9-POINT CYBER RESILIENCE CHECKLIST for manufacturers

Integris.

A cyber resilient organization is well prepared to tackle cybersecurity incidents and can effectively respond and quickly recover when such events occur.

On a scale of 1-5, with 5 being strongly agree, please rate your organization.

	1	2	3	4	5
☑ **Do you feel your business is well prepared to meet the growing cybersecurity requirements and certifications in your industry?** (ie. The CMMC-Cybersecurity Maturity Model Certification, the NIST-National Institute of Standards and Technology Certifications, or The ISO- International Organization for Standardization, and more.)					
☑ **Do you currently have clients that are asking you to present proof of cybersecurity insurance? Are you confident that you are meeting the security protocols required to be covered by a cybersecurity insurance provider?** Do you have the Security Incident and Event Management software (SIEM) that allows you to isolate and forensically investigate breaches once they have occurred? Do you have round-the-clock monitoring of your cybersecurity? Do you have endpoint detection programs that can track hackers once they have slipped past your defenses?					
☑ **Are you confident that you could quickly restore your systems and have your floor running again in the event of a natural disaster or cyberattack?** Where does your system back up? And do you have a secondary backup system? How much downtime would you experience while your backups are being restored? Would any data be lost? Does your leadership team review your response plans regularly, and does everyone know what to do in the event of an emergency? What are the impacts on your client's businesses if you are unable to resume operations? How will you communicate with them?					
☑ **Do you feel that your firewalls and security protocols are updated enough to protect your manufacturing facility and offices from a cyberattack?** Are you sure your system is being promptly updated when the latest security patches come out? Do you have robust systems that protect your system and employee passwords, like multi-factor authentication, and zero trust networks? Do you have threat detection systems protecting your emails from phishing and impersonation attacks?					
☑ **Do your employees have access to cybersecurity training on a regular basis? Are new hires trained on cybersecurity when they start work with your organization?** To keep up with the ever-evolving threats presented by hackers, any employee operating computerized equipment should receive training at least every six months. Do you have experts on hand to teach the material they need to know, or online courses they are required to complete? Are your employees graded for comprehension, and are those results stored so they can be presented when clients or certification agencies ask for them?					
☑ **Does your organization have a budget for cybersecurity, and an investment plan for the future of your security efforts?** Has your organization put together a cybersecurity investment plan that steps out your security spend over the next few years? Is refining and protecting your security system considered a normal cost of doing business?					
☑ **Does your organization have anti-malware protections on your AI, AR, or Robotics Systems?** If the answer to this question is yes, how well do those malware protections integrate into your other office/factory systems?					
☑ **Does your organization have protections in place to keep your client's proprietary and identifying data safe?** Can you articulate your data handling strategies when clients ask to see them? Do you have any mitigation strategies in place in the event of a data breach? Do you have a handle on what a data breach could mean to your manufacturing company?					

TOTAL:

0-25 **25-30** **30-35** **35-40** **40-45**

Got your score? Great! But does your company have insurance that covers the first and third-party financial losses from cyberattacks? If you don't – your company isn't ready for a data breach, no matter what your score

Is your organization cyber resilient? Iconic IT offers free consultations with an expert.
Request yours at at sales@integrisit.com or
integrisit.com/contact