

2022 Cyber Security Insurance Checklist

In today's world, if you don't carry cyber security insurance, you're risking time, money and your organization's reputation. Your lending institutions may require you to have coverage. Government regulations may demand it, and even your IT services provider could insist that you be insured. Still, purchasing a policy isn't as easy as writing a check: Insurers want to know that you're following best security practices before they'll even consider offering you coverage.

As you purchase or renew your policy, here are the types of questions you can expect an insurance company to ask. You may also have to provide additional information for add-on ransomware coverage.



GENERAL SECURITY POLICIES AND PROCEDURES:

- ☐ Do you publish and distribute written policies and procedures regarding computer and information security to your employees? **Yes or No**
- ☐ Do you conduct computer and information security training for every employee who has access to computer systems or sensitive data? **Yes or No**
- ☐ Do you enforce a process for the timely installation of software updates/patches? **Yes or No** (If yes, are critical updates/patches installed within 30 days of release?)
- ☐ Do you restrict user rights on computer systems such that individuals (including third-party service providers) have access only to those areas of the network or information that is necessary for them to perform their duties? **Yes or No**

Which of the following procedures do you employ to test computer security controls?

- Testing / Testing frequency**
 - ☐ Internal vulnerability scanning
 - ___ Continuously
 - ___ Monthly
 - ___ Quarterly
 - ☐ External vulnerability scanning against internet-facing IP addresses
 - ___ Continuously
 - ___ Monthly
 - ___ Quarterly
 - ☐ Penetration testing
 - ___ Quarterly
 - ___ Semi-annually
 - ___ Annually

Do you store data in any of the following environments, and is the stored data encrypted? (Check all that apply.)

- ☐ Laptops (___ Encrypted ___ Not encrypted)
- ☐ Portable media (___ Encrypted ___ Not encrypted)
- ☐ Backup tapes (___ Encrypted ___ Not encrypted)
- ☐ "At rest" within computer databases (___ Encrypted ___ Not encrypted)

Do you outsource any of the following? (Check all that apply and please identify the vendor.)

- ☐ Data center hosting. Vendor: _____
- ☐ Managed security. Vendor: _____
- ☐ Alert log monitoring. Vendor: _____

Do you have centralized log collection and management that allows for review of all access and activity on the network?

- ☐ Yes ☐ No

For how long are logs maintained?

Do you have:

- ☐ A disaster recovery plan? ___ Yes ___ No
Date last tested with full restore: _____
- ☐ A business continuity plan? ___ Yes ___ No
Date last tested: _____
- ☐ An incident response plan for network intrusions and virus incidents? ___ Yes ___ No
Date last tested: _____

If you have a business continuity plan, does the plan contain recovery time objectives for the amount of time within which business processes and continuity must be restored?

- ☐ Yes ☐ No

If yes, what are the current stated and tested recovery time objectives? _____

2022 Cyber Security Insurance Checklist



GENERAL SECURITY POLICIES AND PROCEDURES:

What is your process for backing up data? (Check all that apply.)

- ☐ Full backup
- ☐ Incremental
- ☐ Differential
- ☐ Mirror
- ☐ Replication
- ☐ Other: _____

How often is your data backed up? _____

Where are data backups stored? (Check all that apply.)

- ☐ Onsite
- ☐ Secure offsite
- ☐ Secondary data center
- ☐ Cloud provider i.e. Azure, Amazon AWS, etc.
- ☐ Other: _____

If necessary, how quickly can backed-up data be accessed and restored? _____

ECRIME:

Are all employees who are responsible for dispersing or transmitting funds provided anti-fraud training including detection of social engineering, phishing, business email compromise and other scams on at least an annual basis?

☐ Yes ☐ No

Before processing fund transfer requests from internal sources, do you confirm the instructions via a method other than the original means of the instruction?

☐ Yes ☐ No

Do your procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions?

☐ Yes ☐ No

Do your procedures require review of all requests by a supervisor or next-level approver before processing fund transfer instructions?

☐ Yes ☐ No

When a vendor/supplier requests any change to its account details (including routing numbers, account numbers, phone numbers and contact information) and prior to making any changes, do you:

First confirm all changes requested by the vendor/supplier with a person other than the requestor prior to making any changes?

☐ Yes ☐ No

Confirm requested changes via a method other than the original means of the instruction?

☐ Yes ☐ No

Do your processes and procedures require review of all requests by a supervisor or next-level approver?

☐ Yes ☐ No

TELECOMMUNICATIONS:

Have you established strong alphanumeric passwords for administrative controls of your telecommunications system?

☐ Yes ☐ No

Have you configured your telecommunications system to disable: (Check all that apply.)

- ☐ Remote system administration and internet protocol (IP) access
- ☐ Dialing via remote system access (DISA)

2022 Cyber Security Insurance Checklist



TELECOMMUNICATIONS:

Which of the following procedures do you employ to test computer security controls?

Testing / Frequency of Testing

- ☐ Internal vulnerability scanning
 - ☐ Continuously
 - ☐ Monthly
 - ☐ Quarterly
- ☐ External vulnerability scanning against internet-facing IP addresses
 - ☐ Continuously
 - ☐ Monthly
 - ☐ Quarterly
- ☐ Penetration testing
 - ☐ Continuously
 - ☐ Monthly
 - ☐ Quarterly

EMAIL:

Do you filter/scan incoming emails for malicious attachments and/or links?

☐ Yes ☐ No

Do you strictly enforce SPF on incoming emails?

☐ Yes ☐ No

Guideline: Sender policy framework (SPF) allows you to publish IP addresses that should be trusted for your domain.)

Are external emails tagged to alert your organization's employees that the email originated from outside the organization?

☐ Yes ☐ No

Does your cyber security awareness program include phishing training and testing?

☐ Yes ☐ No

If yes, how often are phishing exercises conducted?

- ☐ Monthly
- ☐ Quarterly
- ☐ Annually

Do you use Office 365 in your organization?

☐ Yes ☐ No

If yes, do you use the o365 Advanced Threat Protection add-on?

☐ Yes ☐ No

Do you enforce multi-factor authentication for all users of Office 365?

☐ Yes ☐ No

RANSOMWARE SUPPLEMENTAL APPLICATION INFORMATION:

Do you use malware protection or endpoint detection and response (EDR) tools?

☐ Yes ☐ No

Guideline: Common EDR tools include Carbon Black Cloud, Cisco AMP, CrowdStrike Falcon, Cylance, Endgame Endpoint Protection, SentinelOne, Windows Defender.

If yes to the above, do you use an external service provider to monitor EDR tools?

☐ Yes ☐ No

Do you use multi-factor authentication to protect privileged user accounts?

☐ Yes ☐ No

Do you use multi-factor authentication for remote access to your organization's network?

☐ Yes ☐ No

2022 Cyber Security Insurance Checklist



RANSOMWARE SUPPLEMENTAL APPLICATION INFORMATION:

Do you have a secure/hardened baseline configuration that is regularly reviewed and updated by someone with security expertise and/or in line with industry standards?

☐ Yes ☐ No

If yes, is this baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?

☐ Yes ☐ No

Do you have established processes for rapidly applying critical security patches across servers, laptops, desktops and managed mobile devices?

☐ Yes ☐ No

Do you route all outbound web requests through a web proxy that monitors for and blocks potentially malicious content?

☐ Yes ☐ No

If yes, which web proxy service do you use (e.g. Websense, Bluecoat)? _____

Do you use a protective DNS service (e.g. DNSFilter, Cisco Umbrella, OpenDNS or the public sector PDNS)?

☐ Yes ☐ No

Do you take regular (at least monthly) backups of key server configurations and data?

☐ Yes ☐ No

Are your backups encrypted?

☐ Yes ☐ No

Are your backups disconnected from and inaccessible through the organization's network?

☐ Yes ☐ No

Do you test the successful restoration and recovery of key server configurations and data from backups?

☐ Yes ☐ No

Do you use credentials unique to backups that are stored separately from other user credentials?

☐ Yes ☐ No



Dealing with cyber security insurance can feel overwhelming. We're here to help you choose the right coverage for your organization and help you prepare for the questions insurers might ask. Contact us today for more information.