MAXSUM CONSULTING

Enabling Opportunity, Realising Potential

Top 10 Tips to Boost Your Cybersecurity Stance

Appoint someone at exec / board level to be responsible for cybersecurity who will have the authority and know-how to address the risks and demonstrate leadership during times of crisis.

Include cybersecurity on every board agenda or senior exec meeting, reporting on: risk to the business, nature of sensitive data and mitigation progress at a minimum.

Treat cybersecurity as a company-wide business risk and assess as you would with other key business risks such as major safety issues, environmental disasters and accounting scandals.

Ensure that the company understands the rapidly developing legal landscape that applies to cyber risk in particular.

Get specialist expertise to advise and inform execs / board, whether from internal teams or external advisors.

Set a programme of work to manage cyber risk, allowing a realistic time and budget.

Encourage discussion about cyber risk management**,** risk appetite, risk avoidance, risk mitigation and cyber security insurance.

Assume you have already been breached but you might not yet know about it. Take action to reassure yourself no such attack has taken place, but plan on the assumption that they have.

Educate your employees regularly and start building cybersecurity education, training and best practice into your organisation's culture.

Ask who uses, accesses, repairs, or maintains your data or systems about your organisation's data compliance rules and requirements.

PTO for Maxsum's Cybersecurity Assessment →

Assess Your Cybersecurity Stance Now!

Category	Actions	Readiness Score (0-10)	Actions/ Comments
Asset Management	• Physical devices and systems are inventoried • Software platforms and applications within the organisation are inventoried Information assets are inventoried Information assets have an assigned owner • Information assets are valued • External information systems are catalogued • The security posture of external service providers and partners is assessed		
Governance	• Organisational information security policy is established • Information security roles & responsibilities are coordinated and aligned with internal roles • Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed • Incident response and recovery plans, including public relations and communications plans, have been prepared and tested		
Risk Assessment	• Asset vulnerabilities are identified and documented • Threats, both internal and external, are identified and documented • Potential business impacts and likelihoods are identified • Threats, vulnerabilities, likelihoods, and impacts are used to determine risk • Risk responses are identified and prioritised		
Identity and Access Management	• Identities and credentials are issued, managed, revoked, and audited for authorised devices, users, and processes • Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties • Two-factor authentication is deployed for key accounts and applications		
Awareness and Education	• All users are informed and trained • Privileged users understand roles & responsibilities • Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)		
Data Security	• Sensitive information is protected, e.g. by encrypted filesystems • Sensitive information in transit is protected, e.g. by use of SSL/TLS or virtual private network • Mobile devices are protected by encrypted filesystems and mobile device management		
Information Protection	• Data on desktop and laptop computers is backed up with an offline backup • Backups of information are conducted, maintained, and tested periodically • Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed • Response and recovery plans are tested		
Maintenance	• Systems are proactively patched		

This checklist has be produced with reference to the NIST Cybersecurity Framework
https://www.nist.gov/cyberframework