U.S. Risk, LLC

CYBER UNDERWRITING: THE RENEWAL PROCESS

With carriers implementing increasingly stringent requirements to renew cyber coverage, there are certain steps that need to be taken to ensure your renewal goes smoothly and favorably. These are the best practices that cyber insurers are looking for from insureds.

Multifactor Authentication (MFA)

How widely is MFA is employed through the organization. Is it used for privileged user accounts, remote access by employees, vendors and independent contractors? Is it used for email, cloud resources, backups? Is remote access required through the entire network? Where is it implemented? How is remote access to systems achieved? If Remote Desktop Protocol (RDP) is not disabled, is MFA required?

End Point Detection and Response (EDR) and Extended Detection and Response (XDR)

Are you using protection solutions? What type? What vendors are used? Are these in place and are they utilized across the entire network?

Vulnerability Scanning

Do you regularly conduct vulnerability scanning? If so, how often? What percentage of your network is covered by the scans?

Network Backups

What types of backups are in operation, how often are they made and where are they located? Do backups require MFA to access? How are these backups stored (on premises, off site, offline, cloud or encrypted)? How often is testing done? Are backups immutable?

Network Segmentation

What critical systems segmentation is in place? What's the process for monitoring and preventing lateral movement? What is the cadence for patching, especially for critical risks? Are EoL and EoS updates in place?

Endpoint Detection

What kind of endpoint protection solution is used? Do you use signature-based antivirus, behavioral based antivirus, advanced EDR?

Privileged Access Management (PAM)

Is PAM in place and what product is being used?

Domain Administrator Assignments

Are these reviewed regularly?

Service Accounts

How many service accounts does the organization have?

Biometrics and Other Privacy Controls Around Data

What policies are in place? GDPR/CCPA/BIPA compliant?

Social Engineering/Phishing/Fraudulent Transfer

Do you conduct employee information security and privacy training? How often?

Security Incident Event Management (SEIM)

Are you using a SEIM? How are security incident alerts monitored and responded to?

Network Monitoring and Security Operations Center

Is monitoring internal or external? Is there 24/7 monitoring of all logs and reports?

Third Party Risk Management

What controls are in place? Do you have a formal vendor checklist? Do you have confirmation that the third-party vendor has E&O or cyber in force? Are vendors required to use MFA to access your networks/systems?

THE BOTTOM LINE

Understanding your organization's total cyber risk can be difficult, but the process can be greatly streamlined when assisted by a trusted insurance expert highly experienced in all the various forms of cybercrime and how to insure them. Preparation is key when it comes to cybercrime prevention and loss controls. Bringing an expert into the process as early as possible can help ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.