Cyber Liability Insurance

Cisco Partner
https://cs.co/1page

Cyber liability insurance: A policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cyber security issues involving sensitive customer information, such as Social Security numbers, credit card numbers, driver's license numbers and health records.

Common Requirements: *(not all inclusive)*

(Potential Security options)

Multi-Factor Authentication (MFA): *(Duo, CSC)*
- MFA for Remote access, Email, Backups etc.
- MFA for Privileged and Administrative access
- MFA for all RDP connections
- MFA for Backups
- MFA to secure cloud (AWS, Azure, GCP)

Data Backup & Recovery: *(UCS, Cohesity, Umbrella)*
- Regularly scheduled, tested & Encrypted
- Backups free of Malware
- Business continuity DR Plan & IR
- Cloud synching services used

Email Security: *(Secure Email, Duo)*
- Scan for malicious attachments and links
- Sender Policy Framework
- Domain Keys Identified Email (DKIM)
- Domain-based Message Authentication (DMARC)

Endpoint Security: *(Secure Endpoint, Duo)*
- NGAV for all computers, networks & mobile
- EDR tool for monitoring & logging
- Endpoint application isolation and containment
- Macros not enabled by default

Firewall (Edge): *(Secure Firewall, Umbrella etc.)*
- Up to date and active & Event Logging
- RDP not exposed externally
- Intrusion Detection/Prevention (IDS/IPS)
- Data Loss Prevention (DLP)

Internal Security Controls: *(ISE, Duo, VM etc.)*
- Protect sensitive records in cloud
- HIPAA, DEA's EPCS for Healthcare
- PCI-DSS, NIST, ISO GDPR for general Compliance
- Monitor all administrator access
- HW/SW asset management
- No local admin rights for non-IT
- Patching cadence
- No EoL and EoS software used
- Security Operations Center (SOC) used
- Vulnerability Management tool used
- Annual Penetration testing
- Complex passwords required

Vendor Management: *(Partner, ISE, Duo)*
- Logging and monitoring vendor access
- Revocation of access process
- Vendors carry separate polices
- Centrally aggregating and storing security event data

Discovery / Auditor Questions:

- Do you have cyber insurance? Does it cover state-sponsored cyberattacks?
- Does your cyber insurance require a Ransomware Supplemental agreement?
- What is your Incident Response plan and how frequently do you test it?
- How are breaches being reported and what volume have you seen in the past 24 months?
- In the event of a breach, how would you notify your customers?
- How have you defined roles based on access to the network and/or applications?
- How do you protect employee personal devices (BYOD) on your work environment?
- How do you train your employees to not fall victim to social engineering attacks?
- How regularly do you scan your systems for vulnerabilities? Are you able to generate scan reports?
- How frequently are you patching your systems?

Partner Benefits:

- A turn-key, low-friction sales campaign
- New, incremental pipeline
- Increased stickiness with your customers
- Opportunity to sell additional value-added services
- New sales relationships with Cisco and Cisco Secure teams
- Partner-led One Year on Us
- Easy to sell / Seller rewards

Coverage Examples:

- Legal fees & Expenses to meet state and federal regulations
- Notification expenses to affected customers about a breach
- Negotiation and payment of a ransomware demand
- Data restoration & IT forensics
- Setting up a call center & Breach response resources
- Public relations expertise to restore company's reputation
- Credit Monitoring and Identity Restoration
- Lost income from a network outage
- Lawsuits related to customer/employee privacy & security

Insurance Trends:

- Premiums Increasing
- Removal of Coverage for Specific Attacks
- Generally, only covers emergency related costs
- Cyber Insurers exiting the market
- Cybersecurity Insurance Alone is a Threat to an Organization
- Organizations Need a Risk Mitigation Strategy
- Investment in Security Program Maturity
- Some companies are refusing to pay on Ransom demands (if you pay out, it encourages more attacks)

Resources:

- Duo Cyber Insurance Guide
- CTIR Order Guide
- Cisco Security Promotions
- What is Cyber Insurance
- Cyber Insurance Cisco Blogs
- Incident Response Plan
- Talos Blog