

SAMPLE REPORT · FICTIONAL BUSINESS

MFA · EDR · BACKUPS · PATCHING · TRAINING · RESPONSE

Cyber Insurance Readiness Report

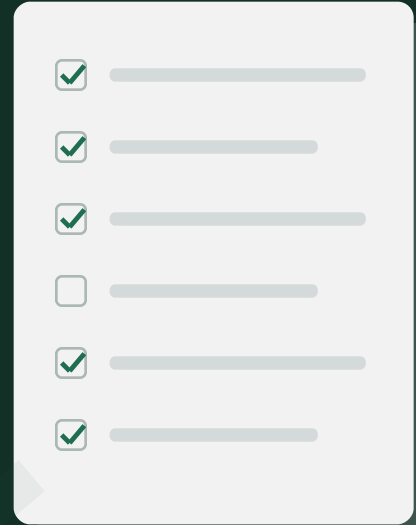
Harbor Point Logistics

Prepared for Jordan Rivera

Completed October 22, 2026 · 11–50 employees · Renewal: 1–3 months

jordan@harborpointlogistics.example

Report ID 8F3A21C4



62

SIGNIFICANT GAPS

READINESS SCORE / 100

CONTENTS

01	Summary	2
02	Gaps ranked by impact	3
03	30/60/90-day plan	6
04	Evidence & agent questions	7
05	Your answers	8
06	Next steps, sources & disclaimer	9

Provided by All Business Technologies. Not affiliated with any insurance carrier, broker or agency.

01 · SUMMARY

Where you stand

Self-assessment of 24 security controls that cyber insurance applications and renewals commonly ask about, grouped into 7 areas.



At a glance

Several controls that applications focus on are missing or unverified. Start with the critical items.

● In place	13
● Partial	6
● Missing or unsure	5

By area

Identity & MFA	86%
Endpoint & Email Defense	44%
Backups & Recovery	63%
Patching & Exposure	33%
Privileged Access	67%
People & Payments	86%
Response, Vendors & Data	57%

2 critical controls are missing or unverified

- EDR on all devices (your answer: No)
- No exposed RDP (your answer: No)

Applications often ask directly about these controls, and answers may be checked after a claim. Answer applications accurately; if something is in progress, say so.

02 · GAPS RANKED BY IMPACT

11 gaps to close

Critical controls first, then by how much weight applications tend to put on each one. Each item is tagged as a quick win, project or documentation task, and as DIY-friendly or typically needing an IT partner.

01 EDR on all devices

CRITICAL

Your answer: No · Endpoint & Email Defense · Often decisive

EDR records what happens on a device and can isolate it, which stops many ransomware attacks before they spread.

- Deploy an EDR product to 100% of laptops, desktops and servers.
- Turn on tamper protection and automatic isolation.

Project

Typically needs an IT partner

Source: CISA #StopRansomware Guide, CIS Controls v8.1

02 No exposed RDP

CRITICAL

Your answer: No · Patching & Exposure · Often decisive

Internet-exposed RDP is scanned constantly and brute-forced.

- Close port 3389 and other admin ports on the firewall.
- Use a VPN with MFA or a zero-trust access gateway instead.

Quick win

Typically needs an IT partner

Source: CISA #StopRansomware Guide, CISA KEV

03 Tested restores

HIGH

Your answer: Not sure · Backups & Recovery · Often decisive

Many organizations find out during an incident that backups were incomplete or too slow to restore.

- Run and document a restore test of a critical server and a sample of files.
- Record how long it took (your real recovery time).

Quick win

Typically needs an IT partner

Source: CISA #StopRansomware Guide, NIST CSF 2.0

04 Timely patching

HIGH

Your answer: No · Patching & Exposure · Often decisive

Unpatched internet-facing systems are a leading way attackers get in.

- Automate OS and third-party patching with reporting.
- Track CISA KEV items and patch internet-facing devices first.

Quick win

Typically needs an IT partner

Source: CISA KEV, CIS Controls v8.1

05 Vendor remote access

HIGH

Your answer: No · Response, Vendors & Data · Commonly asked

A vendor's stolen credentials can be a direct path into your network.

- Give each vendor a named account with MFA; disable it when not in use.
- Review vendor access every quarter.

Project

Typically needs an IT partner

Source: CIS Controls v8.1, FTC Cyber Insurance

06 MFA on remote access

HIGH

Your answer: Partially · Identity & MFA · Often decisive

Attackers scan the internet for VPN and remote desktop logins and try stolen or guessed passwords.

- Require MFA on the VPN and on any remote desktop gateway.
- Put remote-support tools behind MFA and remove unused ones.
- Never expose remote desktop (RDP) directly to the internet.

Quick win

Typically needs an IT partner

Source: CISA #StopRansomware Guide, CISA MFA

07 Advanced email filtering

MEDIUM

Your answer: Partially · Endpoint & Email Defense · Commonly asked

Phishing email is the start of most business email compromise and many ransomware attacks.

- Turn on the advanced protection features of your email platform or add a dedicated email security service.
- Tag external email and warn on lookalike sender domains.

Quick win

DIY-friendly

Source: CISA Cyber Essentials, CIS Controls v8.1

08 Separate admin accounts

MEDIUM

Your answer: Partially · Privileged Access · Commonly asked

Malware runs with the rights of whoever opened it. Without admin rights it does far less damage.

- Remove local admin rights from standard users.
- Give IT staff separate, MFA-protected admin accounts used only for admin tasks.

Quick win

Typically needs an IT partner

Source: CIS Controls v8.1

09 Phishing simulations

MEDIUM

Your answer: Partially · People & Payments · Commonly asked

Simulations measure real behavior and keep awareness fresh.

- Run a phishing simulation at least quarterly and track click and report rates.

Quick win

DIY-friendly

Source: NIST CSF 2.0

10 Encryption of devices & data

MEDIUM

Your answer: Partially · Response, Vendors & Data · Commonly asked

Encrypted devices and data are useless to a thief.

- Turn on BitLocker or FileVault on every laptop and escrow the recovery keys.
- Use encrypted file sharing instead of email attachments for sensitive files.

Quick win

DIY-friendly

Source: CIS Controls v8.1, NIST CSF 2.0

11 SPF, DKIM & DMARC

MEDIUM

Your answer: Partially · Endpoint & Email Defense · Strengthens your application

These DNS records stop criminals from sending email that appears to come from you.

- Publish SPF and DKIM, then DMARC starting at p=none and moving to p=reject.

Quick win

DIY-friendly

Source: CISA Cyber Essentials

Already in place

MFA on email · MFA on admin accounts · MFA on cloud apps · 24/7 monitoring · Offline or immutable backups · Backups cover cloud data · No unsupported systems · Asset inventory · Privileged access controls · Security awareness training · Payment verification · Incident response plan · Prompt offboarding

03 · 30/60/90-DAY PLAN

Your 30/60/90-day plan

Critical gaps and quick wins first, then larger projects, then documentation.

01 First 30 days

Critical gaps and quick wins

6 items

- EDR on all devices**
 Deploy an EDR product to 100% of laptops, desktops and servers. Typically needs an IT partner
- No exposed RDP**
 Close port 3389 and other admin ports on the firewall. Typically needs an IT partner
- Tested restores**
 Run and document a restore test of a critical server and a sample of files. Typically needs an IT partner
- Timely patching**
 Automate OS and third-party patching with reporting. Typically needs an IT partner
- MFA on remote access**
 Require MFA on the VPN and on any remote desktop gateway. Typically needs an IT partner
- Advanced email filtering**
 Turn on the advanced protection features of your email platform or add a dedicated email security service. DIY-friendly

02 Days 31–60

Larger projects

3 items

- Separate admin accounts**
 Remove local admin rights from standard users. Typically needs an IT partner
- Phishing simulations**
 Run a phishing simulation at least quarterly and track click and report rates. DIY-friendly
- Encryption of devices & data**
 Turn on BitLocker or FileVault on every laptop and escrow the recovery keys. DIY-friendly

03 Days 61–90

Documentation and the rest

2 items

- SPF, DKIM & DMARC**
 Publish SPF and DKIM, then DMARC starting at p=none and moving to p=reject. DIY-friendly
- Vendor remote access**
 Give each vendor a named account with MFA; disable it when not in use. Typically needs an IT partner

04 · EVIDENCE & AGENT QUESTIONS

Be ready to back up your answers

Applications may ask you to confirm controls in writing. Keep evidence for each answer, and use the questions below when talking to your agent or broker.

Evidence checklist: 13 of 24 ready

● MFA policy screenshot or admin report showing 100% of users enrolled	READY
● VPN / remote access configuration showing MFA enforced	INCOMPLETE
● List of admin accounts with MFA status	READY
● App inventory with MFA status	READY
● EDR console report showing device coverage	MISSING
● MDR / SOC service agreement	READY
● Email security configuration summary	INCOMPLETE
● DMARC record and grader report	INCOMPLETE
● Backup design showing the immutable/offline copy	READY
● Dated restore-test log with recovery times	MISSING
● Backup scope list	READY
● Patch compliance report	MISSING
● External port scan showing no exposed RDP	MISSING
● Asset list with OS versions	READY
● Asset inventory	READY
● Privileged account list	INCOMPLETE
● Access review record	READY
● Training completion records	READY
● Phishing simulation results	INCOMPLETE
● Written payment verification procedure	READY
● Incident response plan and tabletop notes	READY
● Vendor access list	MISSING
● Encryption status report	INCOMPLETE
● Offboarding checklist	READY

Questions to ask your agent or broker

Questions 1–5 are adapted from the FTC’s cyber insurance guidance for small businesses; 6–7 were added by ABT.

1. Does the policy cover first-party costs (forensics, notification, data recovery, lost income, extortion) and third-party liability?
2. Does it cover attacks on your data held by vendors and other third parties?
3. Will the insurer defend you in a lawsuit or regulatory investigation ("duty to defend")?

4. Does it cover attacks from anywhere in the world?
5. Is there a breach hotline available 24/7, and which response firms must you use?
6. Is social-engineering or funds-transfer fraud covered, and what verification steps does the policy require?
7. What security controls does the application ask you to confirm, and what happens if one is not in place at the time of a claim?

05 · YOUR ANSWERS

Every answer

01	Is multi-factor authentication (MFA) required for every user signing in to company email, including webmail and phones?	YES
02	Is MFA required for all remote access to your network (VPN, remote desktop, remote-support tools)?	PARTIALLY
03	Do all administrator and privileged accounts (domain, cloud, firewall, backup console) require MFA?	YES
04	Is MFA on for your other business cloud apps (accounting, payroll, CRM, banking, file sharing)?	YES
05	Do all computers and servers run endpoint detection and response (EDR), not just traditional antivirus?	NO
06	Are security alerts watched and acted on around the clock (an in-house team or a managed detection and response service)?	YES
07	Is incoming email filtered for phishing, malicious links and attachments (beyond the basic spam filter)?	PARTIALLY
08	Does your email domain have SPF, DKIM and a DMARC policy at quarantine or reject?	PARTIALLY
09	Do you keep at least one backup copy that is offline, air-gapped or immutable (cannot be changed or deleted, even by an admin)?	YES
10	Have you successfully test-restored critical systems and data from backup in the last 12 months?	NOT SURE
11	Do your backups include cloud data such as Microsoft 365 or Google mailboxes, OneDrive/SharePoint or Drive, and line-of-business apps?	YES
12	Are critical security updates applied within 30 days (and actively exploited ones much faster) on all systems?	NO
13	Is remote desktop (RDP) and other admin access closed to the open internet (reachable only through VPN or a secure gateway)?	NO
14	Are all operating systems and key software still supported by the vendor (no end-of-life systems)?	YES
15	Do you keep a current list of your devices, servers and cloud services?	YES
16	Do administrators use separate accounts for admin work, and do everyday users work without local admin rights?	PARTIALLY
17	Are privileged and service-account passwords unique, stored in a vault or password manager, and reviewed at least yearly?	YES
18	Does everyone complete security awareness training at least once a year (and new hires at onboarding)?	YES
19	Do you run simulated phishing tests and follow up with people who click?	PARTIALLY
20	Are new or changed payment instructions (wire, ACH, vendor bank details) verified by calling a known phone number before money moves?	YES
21	Do you have a written incident response plan that names who to call (IT, insurer's breach hotline, legal) and has it been tested in the last year?	YES
22	Is vendor and IT-provider remote access controlled (MFA, named accounts, access only when needed) and reviewed?	NO

- 23 Are laptops encrypted (BitLocker / FileVault) and is sensitive data encrypted at rest and in transit? **PARTIALLY**
- 24 When someone leaves, are their accounts and access removed the same day? **YES**

How the score works: each control is weighted 3 (often decisive), 2 (commonly asked) or 1 (strengthens your application). Yes earns full credit, Partially half, No or Not sure none. If a critical control is No or Not sure, the score is capped at 74. ABT set these weights; insurers use their own criteria.

Want help getting application-ready?

ABT has managed IT and cybersecurity for businesses since 2003. We'll walk through this report with you and help you put the right controls and evidence in place.

Book a free consultation

Call (508) 586-1000

Sources

1. CISA, More than a Password: Multifactor Authentication.
<https://www.cisa.gov/MFA>
2. CISA, Implementing Phishing-Resistant MFA (fact sheet).
<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
3. CISA/MS-ISAC, #StopRansomware Guide.
<https://www.cisa.gov/stopransomware/ransomware-guide>
4. CISA, Known Exploited Vulnerabilities Catalog.
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
5. CISA, Cyber Essentials.
<https://www.cisa.gov/cyber-essentials>
6. NIST Cybersecurity Framework (CSF) 2.0.
<https://www.nist.gov/cyberframework>
7. Center for Internet Security, CIS Critical Security Controls.
<https://www.cisecurity.org/controls>
8. FTC, Cybersecurity for Small Business: Cyber Insurance.
<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance>

Informational only. This is a self-assessment based on your answers; ABT has not verified them. It is not insurance, legal or underwriting advice and does not predict whether any insurer will offer coverage, at what price, or whether a claim will be paid. Requirements vary by insurer and policy; always answer applications accurately and review policy terms with a licensed agent or broker.

Provided by All Business Technologies. Not affiliated with any insurance carrier, broker or agency.