What Your Cyber Insurer Wants from You

Protecting your organization's data is becoming more complex every year. The number of threats, options for risk mitigation and cost of insurance are all rising exponentially. Here's how to lower your cost and gain more control.

Why are Cyber insurance rates skyrocketing?

The Cyber insurance market has shifted dramatically in the last six months and continues to be a challenge. Cyber insurance policies pay ransoms, and insurers are now paying claims in unprecedented numbers. To course-correct, they now require extensive underwriting to offer renewal terms, and even with this added scrutiny, policyholders should be prepared to see increases in premium, deductibles/retentions, and the possibility of lower limits offered and/or restricted coverage.

How can I keep my Cyber premiums as low as possible?

Increase underwriting scrutiny of organizations' data security practices has executives asking, **"What does my Cyber insurer want from me?"** The answer: bring in the experts. Organizations should invite their in-house or outsourced IT team into the application process which should start at least 90 days ahead of any renewal to:

- Respond to underwriter questions
- Decipher the tech jargon
- Confirm what protections you have in place
- Recommend any improvements or modifications that need to be made

Confidently describing your current processes and providing your Cyber insurer with assurances that you can give them what they want proves that you know your risks and your team is doing all it reasonably can to protect your data.

To be in the best position for your insurance renewal, underwriters are looking for:

Multi-Factor Authentication (MFA)	Secured & Tested Backups	Managed Vulnerabilities	Filtered Emails & Web Content
Patched Systems & Applications	Protected Privileged Accounts	Prepared & Tested Incident Response Plans	Protected Network
Secured Endpoints	Phishing-Aware Workforce	Logged & Monitored Network	Hardened Device Configuration

Your IT team will likely know what all of these terms mean, but just in case, here are descriptions of each method and why they are important to an underwriter:

Risk Mitigation Method	What does it do?	Why is it important?	Sample Remedies
Multi-Factor Authentication (MFA)	Validates or verifies a user's request to access an IT resource, such as an application or website, by requiring the user provide two or more pieces of evidence to be authenticated.	Prevents unauthorized access to your applications and network.	RSA SecureID, Duo, Okta, Ping Identity, LastPass
Secured & Tested Backups	Produces backups of your work and data so it can be recovered in the face of an attack or downtime due to a Cyber incident.	Attackers are looking to delete backups prior to launching a ransomware attack launch so they can successfully extort their victims. It is essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access), as well as regularly test backups and recovery plans.	Cloud Backups With MFA-Controlled Access, Offline Backups, Disaster Recovery Plan (DRP) and tests, Business Continuity Plan (BCP), Integrity Checks
Managed Vulnerabilities	Regular vulnerability scans and annual penetration testing simulate cyber-attacks on the network.	Allows organization to uncover existing vulnerabilities and remediate before threat actors have a chance to exploit them.	Qualys VM, OpenVAS, Tenable Nessus, InsightVM, Frontline Vulnerability Manager, Network Security Tests, Patch & Vulnerability Management Policies
Filtered Emails & Web Content	Filter incoming emails, block malicious sites or downloads, and test suspicious content in a secure "sandbox" environment.	Malicious links and files are still the primary way to insert ransomware, steal passwords, and eventually access critical systems so it is vital to implement filters.	Proofpoint Email Protection Suite, Mimecast Secure Email Gateway, Barracuda Sentinel, FortiMail, Office 365 Advanced Threat Protection
Patched Systems & Applications	A system and process and software to support the patching of systems and applications.	Unpatched vulnerabilities remain a leading cause of intrusions into systems. Hundreds of vulnerabilities are revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit their vulnerabilities.	Microsoft System Center Configuration Manager, Atera, Ivanti
Protected Privileged Accounts	Limiting the number of privileged accounts, using strong password security practices/vaults, MFA, and monitoring these accounts is critical to network security.	Privileged accounts are the keys of a network. When attackers compromise these accounts, the likelihood of causing significant harm is extremely high.	Privileged Access Management (PAM) Solutions (CyberArk Software, BeyondTrust)

Risk Mitigation Method	What does it do?	Why is it important?	Sample Remedies
Prepared & Tested Incident Response Plans	A written and tested Incident Response Plan is vital. Draft plans can be sourced by your broker that are good templates for your particular industry.	When combined with backups and business continuity plans, an Incident Response Plan significantly helps to mitigate the impacts on operations and your organization's reputation, thereby limiting overall costs.	Incident Response (IR) Plan, Tabletop or Incident Simulation Exercises, Breach & Attack Simulation Platforms (XM Cyber), Relationships with IR vendors
Protected Network	Ensure efficient firewall and other technologies are in place with well-defined rules, network segmentation, intrusion detection and prevention systems, and data leak prevention systems.	All breached organizations used firewalls to protect their networks - but the technology is often underutilized or outdated. Having robust settings protects against vulnerabilities.	FortiGate: Next Generation Firewall, Cisco, Firebox, WatchGuard
Secured Endpoints	Advanced anti-malware solutions on workstations, servers, and mobile devices detect malicious programs and contain their spread.	Technology allows organizations to remotely respond to attacks and even prevent data leakage. The time when running a simple 'anti-virus' software was good enough is behind us.	Absolute Software, Cylance, VMware Carbon Black EDR, CrowdStrike Falcon, Windows Defender ATP, FireEye HX. SentinelOne, Symantec ATP
Phishing-Aware Workforce	Training and phishing campaigns help ensure people remain aware and vigilant.	Recently, attackers took advantage of COVID-19 (when people were most stressed) as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people.	KnowBe4, InfoSecIQ, Kaspersky, Proofpoint, Cofense PhishMe, Barracuda PhishLine
Logged & Monitored Network	Automated technology combined with operators monitoring is needed to watch network events or anomalous behavior of users.	Logging and monitoring network activities allows organization to identify something possibly harmful might be happening. Attackers' actions can be detected and contained at an early stage.	LogRythm, IBM QRadar, ArcSight, Gigamon ThreatINSIGHT, Scalar, Trustwave
Hardened Device Configuration	Defining security baselines to harden devices, continuously managing secure configurations and change control processes is essential to preventing attackers from reaching their target.	Attackers exploit default device settings or misconfigurations.	Microsoft Endpoint Manager; Security Baselines (CIS baselines, DoD baselines); Change Management Policies

G2 and its resource partners will work side-by-side with your team to develop an implementation plan for these mitigation methods before your next renewal date. While implementing these methods may result in additional cost to your organization, the cost may be far greater if underwriters are not willing to insure your specific risks.

For more information about how to mitigate Cyber risk or enhance your insurance program, please contact G2 Insurance Services at 415.426.6600 or connect@G2insurance.com.