Pillar Technology
PARTNERS

CYBER INSURANCE READINESS

CHEAT SHEET

13 controls underwriters look for to obtain or renew cyber insurance policies

1 MULTI-FACTOR AUTHENTICATION

Cover every user in the organization with MFA and activate on personal and social accounts as well

2 BACKUPS SECURED & TESTED

Follow the 3-2-1 rule
3 backups (1 primary, 2 copies); Store the backups on 2 different types of media; Store at least 1 copy offsite)

3 PATCH & VULNERABILITY MANAGEMENT

Run vulnerability scans frequently; Priortize patches based on their risk and exploitability and applied as quickly as practicable.

4 CONFIGURATION MANAGEMENT

Identify, track and maintain Information assets. Baseline configurations so that changes can be identified and investigated.

5 EMAIL & WEB CONTENT SECURITY

Use filtering technology to prevent weaponized content from exposing users this leading tactic.

6 PRIVILEGED ACCOUNT PROTECTION

Protect accounts with elevated access rights with additional mechanisms to ensure that they are not compromised. Store them in a secured platform such as a Privileged Access Management tool.

7 PREPARED & TESTED INCIDENT RESPONSE PLAN

Be ready to respond quickly. Plan your response, train the team, and test frequently.

8 EFFICIENT & EFFECTIVE NETWORK ACCESS CONTROLS

Implement firewalls and network segmentation to prevent attackers from accessing information assets and being able to move laterally in the organization

9 HARDENED DEVICE CONFIGURATION

Harden device configurations against attack using a hardening standard to limit access and services based on the minimum needed to perform their activities.

10 END-USER AWARENESS TRAINING WITH FOCUS ON PHISHING

Train end-users to reduce the likelihood of falling for a scam. End users are a primary target for attackers and phishing is one of the most common methods.

11 ADVANCED ANTI-MALWARE ENDPOINT SOLUTION

Implement an advanced endpoint protection tool that will not only identify malware based on a signature match but also looks for and stops malware based on abnormal activities.

12 SECURITY LOGGING & MONITORING

Implement a SIEM Monitoing platforms to allow early identification of attacks and correlate activites.Keep and maintain logs that are necessary for investigations.

13 PENETRATION & VULNERABILITY TESTING

Test the defenses of the organization by using the same methods and tactics that threat actors use. This helps an organization eliminate vulnerabilities before they are exploited.

For more details, visit www.pillartechnologygpartners.com