Risk Cooperative

INSURANCE INSIGHTS | CYBER 101

Minimum Cybersecurity Checklist

Companies must be proactive in their cyber defense. In the evolving cyber insurance market, carriers assess client risk when they review applications for cyber coverage. The checklist below summarizes six areas for cybersecurity and the minimum standards that underwriters expect. While criteria for optimum rates and coverage is continually being updated, meeting these standards is a first step toward insurability.

Data Security

- ☐ Are automated virus scans being performed on a regular basis?
- ☐ Do you have real-time network monitoring for possible intrusions or abnormalities?
- ☐ Is there a written information security policy in place, with annual employee training and certification?
- ☐ Do you use multi-factor authentication for remote access?

Security Controls & Testing

- ☐ Do you have an Acceptable Use Policy to communicate appropriate use of data to users?
- ☐ Do you conduct the following exercises to test security controls?
  - Internal vulnerability scanning?
  - External vulnerability scanning?
  - Penetration testing?

Business Interruption & Data Recovery

- ☐ Do you have the following plans in place?
  - Disaster Recovery Plan?
  - Business Continuity Plan?
  - Incident Response plan?
- ☐ Have these been tested within the past year?
- ☐ Do you have offsite (e.g. cloud) back-ups less than a month old?
- ☐ Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?
- ☐ Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?

Contact us today to speak with one of our cyber insurance consultants.

info@riskcooperative.com | +1.202.688.3560 | www.riskcooperative.com

Risk Cooperative

INSURANCE INSIGHTS

CYBER 101

Minimum Cybersecurity Checklist

Funds Transfer

- [ ] Does your team have some method of multi-factor authentication before transferring any funds?

Email Security

- [ ] Do you pre-screen e-mails for potentially malicious attachments and links?
- [ ] Do you provide a quarantine service to your users?
- [ ] Can your users access e-mail through a web app on a non-corporate device? If so, do you enforce Multi-Factor Authentication?

Third Party & Vendor Relationships

- [ ] Do your written contracts with third-party providers address care, use, and control of sensitive or confidential information?
- [ ] Do you have a formal assessment of the security risks associated with the new vendor?
- [ ] Do you have a contractual provision to indemnify your firm in the event of a security failure or loss on confidential information?

Cyber insurance can be complicated. Working with a knowledgeable broker ensures you have the right protection in place when a cyber attack occurs.

Contact us today to speak with one of our cyber insurance consultants.

info@riskcooperative.com

+1.202.688.3560

www.riskcooperative.com

Applicants without detailed cyber response plans and cyber risk policies are likely to be denied coverage while those that have demonstrated cybersecurity expertise are likely to obtain more favorable cyber coverage, pricing and limits.

Our companion document **Cyber 101: Sample Technical Specifications** provides additional details about the common questions on cyber insurance applications.