DEFENDIFY

Cyber Insurance Readiness Checklist

The cyber insurance market is rapidly changing, and requirements for obtaining coverage are becoming more stringent. This Cyber Insurance Readiness Checklist includes vital questions to help your organization understand if your cybersecurity program can meet these changing insurance coverage requirements. If you cannot check the boxes of the checklist, Defendify can help set your organization up for success when obtaining cyber insurance coverage, or to reduce the cost of cyber insurance premiums.

- Does your organization perform regular cybersecurity health checkups or risk assessments?
- Do you have a documented and enforced process for regularly updating/patching all organization-owned IT devices? This includes computers, servers, building controls, security cameras, and IoT Devices.
- Do you have a written plan to restore your data from a backup, should you ever need to?
- Do you have an Incident Response Plan, updated annually, that details the steps your organization is to take in the case of a cyber incident?
- Have you reviewed the privacy and security policies from your 3rd party vendors and/or cloud provider(s) to make sure that they meet industry standards?
- Do you allow your employees to work with organization-owned devices outside of the network?
- Do you have behavior-based antivirus software installed on your computers and servers?
- Are employees able to install software of their choice on their organization-owned devices?
- Do you regularly perform cybersecurity awareness training?
- Do you have a password manager available to employees to manage and track their passwords?
- Do you store logs from all networked infrastructure (computers, servers, firewall, VOIP, email)?
- Has your organization ever had a data breach, loss of data, virus/malware attack, or any other security-related incident?

Learn More about Cyber Insurance Readiness

www.defendify.com/cyber-insurance