

BOSTON TECH ADVISORS™

COMPLIMENTARY RESOURCE

IT Security Checklist

for Growing Boston Businesses

8 checks. 30 minutes. One honest answer about where you actually stand.

HOW TO USE THIS CHECKLIST

8 checks. Answer yes or no. Add up your score.

Work through each item honestly. Mark it yes only if you can verify it is true today, not if it is planned or partially in place.

Each yes is worth 1 point. Each no is worth 0. There are 8 checks in total, so the highest possible score is 8.

Add up your total, then turn the page to see what your score means and what to do next.

IDENTITY · ENDPOINTS

01 Multi-factor authentication is enabled sitewide

Every account, email, SaaS apps, cloud services, and VPN, requires a second factor beyond a password. Authenticator apps or hardware keys are significantly stronger than SMS codes.

02 All devices are enrolled in a unified management system

Every laptop, desktop, and mobile device used for work is managed through a single platform such as Intune, Jamf, or Kandji. You cannot patch, monitor, or wipe what you cannot see.

03

Former employee accounts are deactivated within 24 hours

Access removal follows a documented same-day offboarding process. **Spot check:** search your identity platform for accounts belonging to anyone who left in the last 6 months.

04

All SaaS applications sit behind a single identity layer

Your team accesses SaaS tools through a centralized identity provider with Single Sign-On. One place to grant access, and one place to revoke it completely when someone leaves.

05 Data backup runs automatically and has been tested recently

Backups run on an automated schedule and the restore process has been tested in the last 6 months. A backup you have never restored is not a backup, it is a hope.

06 Software and systems are patched within 14 days of release

Critical security patches are applied across all devices within two weeks. Unpatched software is the most common entry point for ransomware targeting growing businesses.

PEOPLE · INCIDENT RESPONSE

07 Employees have completed security training in the last 12 months

Phishing is still the most common attack vector. A one-hour annual session covering phishing, password hygiene, and social engineering reduces risk significantly.

08 An incident response plan exists and key staff know it

If something happens tomorrow, who gets called first, who isolates the systems. A one-page plan reviewed annually is dramatically better than no plan at all.

WHAT YOUR SCORE MEANS

7 to 8

Solid foundation

A few gaps remain. Consider a full security assessment to verify your existing controls hold up under real world conditions.

WHAT YOUR SCORE MEANS

4 to 6

Meaningful exposure

Several gaps that compound each other. One incident at this posture would be expensive. A structured review is overdue.

WHAT YOUR SCORE MEANS

0 to 3

Significant risk

Your current setup was not built for today's threat landscape. This is the conversation to have before something forces it.



THE SESSION

What the hour with Ben actually looks like.

No questionnaire beforehand. No deck to sit through. He asks focused questions, listens, and gives you a clear, independent read by the end of the conversation.

This is not a sales pitch.



BOSTON TECH ADVISORS™

Find out where you actually stand.

A complimentary 1-hour session. No pitch, no obligation.

Reserve your complimentary session
bostontechadvisors.com/ceo-session