Cyber Insurance Readiness Checklist

Streamlining the application and evidence gathering process

The following checklist helps us successfully prepare for your cyber insurance application, maintain the required technical controls, and provide evidence in the event of a claim.

AUTHENTICATION & MFA

- ☐ Multi-factor Authentication (MFA)
  All user email accounts should have MFA enforced
- ☐ Privileged Users
  Verify privileged accounts are separated

WORKSTATIONS & SERVERS

- ☐ Encryption at Rest
  Verify that drives are encrypted with BitLocker on Windows or File vault on Macs
- ☐ Remote Desktop Protocol Disabled
  Verify if RDP is allowed on workstations and servers
- ☐ Endpoint Protection, Anti-Virus, Anti-Malware
  Identify the endpoint protection and AV provider, and whether it is properly installed, activated, and up to date.
- ☐ Domain, Public, Private Firewalls
  Verify all devices have local firewalls enabled
- ☐ Supported Software
  Verify if any software being used has reached end-of-life

EMAIL SECURITY

- ☐ Domains with Email Enabled
  Identify and document the email domain along with verification of DNS Mail Exchange (MX) details, SPF, DKIM and DMARC configurations
- ☐ Advanced Threat Protection
  Identify and confirm the email filtering service, and that it is enabled and properly configured to scan attachments, validate links and prevent phishing.

DOMAIN & WEBSITE SECURITY

- ☐ Website Domains
  Identify the primary corporate domain(s), subdomains and document DNS and expiration dates
- ☐ TLS/SSL Certificates
  Verify if website traffic is encrypted and protected, and document expiration dates

BACKUPS

- ☐ Workstations & Servers with Backups Present
  Identify the cloud provider and verify if recent backups have occurred, are encrypted, and have completed in the last 30 days
- ☐ Test Backups
  Verify if a successful restoration of backup data has been performed in the last 6 months

NETWORK

- ☐ Segmentation
  Verify if the network is segregated between public and trusted networks via properly configured Access Rules and NAT policies

IMPORTANT TERMS

▶ **Failure to Maintain** This clause enables insurance providers to limit coverage if evidence suggests the policyholder's organization is improperly maintained and kept secure with the basic security controls identified in this document.

▶ **Neglected Software Vulnerabilities** Threat actors will often seek to exploit software that is out-of-date or unpatched. Insurance carriers expect the policy-holder to practice proper cyber hygiene and maintain the latest secure versions. They may provide a grace period, but once lapsed, will require co-insurance and progressively reduce the coverage amount if the software is exploited in an incident.

▶ **Safe Harbor Laws** In the wake of an breach, if an organization can prove that they have a cyber security program, and reasonably conform to established standard frameworks such as NIST, ISO 27001, or CIS, these laws can provide an affirmative defense to liability caused by the breach.