ARTICLE

Top Ten Network Security Controls That Cyber Underwriters Expect to See

The cyber insurance market continues to be marked by volatility, keeping insureds and underwriters alike on their toes. In early 2021, the market shifted very abruptly, and increasing frequency, severity, and the sophistication of cybercrime pushed cyber underwriters to re-evaluate their approach to pricing, appetite, coverage, and underwriting. Insureds renewing cyber insurance programs in the last 18 months know that underwriters have substantially upped their game when it comes to underwriting cyber risk.

At the beginning of this shift to a hard market, there was a definitive change to more detailed and technical underwriting. There was also inconsistency regarding the network security controls that were considered the most important, but today, the markets are in closer alignment.

Below are the top 10 network security controls that most cyber underwriters expect to see. They will differ based on carrier, individual underwriter, organization size, industry, etc. and are subject to change.

1. Comprehensive Multi-factor Authentication (MFA) plus Strong Password Controls:

MFA (privileged access, remote access, remote cloud-based apps/O365) and strong password controls protect an organization against phishing, social engineering and password brute-force attacks and help prevent logins from attackers exploiting weak or stolen credentials. For many cyber underwriters, this is **the** most important control.

2. Network Segregation and Network Segmentation:

Network Segregation (separation of critical networks from the internet) and Network Segmentation (splitting larger networks into smaller segments) help reduce the risk and potential impact of ransomware attacks and will improve IT professionals' auditing and alerting capabilities, which will assist in identifying cyber threats and responding to them.

3. Strong Data Backup Strategy:

A strong data backup strategy is typically part of a solid Disaster Recovery/Business Continuity Plan. Underwriters want to see daily data backups, backups stored in more than one location, access rights limited to data backups, etc.

4. Disabled Administrative Privileges on Endpoints:

Disabling administrative privileges on endpoints improves security posture. An administrative end-user on an endpoint for even a few minutes can lead to catastrophic data breaches if the endpoint is compromised.

5. Security Awareness Training for Employees:

Security awareness has never been more important. The threat environment is evolving rapidly. Regular and frequent employee training is a must in today's environment.

6. Endpoint Detection and Response (EDR) and Anti-Malware:

EDR provides advanced measures for detecting threats and provides the ability to identify the origin of an attack as well as how it is spreading. Anti-malware is a version of EDR - it scans your system for known malware such as trojans, worms, and ransomware, and upon detecting them, removes them. Underwriters look for both.

7. Sender Policy Framework (SPF):

SPF plays an important role in email authentication. It helps prevent emails from unauthorized senders from hitting an employee's inbox. Underwriters look for this defensive tool.

8. 24/7 Security Operation Center (SOC):

A dedicated SOC acts as the first line of defense against cyber threats. The analysis and threat hunting conducted by SOC teams help prevent attacks from occurring in the first place. SOCs provide increased visibility and control over security systems, enabling the organization to stay ahead of potential attackers. Cyber underwriters view this as a key proactive approach to network security.

9. Security Information Event Management (SIEM) Platform:

SIEM tools collect and aggregate log and event data to help identify and track breaches. They are powerful systems that provide security professionals with insight into what is happening in their IT environment and help track relevant events that have happened in the past.

10. Strong Service Accounts Security in Active Directory:

Assigning service accounts in built-in privileged groups, such as the local Administrators or Domain Admins group, can be risky. Underwriters want service accounts removed from Domain Admin groups.

The implementation of these top 10 network security controls does not represent the full extent of the cyber underwriting process nor will they be the basis for a premium discount. There are a host of additional controls, policies, procedures, and processes that underwriters will be evaluating. But checking these boxes will provide insureds with a solid foundation designed to meet the baseline expectations of cyber underwriters.

Let's Talk

Find out how EPIC Insurance Brokers & Consultants can help your business.

Visit epicbrokers.com →