Can You Qualify For Cyber Insurance?

Cyber insurance is an integral part of a comprehensive IT security program. It reduces your financial loss from cyber incidents, such as breaches, ransomware, and theft. But in today's risk environment, it's not easy to get.

Everything you do to assume more responsibility for protecting your IT environment improves your ability to get cyber insurance — with the coverage you need at a reasonable rate.

First, your IT department should be doing the basics to protect and defend your environment. EDR, or Endpoint Detection and Response, is an example of a security tool that insurance companies require. Then, add greater security by taking further steps to contain and monitor your environment. Finally, consider hiring an external security firm to try to penetrate your network before insurance company experts test for themselves.

Protect and Defend: Perform basic cyber hygiene

The Big Picture:	The Weeds:
Secure what's most important	Maintain an accurate, **up-to-date inventory** of all business systems, applications, and websites so you know what needs to be protected and store your most critical business information on **ransomware-resistant backups**
Keep out unauthorized users	Implement **Multi-Factor Authentication (MFA)**, have unique user accounts for each employee, and enable **concise access controls and permissions** for employees
Keep everything up to date	Apply the most recent **patches and updates** to your systems (not just Windows) as soon as they're available and **replace or retire** hardware and software that has reached end of life
Make your information unreadable to others	**Encrypt your data and devices** to prevent access by unauthorized users who do not have the decryption key
Secure email and mandate Security Awareness Training	Use an **advanced email security platform** to block phishing and malicious attachments, and contract with a reputable **training partner** to train and test your team (including the C-Suite)
Monitor your endpoints for threats	Deploy, customize, and manage an **Endpoint Detection and Response (EDR)** solution to prevent attacks originating in devices connected to your network (including ransomware)
Simplify protection with an all-in-one solution	Use a modern **Unified Threat Management (UTM) system** that protects against a multitude of threats, including viruses, worms, spyware, intrusions, leaks, and network attacks

Contain and Monitor: Up your game to better manage risk

The Big Picture:	The Weeds:
Use proven security standards	Adhere to the **NIST, ISO, or other security standards** that best match your industry/needs and then inform all of your vendors about your selected standards
Minimize exposure in the event of a compromise	Perform **network segmentation** and enforce **firewall policy-based boundaries** within your environment
Make the best use of your available security	Enable the latest **security controls** for your network, cloud platforms, and endpoints to fully leverage their security capabilities
Reduce points of compromise	Conduct **vulnerability scans** to confirm you've treated all known vulnerabilities and **remove, replace, or retire** any technology with untreatable vulnerabilities from your systems even if they're still operable
Improve your ability to spot and respond to events	Use a managed **Security Incident and Event Management (SIEM)** solution that provides consolidated monitoring visibility and use tools that **identify compromised credentials** in advance
Classify all data based on their sensitivity level	Use **data classification** to determine relative risk by category and use follow-up processes and frameworks to keep sensitive data where it belongs
Limit third-party risk and leverage third-party expertise	Require your **third-party vendors** (and their subcontractors) to meet the same security standards you do and get a third-party **Business Impact Analysis (BIA)** to ensure you're protecting what's most important
Put processes in writing and practice for emergencies	Implement a written **Information Security Policy (ISP)** that documents your security activities and update and practice your **Incident Response Plan (IRP) and Disaster Recovery Plan (DRP)** so you're ready to respond and restore quickly

Infrastructure first! To qualify for cyber insurance, your infrastructure needs to support the activities that protect your IT environment. The best plan is to build a strong foundation in anticipation of new technologies, processes, and opportunities — including advanced security tools. Your infrastructure will be ready to support your business continuity and growth.