MITIGATION MEASURES CARRIERS WANT TO SEE

Below are 6 tips for mitigating a cyberattack that will get carriers to take notice when your cyber liability policy is up for renewal.

Strong Overall IT Security Posture, Procedures and Response Capabilities

Carriers are reviewing all of the above against their other insureds (industry agnostic) to ensure best practices are being maintained. A key focus is placed on protecting privileged credentials and access rights.

Deployment of Patches Regularly

As many recent attacks have exploited machines that have not been "patched" with latest versions, carriers are looking to ensure clients are patching their network/devices without unreasonable delay i.e. limited number of hours/days before patch is released.

Multi-Factor Authentication (MFA) & Secure Remote Desktop Protocol

Ideally, carriers would like to see this for all devices connected to the network – domestically and globally. For global risks where MFA is not available, details about measures put into place need to be provided specific to secure remote desktops.

Security Efforts Used to Filter Attacks, Secure Open Ports & Endpoint Security at Workstations

Carriers are closely evaluating the IT filters in place, as well as open-source reviews to ensure open ports are closed/secured. Carriers are looking at endpoint security measures closely.

Disaster Recovery & Continuity Plans

Carriers are looking for these plans to be in place, updated regularly and tested pre-incident. Understanding how long it would take a client to contain an incident will be important.

Phishing & Security Awareness Training

Such training includes traditional education but also "white-hat" attacks on staff to test overall awareness.