Qualifying for Cyber Insurance in 2022

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Qualifying for Cyber Insurance in 2022

As cyber insurance premiums continue to climb, insurance providers are getting increasingly selective about who and what they'll cover.

Cyber criminals are only getting better—a fact reflected in their increasingly sophisticated attacks. And with the heightened frequency, scale and impact of these attacks comes higher cybersecurity insurance premiums for many businesses. Many organizations are finding that the cost of cyber insurance has increased dramatically in the past few years.

But premiums aren't the only costs that are rising. The price of admission to even be considered for coverage is going up as well. If a business wants to qualify for cyber insurance, there are several security controls they need to have in place before an insurance company will consider underwriting the policy:

- **Multi-factor authentication**: When it comes to any remote access or accounts with administrative privileges, it is critical that businesses require users identify themselves with something more than just a username and password. The second form of identification needs to be something you are or something you possess.
- **Endpoint Detection and Response (EDR)**: Businesses need to make sure that their employees' devices are protected by second generation anti-virus and anti-malware software. The solutions that only look for a virus' "fingerprint" are no longer considered acceptable.
- **Secured, Encrypted and Tested Backups**: To protect their data, businesses need to ensure that their backups are both encrypted and stored in a secure location. Many of the underwriters are defining "secure" as: the backups are either offline or immutable.
- **Privileged Access Management**: Businesses should make sure that access to highly privileged accounts (including system accounts) are protected and managed using an encrypted password vault.
- **E-mail Filtering and Web Security**: The easiest way to access one's system is to take advantage of human curiosity. Automatically interrogating emails for suspicious content (attachments and links) before the designated recipient has a chance to open them can help reduce the risk of falling for a phishing attack.

These are the five controls that are most important to insurance companies right now. In the coming years however, organizations can expect these additional controls to come into play:

- **Patch Management and Vulnerability Management**: Businesses should make sure they are continuously patching their applications, databases and operating systems timely.
- **Incident Response Plan**: It is critical that organizations have a formalized plan for how to respond if something goes wrong. It is equally important that this plan is periodically tested and modified as needed.
- **Required Cybersecurity Awareness Training**: While technology can help reduce the risk of cyber-attacks, your employees are still the easiest path to compromise. Mandatory security awareness training, with a focus on phishing, for all employees is a critical component of improving your overall cyber security profile.
- **Network Device Hardening Standards**: Organizations should have configuration standards defined to improve the security of network devices by eliminating non-essential services and minimizing vulnerabilities.
- **Login and Active Monitoring of Network Devices**: This is not as simple as monitoring the network traffic that enters and leaves the system. Organizations must also be cognizant of the traffic that flows between their internal network devices. Logs should be aggregated, and analytics should be used to identify and alert management of suspicious activities.
- **Management of End-Of-Life Systems**: When an organization's technology is no longer receiving updates or support services from vendors, the end-of-life systems must either be replaced or isolated from the rest of the network through segmentation.
- **Robust Third-Party Risk Program**: Companies must have protocols in place to assess the controls of vendors that have access to your systems or data.

Going forward, businesses can expect the cyber insurance landscape to remain pricey and more difficult to obtain the desired coverages. Given the cost and frequency of today's cyber-attacks, more companies are looking to outsource some the risks as part of their mitigation strategy. Continuously monitoring and investing in their cybersecurity postures can help organizations improve their chances of obtaining the cyber coverages they desire.

How Can Schneider Downs Help?

Schneider Downs can help your organization to be better prepared. We offer a comprehensive set of information technology security services, including network penetration assessments, network vulnerability assessments, web application security testing and IT security maturity assessments. Our team of network security specialists, application configuration specialists, implementation consultants and certified information system auditors provide a growing slate of services dedicated to keeping organizations secure, including:

- Digital Forensics and Incident Response
- Enterprise Information Security Program Review and Consultation
- External Footprint Analysis Firewall Configuration Review
- Forensic Analysis
- Incident Response Plan Development, Testing and Training
- Indicator of Compromise Assessment
- Information Security Program Maturity Assessments
- Infrastructure Assessments
- Intrusion Prevention/Detection Review
- MS Office 365 Security Assessments
- Penetration Testing
- Phishing Simulation Exercises
- Purple Team Assessments
- Ransomware Security Service
- Recovery and Remediation
- Vulnerability Assessment
- Web Application Penetration Testing

Breached?

Our Incident Response Team is available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident.

Contact Us
cybersecurity@schneiderdowns.com
www.schneiderdowns.com/cybersecurity

Want to be in the know? Subscribe to our bi-weekly cybersecurity newsletter at www.schneiderdowns.com/subscribe.