RISK strategies

CYBER HYGIENE

Mitigate Risk of Ransomware and Other Cybercrime

Before underwriting or renewing cyber coverage, insurers are taking a deep look at each organization's cyber practices. To qualify for coverage — and particularly, if you want the best rates and terms — you need the following resources and procedures in place.

Governance

- Dedicate employees/personnel to IT and cybersecurity (such as hiring a CISO)
- Define roles of each member of the IT and cybersecurity teams

Inventory Management

- Identify, manage, and track all enterprise assets (end-user devices including portable and mobile devices, network devices, non-computing devices, and servers) that are connected to your infrastructure physically, virtually, and remotely, including those within the cloud environment and those not "owned" by IT

To protect what you have, you must first know what you have.

- Manage software assets (i.e., operating systems and applications) on your network proactively, so users can only install and execute authorized software
- Implement procedures to recognize and remove unauthorized and unmanaged software

Endpoint Protection

- Use advanced anti-virus technology with heuristic or behavioral analysis capabilities, in addition to signature-based anti-virus scanning

User/Access Management

- Require multi-factor authentication (MFA) for remote access
- Enforce the principle of least privilege through technology-based restrictions (such as grouping employees together based on roles and granting "need to know" access only)

Insurers **require** MFA, privileged access management, and employee training. Without these critical controls, coverage will be unavailable or limited.

Privileged Access Management

- Put MFA in place for privileged users (employees and vendors with access to sensitive information such as PII or PHI) and service accounts
- Audit logs for all privileged users

Patch Management

- Patch all software and firewalls with critical vulnerabilities within 7 days or less
- Patch software and firewalls with non-critical vulnerabilities within 30 days
- Run vulnerability scans at least quarterly
- Protect un-patchable and end-of-life systems (i.e., through segmentation)

RISK strategies

CYBER HYGIENE
Mitigate Risk of Ransomware and Other Cybercrime

Segmentation

- Segment networks to protect critical information and valued assets
- Implement IT/OT segmentation

Insurance companies are placing more emphasis on IT/OT segmentation for industrial classes of business: manufacturing, utilities, and infrastructure-related operations.

Traffic Filtering

- Utilize sender policy framework (SPF) tool
- Institute both intrusion detection and intrusion prevention tools
- Use tools to monitor and filter email traffic
- Sandbox suspicious emails

Training

- Train employees at least annually in basic cyber security awareness
- Conduct phishing training and simulations at least annually

Best practice: Do phishing simulations continuously throughout the year.

Detection

- Use a SIEM (security information and monitoring) tool
- Perform penetration (or “pen”) testing at least annually

Incident Response

- Develop a comprehensive incident response plan
- Ensure all necessary parties understand the plan and roles
- Conduct tabletop exercises

Business Continuity

- Perform backups on a weekly basis
- Encrypt backups
- Create a business continuity plan, test it annually, and update when necessary
- Store backups offsite and locally
- Implement MFA for backups
- Decide disaster recovery strategy: cold, warm, or hot site

FOR MORE INFORMATION, CONTACT:

Allen Blount
National Cyber & Technology Product Leader
ablount@risk-strategies.com
212-338-4321