still occur, and organisations must be prepared to respond effectively.

Assess: Initially run vulnerability assessments across the full IT landscape to discover all vulnerabilities and weaknesses in your systems.

Prevention: Implement strong security measures to reduce the risk of cyber-attacks.

Detection: Use monitoring tools and threat intelligence to identify cyber threats promptly.

Response: Have well-defined incident response plans for effective action during breaches.

Recovery: Restore systems and data quickly after a cyber incident.

Resilience Testing: Regularly test response plans and preparedness.

Business Resilience: Ensure essential business functions can continue during incidents.

Redundancy and Backup: Use redundant systems and regular data backups.

Employee Training: Train employees to recognize and respond to threats.

Vendor Risk Management: Assess and manage third-party security risks.

Regulatory Compliance: Comply with relevant security regulations and standards.

Partner Compliance: Ensure all new and existing partners/vendors are aligned with the security regulations and standards.

HOW CAN DISCLOSURE HELP YOU BECOME CYBER RESILIENT?

Disclosure Cybersecurity can play a significant role in assisting businesses with enhancing their cyber resilience through various services and practices:

Penetration Testing: Disclosure can conduct regular penetration tests to identify vulnerabilities in an organisation's systems and networks, helping in prevention and detection efforts.

Vulnerability Scanning: Using a range of tools, we will identify weaknesses in computer systems, networks, or applications, aiding in preemptively addressing potential security threats and breaches.

Incident Response Planning: We can assist in developing and fine-tuning incident response plans, ensuring a swift and effective response to cyber incidents when they occur.

Threat Intelligence: Providing real-time threat intelligence, Disclosure Cyber Security helps businesses stay informed about evolving cyber threats, aiding in timely detection and response.

Blue Team: Disclosure will implement various tests to improve the internal defense, vulnerability discovery, threat hunting & modeling, as well as incident management capabilities of an organisation's security team.

Red Team: By simulating cyber-attacks, we can help organisations assess their readiness and improve resilience through red team exercises.

Green Team: Provides vision, operating principles, strategy, and policy to security while maintaining communication with the executive team, with the focus on proactive measures and guiding the organisation's overall security posture

Purple Team: Ensuring governance and risk mitigation to the organisation's security by understanding the evolution of cyber threats, assuring adequate defence measures, and orchestrating comprehensive assessments to enhance resilience and minimise risks effectively, ensuring alignment with organisational goals and executive oversight.

Employee Training: Offering cyber-security awareness training, Disclosure can educate employees on recognising and mitigating threats, strengthening the human element of resilience.

Compliance Guidance: We can provide guidance on adhering to relevant cybersecurity regulations, helping businesses achieve regulatory compliance as part of their resilience strategy.

Vendor Risk Assessment: Conducting assessments of third-party vendors' cybersecurity practices ensures that the supply chain doesn't introduce vulnerabilities that could compromise resilience.

Data Backup and Recovery Planning: Assisting with robust backup and recovery strategies ensures that businesses can quickly restore critical data and systems after an incident.

Continuous Monitoring: Implementing monitoring solutions and providing 24/7 security operations centre (SOC) services aids in the early detection of threats.

Resilience Testing: Disclosure Cyber Security can help organizations regularly assess and refine their cyber resilience plans through testing and evaluation.

By leveraging Disclosure Cyber Security's expertise in these areas, businesses can strengthen their cyber resilience, reducing the impact of cyber threats and ensuring their ability to adapt, recover, and continue operations in the face of a breach.

GIVE US A CALL OR BOOK A DEMO HERE

WHO ARE DISCLOSURE?

Disclosure CyberSecurity Limited ('DCS' or 'Disclosure') is a specialist cyber security company, formed by experienced consultants with extensive knowledge and wide exposure in the cyber security market. We have the breadth and depth of experience to think differently about what really needs to change in a cyber security environment to make our clients more secure and most importantly we have the proven ability to implement this change.

At Disclosure we understand that cyber security is a critical aspect of any modern business. In today's digital world companies are facing an unprecedented situation; the compromise of a cyber-attack is just a "mouse click" away. It's a matter of when, not if, an attack will take place. All organisations, no matter of their size or vertical, are at risk as the cyber criminals are deploying the latest tools, methods and artificial intelligence technologies to automate their concentrated attacks. Continually probing for the weak points in cyber defences, learning and adapting their attacks until they finally succeed!

CYBER ESSENTIALS PLUS

Disclosure currently possesses a vast range of cyber security accreditation.

Our guidance, expertise and technology will assist in the acquisition of a variety of Cyber Security Certification for your Business.

FIND OUT MORE

Information Security Management System ISO 27001 Certified

CREST

50%

OF UK BUSINESSES STILL REPORT A BASIC TECHNICAL CYBER SECURITY SKILLS GAP

39%

ALMOST TWO IN EVERY FIVE BUSINESSES REPORTED SUFFERING CYBER SECURITY BREACHES OR ATTACKS IN THE LAST YEAR

Source: NCSC

CONTACT US

+44 7903 565 861

info@disclosurecybersecurity.com

@ disclosurecybersecurity

/ disclosurecybersecurity

Disclosure Cyber Security (UK&I)
Basepoint
1 Winnal Road
Winchester
SO23 0LD