Risk Cooperative

INSURANCE INSIGHTS | CYBER 101

Sample Technical Specifications

In the increasingly challenging cyber insurance market, clients must be prepared to provide detailed descriptions of their cybersecurity programs. The below sections provide key underwriting questions and considerations required to obtain a cyber quote.

Data Security

Sample Question

Do you have the following methods of data security, breach prevention/ detection, and data security risk management in your operations to protect Personally Identifiable Information (PII) and Protected Health Information (PHI) under your control?

Details Requested

- Automated Virus scans of computer system
- Firewalls
    - Firewalls at the perimeter of the network?
    - Firewalls in front of sensitive resources inside the network?
    - Have you configured host-based and network firewalls to disallow inbound connections by default?
- Intrusion detection systems
- Centralized log collection and monitoring
- Proactive vulnerability scanning/penetration testing
- Endpoint Detection monitoring
    - Do you use an endpoint protection (EPP) product across your enterprise?
    - Do you use an endpoint detection and response (EDR) product across your enterprise?
    - Do you use an endpoint application isolation and containment technology?
- Physical controls preventing access to the devices themselves
- Encryption of laptops or mobile devices
- Encryption of network data at rest during file transfers (including backup files stored off-site)
- Password protection for access to network (including all mobile or portable devices)
- Real-time network monitoring for possible intrusions or abnormalities
- Automated patch management program
- System Security Audit (performed annually or more frequently)
- Written information security policy with annual employee training and certification
- Privacy disclosure statement on website
- Computer system and data back-ups on regular basis?
- Use Multi-factor authentication when for remote access?
- Do you use a protective DNS service (e.g. Quad9, OpenDNS or the public sector PDNS)?

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

Sample Technical Specifications

Security Controls

Sample Question

Do you have the following security controls in place?

Details Requested

- A formal risk assessment methodology which includes at least an annual review of organizational risks
- Individual officially designated as a responsible security officer (CISO, CSO, etc ...)
- An Information Security Policy communicating how information is protected by the organization
- An Acceptable Use Policy communicating appropriate use of data to users
- How often is phishing training conducted to all staff (e.g. monthly, quarterly, annually)?
- Do you provide your users with a password manager software?
- Do your users have local admin rights on their laptop / desktop?
- Can users run MS Office Macro enabled documents on their system by default?
- Do you manage privileged accounts using tooling? E.g. CyberArk
- If you have any end of life or end of support software, is it segregated from the rest of the network?
- Do you have a security operations center established, either in-house or outsourced?

Business Interruption and Data Recovery Coverage

Details Requested

- Do you have a formal incident response plan?
- Do you have a formal Business Continuity/Disaster Recovery Plan tested during the past year?
  - What is the expected downtime, in hours, for critical business systems?
- Can you recover all of your business critical data and systems in 10 days?
- Do you have offsite (e.g. cloud) back-ups less than a month old?
- Are your backups encrypted?
- Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?
- Do you use a Cloud syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Yes No Drive) for backups?
- Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?
- Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?

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

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

CYBER 101

Sample Technical Specifications

Funds Transfer

Sample Question

Steps you take to authenticate funds or securities transfer instructions prior to transfer.

Details Requested

- Call the customer or client at a predetermined number
- Send a text message to the customer or client at a predetermined number
- Receipt by the Applicant of a code known only to the customer or client
- Does the Applicant verify all vendor or supplier bank accounts by a direct call to the receiving bank prior to adding the vendor or supplier to the authorized master vendor list?
- When a vendor or supplier requests any changes to its account details (including, but not limited to, bank routing numbers, account numbers, telephone numbers, or contact information), does the Applicant:
    - confirm all requests by a direct call to the vendor or supplier using only a contact number provided by the vendor or supplier before the request was received?
    - send notice of receipt of the request to someone other than the person who sent the request, before making the change (multi-factor authentication)?
    - require review of all requests by a supervisor or next- level approver before any change is made?
- Can funds or securities transfer authority be delegated to anyone verbally or in writing?
- If online banking software is used to perform funds transfer functions, is access to the portal restricted to specific users and terminals?

Email Security

Details Requested

- Do you pre-screen e-mails for potentially malicious attachments and links?
- Do you provide a quarantine service to your users?
- Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user?
- Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails?
- Can your users access e-mail through a web app on a non-corporate device?
    - If Yes: do you enforce Multi-Factor Authentication (MFA)?
- Do you use Office 365 in your organization?
    - If Yes: Do you use the o365 Advanced Threat Protection add-on?

Risk Cooperative

INSURANCE INSIGHTS

CYBER 101

Sample Technical Specifications

Third-Party Relationships

Sample Question

If you collect, input, store, process, or maintain any PII or PHI data, and utilize a third party computer system or network that is maintained off-site...

Details Requested

- Do you enter into written agreement for such third-party services that address care, use, and control of sensitive or confidential information?
- Do the written agreements provide you with indemnification in the event of a breach of such third-party service provider's systems, networks, or other assets?
- Do you require such third parties to provide evidence of network security and privacy liability coverage?

New Vendor Selection

Sample Question

Do you conduct the following for due diligence before engaging a new vendor?

Details Requested

- Formal assessment of the security risks associated with the vendor?
- A means to assess the vendors' security posture such as SAS70, CICA Section 5970, BITS or other?
- Contractual provision to indemnify your firm in the event of a security failure or loss on confidential information?

With cyber attacks growing both in frequency and costs, companies of all sizes must be proactive in their cyber defense.

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.

Insurers are eager to reward proactive mitigation strategies, such as those provided by a Managed Security Service Provider, which reduce claims expenses significantly.