SecureLink®
an Imprivata company

Does My Business Qualify For Cyber Insurance?

Cyber threats are rising. Bad actors are becoming more sophisticated and taking advantage of the new digital, cloud-based, and decentralized business landscape.

Building a proactive cybersecurity strategy is the best way to defend against an attack. But to protect your company from the physical and financial ramifications of a cyberattack, you need one more weapon in your arsenal—cyber insurance.

WHAT IS CYBER INSURANCE?

Cyber insurance (or cyber liability insurance) is coverage you receive to help offset the costs associated with experiencing a cyberattack. Traditional liability insurance doesn't cover cyber risk, which is why cyber insurance has been an emerging necessity.

WHAT DOES CYBER INSURANCE COVER?

Cyber insurance can cover costs such as:

- Legal fees and expenses
- Recovery of compromised data
- Ransom payment and extortion costs
- Fines and penalties
- Notifying impacted customers of the security breach
- Repairs to damaged and compromised computer systems
- Lost income as a result of downtime or service interruption
- Identity theft and credit monitoring services
- Forensic investigation

To get specific details on what a cyber insurance policy would cover for your organization, consult an insurance agent. But to get that conversation started, you should first know if your business has everything it needs to qualify for cyber insurance.

Cyber insurance protection saved organizations

$240,488

on the average cost of a data breach according to IBM.

Checklist: Does my business qualify for cyber insurance?

The requirements to qualify for cyber insurance are based on what insurers have seen from their customers that have experienced an attack. They see large ransoms, disrupted services, litigation costs, and the security systems that worked (or didn't work).

Consequently, they're expecting more from their customers' cybersecurity strategies. Insurers now require organizations to deploy certain controls to obtain or maintain coverage of cyber liability insurance.

QUALIFICATIONS FOR CYBER INSURANCE

CHECK ALL THAT APPLY TO YOUR ORGANIZATION

SECURITY PRACTICES AND RISK ASSESSMENT

□ Proactive measures are in place to prevent, detect, and respond to ransomware attacks and cyber threats

□ Employee cybersecurity training has been initiated and is in-progress

□ Environment has been reviewed for any signs of compromise

  □ If a sign of compromise was found, it's been remediated

□ Cybersecurity and third-party risk assessments have been conducted

AUTHENTICATION

□ Mutli-factor authentication (at a minimum of two-factor authentication) is deployed for:

  □ All individual users

  □ Business emails

  □ Employee remote access via VPN, desktop sharing, etc.

  □ Third-party vendor remote access via VPN, desktop sharing, third-party management platforms, etc.

  □ Privileged access

ACCESS CONTROL

□ User access is restricted to only what's needed based on job responsibility

□ External users' network access is limited to the application or protocol level

□ Access policies are established for internal and external users

□ Streamline remote access of employees and third-party vendors

□ Administrator access is monitored for unusual behavior

□ Remote access from external sources is secured, controlled, and monitored

□ User access is revoked when an employee leaves the company or when a third-party

CREDENTIAL MANAGEMENT

□ Privileged accounts are managed through a privileged access management system

□ Password management includes password vaulting, rotation/randomizing, masking, and injection

□ Provide cybersecurity awareness and training for employees and external third-party users

□ Create and establish incident response plans and recovery plans in the case of cyber incidents

□ Control and log all instances of remote maintenance

Is Cyber Insurance Worth It?

Cyber insurance is worth the cost if your business stores valuable, sensitive data such as PII. As the number of cyberattacks grows, so does your chance of experiencing a data breach.

Once a data breach happens, there's no going back. Customers, employees, systems, and data are all impacted as soon as a bad actor breaks in. The only way to recover is to address and repair what's been damaged.

Cyber insurance helps repair the financial and reputational damage done by the attack, taking that heavy burden off your organization and allowing you to focus on the most important part of remediation: patching the security gaps that led to the breach in the first place.

About SecureLink

SecureLink, an Imprivata company, is the industry leader in critical access management, empowering organizations to secure access to their most valuable assets, including networks, systems, and data. By leveraging Zero Trust principles, machine learning, and artificial intelligence, SecureLink provides comprehensive security solutions to govern, control, monitor, and audit the most critical and highest risk access points. Organizations across multiple industries -- including healthcare, manufacturing, government, legal, and gaming -- trust SecureLink to secure all forms of critical access, from remote access for third parties to access to critical infrastructure, regulated information, IT, and OT.