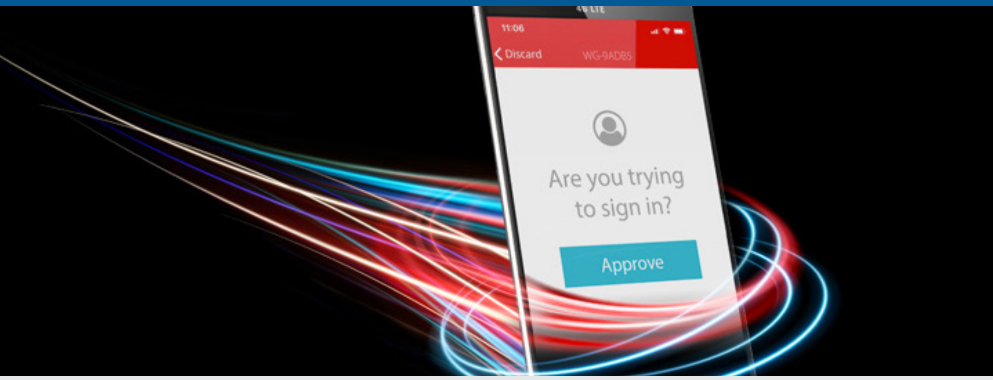
WatchGuard®

BUYERS GUIDE

LBMC TECHNOLOGY SOLUTIONS

A Buyers Guide to Cyber Insurance



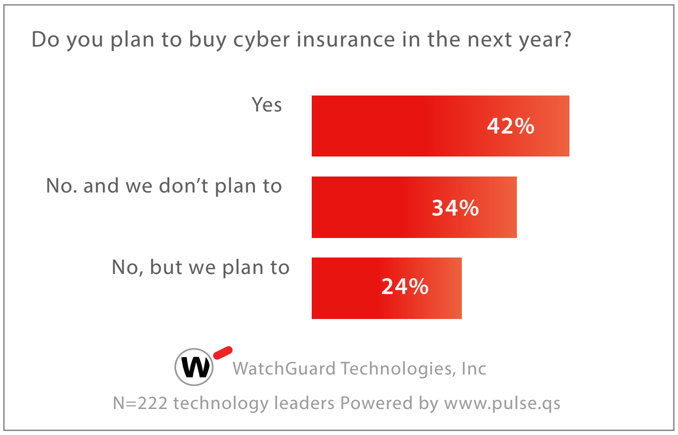
MFA is a must-have if you are looking to purchase cyber insurance for your business.

Recent cybersecurity incidents and ransomware attacks have increased, driving companies to apply for cyber insurance. When doing so, companies have been facing one new pre-requisite to become eligible: multi-factor authentication protection of your users and assets.

How to get started when shopping for cyber insurance

How do you know if you need cyber insurance?

There are many important differences between large and smaller companies when it comes to cyber insurance needs. Smaller businesses are more at risk of successful cyber-attacks than larger ones as they often lack the budget and expertise to implement effective cybersecurity strategies. Large corporations are more likely to be targeted in hacks, so they buy coverage directly from insurers, and have their own legal, public relations, and technology expertise. Small and medium-sized companies are increasingly looking at cyber insurance as another way to mitigate risk. They usually shop through agencies and typically need outside crisis management help.



Find the coverage that works for you

Did you know that general business insurance does not cover cyberattacks? There are different coverages and requirements, depending on what you are looking for. Use this guide to make sure you don't pay high premiums and that you choose the liability policy that will actually respond to your risks and vulnerabilities.

Ensure that your business qualifies for coverage

Underwriters may refuse to cover organizations that don't use multi-factor authentication or specific categories of endpoint protection products. Some insurance providers give precedence to companies with network features that stop attacks from spreading through the system when considering who to underwrite.

What does cyber liability cover?

Unlike general liability insurance, cyber liability policies don't offer all-inclusive coverage.
Most SMB companies that do have cyber insurance only cover liability ($50K), which against a major breach won't be enough. Cyber liability provides financial coverage for expenses related to a data breach. These expenses can accumulate rapidly once a data breach is discovered and reported. Here is a breakdown of what is typically covered:

- ✓ **Customer Loss**
- ✓ **Business Disruption**
- ✓ **Regulatory Fines**
- ✓ **Legal Costs**
- ✓ **Public Relations**
- ✓ **Direct Financial Loss**

Types of Cyber Insurance

Hacksurance: Insurance against cyberattacks and hacking attacks

Theft and fraud: Covers destruction or loss of the policyholder's data as the result of a criminal or fraudulent cyber event, including theft and transfer of funds

Forensic investigation: Covers the legal, technical, or forensic services necessary to assess whether a cyberattack has occurred

Business interruption: Covers lost income and related costs where a policyholder is unable to conduct business due to a cyber event or data loss

Extortion: Provides coverage for the costs associated with the investigation of threats to commit cyberattacks against the policyholder's systems and for payments to extortionists who threaten to obtain and disclose sensitive information

Reputation Insurance: Mitigates against reputation attacks and cyber defamation

Computer data loss and restoration: Covers physical damage to computer-related assets, including the costs of retrieving and restoring data, hardware, software or other information destroyed or damaged as the result of a cyberattack

Cyber Insurance Checklist

No business is excluded from the risk of a cyberattack. If you are considering adding insurance to your security infrastructure, you will likely need to adopt multi-factor authentication to qualify for coverage. Use this checklist to evaluate your existing cybersecurity practices and determine which insurance type is right for you.

Management

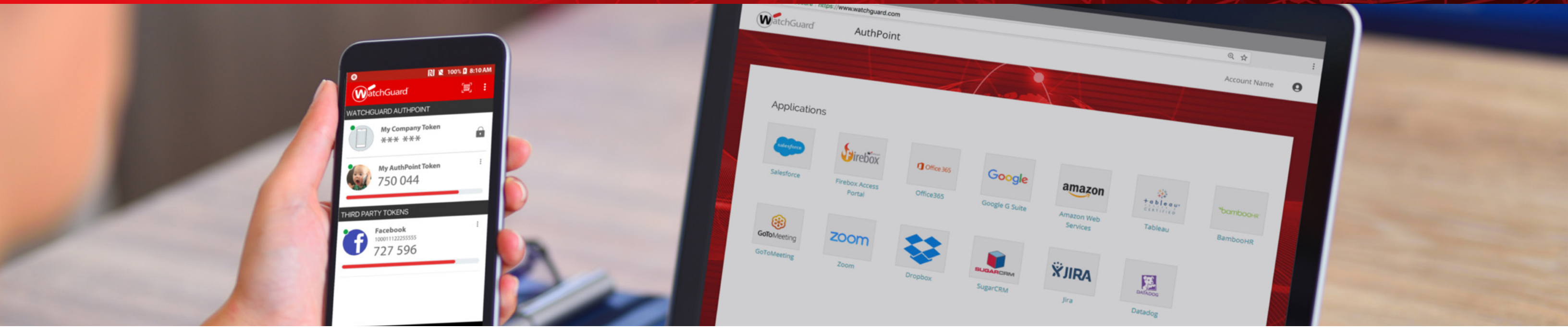
- Do you have the budget to cover implementation costs and policy coverage?
- Do you have an attestation document?
- Have you identified the type of insurance that fits your business?
- Are you educating your staff about cybersecurity best practices?
- Have you identified key vulnerabilities your business is exposed to?
- Are you complying with regulations such as GDPR, HIPAA, and PCI DSS, if they apply to your business?

IT Operations

- Do you have internal IT staff or service providers managing security?
- Are you performing security tests?
- Do all computers have antivirus software?
- Are you scheduling system backups regularly?
- Are you documenting known issues or risks?

Security Controls

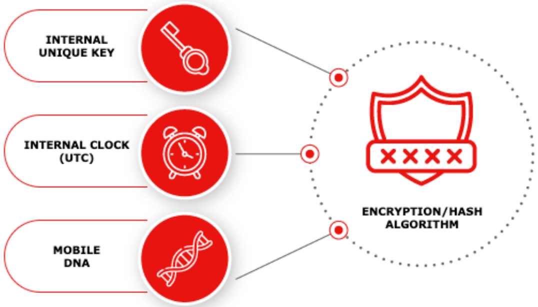
- Is MFA required to ensure secure email access?
- Is MFA required for all remote access to your company network? Are you protecting internal and remote access to network infrastructure components (routers, firewalls)?
- Are you protecting internal and remote access to your company's endpoints and servers?



Qualify for Cyber Insurance with AuthPoint MFA

Effective MFA protection with unique mobile DNA

AuthPoint uses a mobile device DNA to match the authorized user's phone when granting access to systems and applications. Therefore, any attacker who clones a user's device to access a protected system would be blocked – since the device DNA would differ.



AuthPoint protects your business and blocks cyber attacks

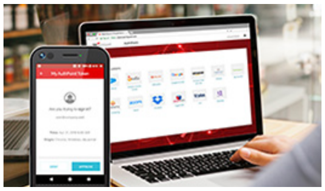
SECURITY IN KEY AREAS	PREVENTION OF MOST COMMON THREATS
User access	User credential hacks
Cloud applications	Phishing
Company networks	Keyloggers
Remote access/VPN	Brute force attacks

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

THE WATCHGUARD UNIFIED SECURITY PLATFORM™

Network Security



Multi-Factor Authentication

Secure Cloud Wi-Fi

Endpoint Security

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis.

Part No. WGCE67528_100821