Cyber Risk Exposure Scorecard
– Manufacturing

The manufacturing industry is at a crucial turning point of constant technological progress and heightened interconnectivity between systems and procedures. While the traditional focus on efficiency, productivity and quality remains, it's becoming increasingly important to incorporate cybersecurity principles into the core of operations.

A comprehensive cybersecurity scorecard is a valuable asset for evaluating the overall security stance of manufacturing companies that increasingly rely on internet-connected industrial systems and machinery. This scorecard highlights key areas of focus, including governance and policies, access control, network security, data protection, security awareness and training, vendor and supply chain security, compliance and regulation, security technology and cybersecurity culture.

Please assign a score from 0-5 for each question based on your organization's compliance or implementation level. A higher score indicates a better cybersecurity posture. Consistently evaluating and updating the scorecard will aid in monitoring progress and pinpointing areas for enhancement.

Questions	Score
Governance and Policies	
Has a documented cybersecurity policy and incident response plan been developed for the business?	
Are regular cybersecurity risk assessments conducted specific to the manufacturing environment?	
Are security roles and responsibilities clearly defined within the organization?	
Access Control	
Are access controls implemented for systems and personnel?	
Are strong authentication methods (e.g., multifactor authentication) in use?	
Is user access reviewed and updated on a regular basis?	
Is third-party access to critical systems controlled and monitored?	
Network Security	
Are firewalls and intrusion detection/prevention systems in place to protect networks?	
Is the network segmented to limit the lateral movement of attackers with manufacturing operations?	
Are regular network vulnerability assessments conducted?	
Is network traffic continuously monitored for anomalies?	
Data Protection	
Is sensitive data encrypted in transit and at rest?	
Are data backup and recovery procedures established?	
Are regular data security audits conducted?	

Questions	Score
Security Awareness and Training	
Do employees receive training to educate them on cybersecurity threats within the manufacturing environment?	
Are there procedures for reporting security incidents?	
Is the security training frequently updated to address new threats?	
Vendor and Supply Chain Security	
Are cybersecurity requirements in vendor contracts?	
Is vendor security assessed before engagement?	
Are there mechanisms in place to monitor vendor cybersecurity?	
Is there a process for assessing and mitigating supply chain risks?	
Compliance and Regulation	
Are cybersecurity standards and regulations relevant to the manufacturing industry complied with?	
Are regular compliance assessments and audits conducted?	
Security Technology	
Are antivirus/anti-malware solutions deployed and updated?	
Is security patch management implemented for all systems?	
Is endpoint security configured and managed effectively?	

Questions	Score
II. Cybersecurity Culture	
Does the company foster a culture of cybersecurity awareness and responsibility?	
Is cybersecurity integrated into the company's core values and mission?	
Total Score:	

Very High Risk: 0-50

High Risk: 55-80

Moderate Risk: 85-110

Low Risk: 115-140