

EXAMPLE SECURITY PARTNERS

SECURITY READINESS CHECK

37

/100

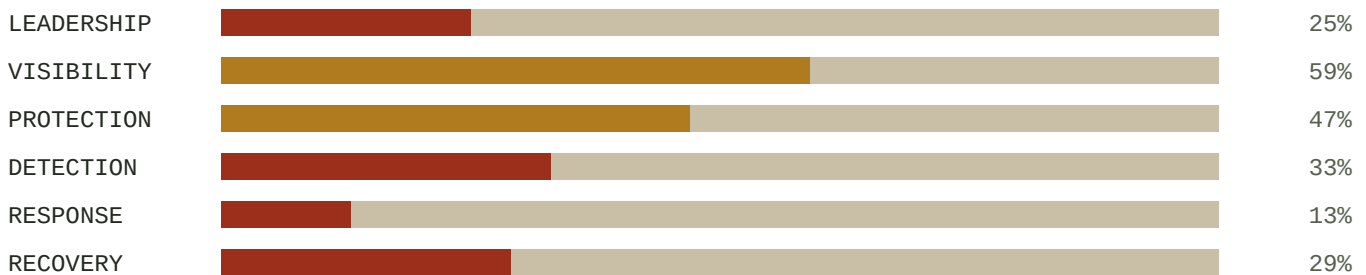
Sample Dental Group (made up) · 1–25 employees · Healthcare
Completed October 16, 2026

AT RISK

AT HIGH RISK FROM COMMON ATTACKS

Several basic protections are missing. The good news: the first fixes below are often quick and low-cost.

YOUR RESULTS BY AREA



YOUR TOP PRIORITIES

1 Stop fake emails in your name

PROTECTION · YOU ANSWERED: NOT SURE

Why it matters: Without it, anyone can send email that looks like it's from your company to your customers and staff.

First step: Ask your email provider to turn these protections on and set them to block fakes.

Guide: FTC: stop fake emails sent in your name

<https://ftc.gov/business-guidance/small-businesses/cybersecurity/email-authentication>

SHOWS UP IN: Cyber insurance applications · Customer security questionnaires · CISA CPG 3.L · NIST CSF: Protect

2 Make vendors tell you about breaches

LEADERSHIP · YOU ANSWERED: NO

Why it matters: If a company you rely on is breached, your information may be exposed too, and you may be the last to know.

First step: Add a "tell us promptly if you're breached" clause to contracts with your most important vendors.

Guide: CISA's essential security goals (CPG 2.0)

<https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0>

SHOWS UP IN: Customer security questionnaires · CISA CPG 1.D · NIST CSF: Govern

3 Get an outside security check

VISIBILITY · YOU ANSWERED: NO

Why it matters: An outside check finds blind spots your own team can miss.

First step: Sign up for CISA's free outside scanning service as a no-cost starting point.

Guide: CISA's free security services

<https://www.cisa.gov/stopransomware/services>

SHOWS UP IN: Customer security questionnaires · CISA CPG 2.C · NIST CSF: Identify

4 Limit admin access and cut off leavers

PROTECTION · YOU ANSWERED: NO

Why it matters: Everyday accounts with too much power, and accounts left open after someone leaves, are easy targets.

First step: Give admins a separate account for admin work, and add "shut off access" to your checklist for departing staff.

Guide: CISA's essential security goals (CPG 2.0)

<https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0>

SHOWS UP IN: Cyber insurance applications · Customer security questionnaires · CISA CPG 3.D / 3.G · NIST CSF: Protect

5 Keep records of important activity

DETECTION · YOU ANSWERED: NO

Why it matters: Without these records, you can't tell what happened, how far it spread, or when it started.

First step: Send your most important records to one central place and confirm how long they're kept.

Guide: CISA's free ransomware guide

<https://www.cisa.gov/stopransomware/ransomware-guide>

SHOWS UP IN: Cyber insurance applications · Customer security questionnaires · CISA CPG 3.Q · NIST CSF: Detect

ANSWER ONCE. USE IT EVERYWHERE.

Your cyber insurer, your biggest customers, and your auditors all ask about the same practices in different words. Most companies treat every questionnaire as a new project. When each practice is documented once, with the proof saved where it already lives, the next questionnaire becomes copy-and-paste instead of a scramble.

8 of your gaps are practices cyber insurers commonly ask about on applications and renewals.

One business day offline: about \$12,308 in revenue; a one-week outage, about \$61,538 before recovery costs.

Answering security questions: about 50 hours (\$2,750) a year. Reusable evidence that halved that time would return about \$1,375 a year.

Rough estimates for discussion, not a guarantee. For scale, IBM's 2025 Cost of a Data Breach Report puts the average U.S. breach at \$10.22 million, an average driven by larger organizations.

YOUR ANSWERS

LEADERSHIP

Is one specific person responsible for your company's cybersecurity?

PARTLY

Do you have written rules for how people use company computers, email, and information?

PARTLY

Do your contracts require key vendors, like your IT provider or software companies, to tell you if they're hacked?

NO

Does leadership talk about cybersecurity risk at least a few times a year?

NO

VISIBILITY

Do you have an up-to-date list of every computer, server, network device, and online service your business uses?

YES

Do you know where your most sensitive information is kept, such as customer, financial, and employee records?

YES

Are updates installed quickly on systems that face the internet, like your firewall, remote access, email, and website?

PARTLY

Has an outside expert checked your security in the last 12 months?

NO

PROTECTION

Do people need a second step to log in, like a code on their phone, for email, remote access, and admin accounts?

PARTLY

Have factory-set passwords been changed on all devices, and does your team use long, unique passwords or a password manager?

PARTLY

Do only a few people have full admin control, and is access shut off the same day someone leaves?

NO

Does everyone get cybersecurity training at least once a year?

YES

Is your company email set up to stop criminals from sending fake emails that look like they come from you?

NOT SURE

Is a copy of your backups kept separate from your network, where a hacker couldn't reach or delete it?

YES

DETECTION

Are records of important activity, like logins, firewall, and email activity, saved in one place and kept for at least 90 days?

NO

If someone keeps failing to log in, or something suspicious happens, does a real person get alerted and act on it?

NO

Does every computer and server have security software that someone actively watches?

YES

RESPONSE

Do you have a written plan for what to do if you're hacked, including who does what and who to call?

NO

Have you practiced that plan in the last 12 months, like a fire drill?

NO

Do you know who to call if you're hacked: your lawyer, your cyber insurance company, a response firm, and law enforcement?

PARTLY

RECOVERY

In the last 12 months, have you actually restored an important system from backup to prove it works?

NO

Have you decided which systems to bring back first, and how quickly, after an outage?

PARTLY

Do you have a plan for what to tell customers, employees, and partners during an outage or breach?

PARTLY

WANT TO TALK THROUGH YOUR RESULTS?

This report is yours. We don't keep a copy of your results, so save it and bring it to a free 30-minute conversation. I'll tell you, in plain language, what I'd do first. Alex Sample, CISSP — Security leadership for growing businesses.

hello@example.com example.com