Measured
Trust, quantified.

Cyber Insurance Checklist: 12 Essential Security Controls

Sharp increases in ransomware and other malicious cyberattacks are leading more companies to consider purchasing cyber insurance. Forced to pay out larger and more frequent claims, **insurers are hiking premiums while also being more selective about who they will cover.** Underwriters now commonly require organizations to document their cybersecurity practices in order to qualify for coverage. **Most want to see that the following 12 security controls are in place:**

1. Multifactor authentication (MFA)

Ransomware and other attacks frequently exploit weak or stolen passwords to infiltrate systems. MFA reduces the risk by requiring a combination of verification factors such as a password or PIN along with a security token, mobile app or a biometric identifier. It's almost impossible to get cyber insurance without MFA.

2. Endpoint detection and response

Endpoint devices such as laptops, tablets and mobile phones are enticing targets because they provide a direct route into corporate networks. Unlike traditional signature-based threat detection tools, EDR solutions use machine learning (ML) and continuous monitoring to identify stealthy threats that lack the usual signs of an infection.

3. Secure backups

Many ransomware attacks now target backup data to prevent recovery. Immutable backups that cannot be encrypted, deleted or otherwise modified ensure you have an untouched version of data that is always recoverable. For additional protection, the immutable backup should be isolated from local systems.

4. Secure remote access

Remote desktop protocol (RDP) enables users to access company resources from a home PC using an Internet connection, but it has known vulnerabilities. Apply encryption, MFA and other security features to mitigate risk. In addition, block all remote access ports at the firewall or network gateway unless there is a valid business reason for having them open.

5. Vulnerability and patch management

A vulnerability and patch management plan should include a risk-based approach for identifying, prioritizing, patching and testing software and operating systems. This significantly helps limit exposure to ransomware and other exploits.

6. Network access controls

Enforce least privilege access principles to ensure users are limited to only the data and systems access necessary for their jobs. Identity and access management (IAM) and privileged access management (PAM) solutions deliver strong access controls. IAM solutions provide a framework for verifying user identities, while PAM delivers more control over privileged identities and activities.

7. Incident response planning

A formal incident response plan should outline specific procedures for detecting, responding to and recovering from a cyberattack. The plan should describe technical requirements for containing and eradicating threats as well as business requirements for maintaining operations.

8. Cybersecurity awareness training

Regular security awareness training promotes general security best practices and an understanding of social engineering and phishing techniques. Users who can spot the telltale signs of an attack can preemptively thwart many attacks.

9. Monitor event logs

Enable security event logging for all systems, software and endpoint devices, and actively review and analyze those logs to detect attacks and launch countermeasures.

10. Secure/replace end-of-life systems

Hackers commonly target applications and systems that have reached end-of-support or end-of-life because they know security issues are no longer being addressed. Companies with outdated systems and no plan for upgrades are viewed as poor risks by most insurance underwriters.

11. Manage supply chain risk

Supply chain attacks allow cybercriminals to distribute malware to mass numbers of victims simultaneously. Organizations should evaluate their suppliers' security practices and incorporate specific security requirements into their contracts.

12. Filter content

Content filtering solutions scan web applications, identify malware signatures and examine text and email messages to protect against data leakage.