RCM&D

A UNISON RISK ADVISORS Company

PREPARING FOR YOUR CYBER RENEWAL

The cyber liability marketplace is currently experiencing a sudden, substantial shift.
In recent years, cyber liability incidents have been increasing in both severity and frequency, with a 73% loss ratio measured in 2020 according to Fitch Ratings. As claims continue to rise, insurance carriers are scrutinizing cybersecurity controls and rigorously underwriting every risk. Implementing measures like multi-factor authentication and maintaining proper cyber hygiene practices are more crucial than ever before to obtaining coverage.

How many boxes does your organization check?

- ☐ Encryption in place for sensitive data while in transit, at rest and for backup media
- ☐ Enforce the use of dedicated accounts for privileged/administrative access (no shared accounts)
- ☐ Multi-Factor Authentication
  - ◯ Remote access for all employees, corporate users and third parties accessing your system
  - ◯ Email access on non-corporate devices or web app
  - ◯ Privileged/administrative access within your network
  - ◯ Core applications
- ☐ Employee security training and awareness (at least monthly)
  - ◯ Phishing-specific simulations/training
- ☐ Email scanning and filtering (Secure Email Gateway + SPF/DMARC best practices implemented)
- ☐ Endpoint detection, response and intrusion detection tools from a leading provider
- ☐ Segregated back-ups (multi-layer) and access control
  - ◯ They should be airgapped from your network
  - ◯ Understand your recovery point objective and recovery time objective
- ☐ Continuous network scanning and patch management (track exceptions)
- ☐ Vulnerability management, penetration and compromise assessments are completed by a third party
- ☐ Ideally, there is no end-of-Life technology. If it exists, we need to know:
  - ◯ Details on the devices/software
  - ◯ Compensating controls/if segmentation exists
  - ◯ Timeframe to sunset the technology