9-POINT CYBER RESILIENCE CHECKLIST for nonprofits

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
☑ **How well do you understand your organization's cyber risks?** Does your board and leadership team understand and periodically review the organization's exposure to cyber compromise? Do they know how to address the risk of a cyber breach, and ensure that cyber resilience is built into the core operating processes?					
☑ **How well do you understand the consequences of a breach?** Does your board and leadership team understand the consequences to the organization, donors, clients, and the community in the event of a failure or disruption of operating systems or the compromise of intellectual property, commercially sensitive information, or data held in trust for employees, clients and donors (such as personal and credit card details)? Can they predict how such a breach will be reflected in the organization's reputation, and credibility?					
☑ **How well do you understand your IT systems and the data it holds?** Does your board and leadership team understand the value of your data to those of malicious intent? Do they know where the data is, how it is protected, and who has access to it?					
☑ **How good is your cyber hygiene?** Do you have regular patching of software and operating systems, password policies, multi-factor authentication (MFA), monitoring, email threat detection?					
☑ **How solid is your backup and recovery process?** Do you have a backup strategy that is redundant and can recover your operations quickly after an attack? Does your board and leadership team review the response plans on a regular basis, so it is ready to be implemented immediately if an attempted attack is detected?					
☑ **How advanced is your malware protection?** Do you have artificial intelligence and/or a manned security operations center monitoring for malware on your network? Does your organization have anti-malware system beyond firewalls and off-the-shelf software? Can that system offer more predictive and intuitive digital analysis, round-the-clock security center monitoring, and a deeper layer of security?					
☑ **How would you rate your access to professional expertise?** Do you have access to cybersecurity providers with expertise in the kind of protective cyber security systems that will assist your organization? Can they offer professional advice, customized solutions and remediation?					
☑ **Does your technology roadmap include a cybersecurity investment plan?** Do you have a continuous investment plan that allows you to upgrade and refine your protective systems as a normal cost of business?					
☑ **Is your organization culturally committed to cyber security?** How strong are your security controls, including access and usage monitoring? Does security play a part in your overall management processes? Do you have a culture that consists of an informed and committed staff with regular training and testing?					

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