Breckenridge INSURANCE

Problem solvers found here

RISK MANAGEMENT CHECKLIST

- ☑ Multi-Factor Authentication (MFA) – this will be required not just on email or remote access, but an additional layer for accounts with administrator privileges and should include MFA for all systems.
- ☑ Email Filtering:
  - » Tagging of external emails
  - » Multi-layer email filtering
  - » Screening of emails for malicious attachments
  - » Sender Policy Framework (SPF)
  - » Domain Keys Identified Mail (DKIM)
  - » Domain Based message Authentication, Reporting and Conformance (DMARC)
- ☑ Updates/patches to fix vulnerabilities such as Log4J, Solar Winds, etc.
- ☑ Regular updates of MS/Operating System patches and updates
- ☑ Use of Remote Desktop Protocol (RDP) when remote access is allowed
- ☑ Data Encryption
- ☑ Use of Next Generation Antivirus (NGAV)
- ☑ Use of Endpoint Detection and Response (EDR)
- ☑ Use of Privileged Account Management Software (PAM) -i.e. CyberArk, BeyondTrust, etc.
- ☑ Active monitoring of admin accounts for unusual patterns
- ☑ Hardened baseline configuration across servers, laptops, and managed mobile devices
- ☑ Use of a Protective DNS Services (PDNS) – e.g., Zscaler, Quad 9, etc., to block access to known malicious websites
- ☑ Endpoint application isolation and containment technology for all endpoints
- ☑ Security Information and Event Management System (SIEM)
- ☑ Utilization of a Security Operations Center (SOC) that is managed 24/7 (outsourced or inhouse)
- ☑ Use of a Vulnerability Management Tool
- ☑ Regular backups that are encrypted and stored off site/off network
- ☑ Securing/Closing of any open ports