Cyber Liability

Guideline to Help Prepare Your Clients

FACTS

- Premiums are increasing between 10% - 300%
- Average Data Breach costs in 2021 are $4.24M
- Average Ransomware costs in 2021 are $1.85M
- Retentions are rising, and coverages are being restricted
- Carriers are having capacity issues resulting in limits being cut
- No guaranteed coverage without strong security controls

BEST PRACTICES

- **Multi-Factor Authentication** – Ability for users to verify their identity before accessing the company systems. It can be implemented for a reasonable fee per employee per month. Vendors include Google Authenticator, LastPass, Duo Security, Ping Identity, and Okta.
- **End-Point Detection & Response** – Tools provided by a third-party provider to monitor computer systems for signs of unusual or malicious activity. Vendors include FireEye, Symantec, RSA, CrowdStrike, and Cynet Security Platform.
- **3-2-1 Backups** - Backup data daily and ongoing. Keep 3 copies of data, 2 copies on different media, 1 copy off-site.
- **Email Security** – Implement email gateways and threat protection to protect against email fraud, phishing, etc.
- **Employee Training** – Teach best practices for avoiding breaches through password updates, phishing exercises, and detecting potential problems to keep the thieves at bay. Employees are still the "weakest link" in the security chain.
- **Incident Response Planning** – Establish a written plan for detection, analysis, containment, and recovery from a cyber incident. Sample plans can be included with cyber policies.
- **Encryption of data** – Prevents use and ability to see data by threat actors; should at a minimum be used for back-ups.
- **Segregation of Networks & Firewalls** – Limits movement within an organization to prevent total infection of a network. A high priority of segregation for end-of-life systems, support systems, and software.
- **Application Permissions** – Company should have a system where only trusted applications can be downloaded and run on network devices.

CSRisks℠
CAPITOL SPECIAL RISKS
Division of Specialty Program Group, LLC

Contact Keanna Dillard
KDillard@csrisks.com | P 770.618.2846 |

Cyber Prep Checklist

- ☐ **Start Early** - Give yourself enough time to talk to all internal parties about the information needed.
- ☐ **Get IT Department Involvement** - Specific data is needed regarding network systems utilized and security measures already in place as well as those being implemented.
- ☐ **Implement Employee Training** - Teach security measures around email, phishing attempts, downloaded files, requests for information, etc.
- ☐ **Secure Network Access** - Implement Multi-Factor Authentication for all users and restrict access for critical network spaces to privileged users.
- ☐ **Confirm Detection Protection** - End-point detection response tools **(EDR)** can alert IT of abnormal or malicious network events. Determine what products are being used internally.
- ☐ **Incident Response Plan** - Ensure you have a plan in place to prepare for, detect, contain and recover from a data breach.
- ☐ **Applications Completed** - Most carriers are requiring supplemental applications (Ransomware, Business Interruption Data Restoration (BIDR), Manufacturing, Biometric Info., etc.) along with the full application and all need to be **FULLY** completed.
- ☐ **Gather Incident Data** - If there has been a breach or other incident, be prepared to provide the following information with the submission.
    - Date of Discovery
    - Details of What Occurred
    - Amount Paid
    - Steps Taken to Prevent Future Incidents
- ☐ **Tell Your Story -** Provide written information regarding the steps being taken to make cyber security better over the next 3 months.

CSRisks℠
CAPITOL SPECIAL RISKS
Division of Specialty Program Group, LLC

Contact Keanna Dillard
KDillard@csrisks.com | P 770.618.2846 |