Security self-assessment summary

Quick check for Harbor Dental Group (a fictional example), completed September 1, 2026

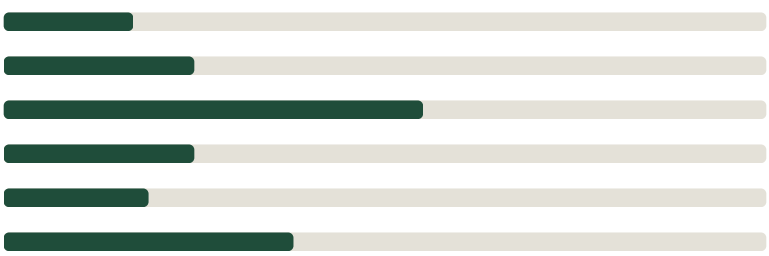
Developing

30% self-reported security practices score

Some good practices exist, but they're informal or patchy. Writing them down and making them routine is the next step.

Based on 22 of 22 questions answered, 2 not sure. Reflects your own answers about your security practices: not a measurement of how protected you are, and not an audit.

Score by area



Your top 5 priorities

1. **Name an owner for cybersecurity, give them the time and budget to do it, and make leadership accountable.**
   High impact · Quick win · Owner: Leadership
2. **Turn on multi-factor authentication, end shared accounts, and review who has access to what every few months.**
   High impact · Quick win · Owner: IT lead or IT provider
3. **Name an incident lead, agree how to rate incident severity, and know who to call for outside help.**
   Medium impact · Quick win · Owner: Cybersecurity owner, with leadership
4. **Send security alerts to a named person or provider, and agree clear rules for when an alert becomes an incident.**
   Medium impact · Quick win · Owner: IT lead, IT provider, or security monitoring service
5. **List who you'd have to notify after a breach, such as customers, partners, and regulators, and the deadline for each.**
   Medium impact · Quick win · Owner: Leadership, with legal or compliance advice

Details, first steps, and the reasoning for each priority follow on page 2.

Your top 5 priorities in detail

Ranked by how much each gap matters, not just by your lowest answers: the most common ways attackers get in and the hardest damage to recover from come first, and quick wins get a nudge up.

1 Name an owner for cybersecurity, give them the time and budget to do it, and make leadership accountable.

Govern · Who's responsible. You answered "Sometimes" to: Is it clear who is responsible for cybersecurity, do they have the time and budget to do it, and do leaders take ownership?

High impact · Quick win (days, not weeks) · Owner: Leadership

Missing, time and budget: Agree how much of the owner's time and budget goes to cybersecurity, and review it every year.

Missing, leadership ownership: Have leadership formally own cybersecurity risk, with a short update from the owner at least every quarter.

Already in place: a named owner.

Why it matters: When nobody clearly owns cybersecurity, important work falls between the cracks and nobody has the authority or budget to fix what's found. Most of the other recommendations depend on having an owner.

Why it ranks here: Most other improvements need someone accountable for them, so a missing owner holds everything else back.

Your note: Our office manager handles IT alongside everything else.

NIST GV.RR: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated

2 Turn on multi-factor authentication, end shared accounts, and review who has access to what every few months.

Protect · Logins and access. You answered "Sometimes" to: Does everyone have their own login, is multi-factor authentication used, and do people only get the access they need?

High impact · Quick win (days, not weeks) · Owner: IT lead or IT provider

Missing, multi-factor authentication: Turn on multi-factor authentication for email, remote access, and admin accounts first, then everything else that supports it.

Not sure: only the access people need. Worth finding out.

Already in place: individual logins.

Why it matters: Stolen and guessed passwords are among the most common ways attackers get in. Multi-factor authentication blocks most of these attacks, and removing shared accounts and old access limits the damage when one account is compromised.

Why it ranks here: Weak logins are one of the most common ways attackers get in, and multi-factor authentication is one of the cheapest, most effective fixes.

Your note: Everyone has their own login. Multi-factor authentication is on for email, but not for the practice-management system.

NIST PR.AA: Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access

3 Name an incident lead, agree how to rate incident severity, and know who to call for outside help.

Respond · Managing incidents. You answered "No" to: When a security incident happens, is there a plan that says who leads, how serious it is, and when to escalate?

Medium impact · Quick win (days, not weeks) · Owner: Cybersecurity owner, with leadership

Why it matters: In the first hours of an incident, confusion about who's in charge and who to call costs time and money. A short plan gets the right people moving fast.

First step: Write a one-page plan naming who leads during an incident, who they call (IT provider, insurer, lawyer), and how to reach them out of hours.

Why it ranks here: A one-page plan is quick to write and saves critical time when something goes wrong.

Works best after: Who's responsible

NIST RS.MA: Responses to detected cybersecurity incidents are managed

4 Send security alerts to a named person or provider, and agree clear rules for when an alert becomes an incident.

Detect · Spotting warning signs. You answered "Not sure" to: When something unusual happens on your systems, does someone review it and decide whether it's a real incident?

Medium impact · Quick win (days, not weeks) · Owner: IT lead, IT provider, or security monitoring service

Why it matters: Security tools raise alerts, but alerts nobody reads don't stop anything. Attackers often go unnoticed for weeks when warnings aren't reviewed.

First step: Find out where security alerts from your email, antivirus, and firewall go today, and make sure a named person or provider reviews them.

Why it ranks here: Spotting an attack early greatly reduces the damage it can do.

Works best after: Monitoring

Your note: Our IT provider may watch for alerts. Need to ask them.

NIST DE.AE: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents

5 List who you'd have to notify after a breach, such as customers, partners, and regulators, and the deadline for each.

Respond · Telling people. You answered "Sometimes" to: Do you know who you must notify during an incident, such as customers, partners, regulators, or police, and how?

Medium impact · Quick win (days, not weeks) · Owner: Leadership, with legal or compliance advice

Why it matters: Many laws and contracts set strict deadlines for reporting a breach, sometimes within 72 hours. Missing them can bring fines and damage trust more than the breach itself.

First step: List everyone you'd have to notify after a data breach (regulators, customers, partners, insurer) with the deadline for each, and keep it with your incident plan.

Why it ranks here: Notification deadlines are short and legally binding, and missing them adds cost to an already bad situation.

Works best after: Your mission and obligations

NIST RS.CO: Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies

Reading your score

“Not sure” counts as 0 points, because a practice nobody can confirm can't be relied on when something goes wrong. Finding out often raises your score.

Score by topic

Govern	
Your mission and obligations	50%
Your approach to risk	25%
Who's responsible	25%
Security policy	0%
Checking it's working	0%
Suppliers and partners	0%
Identify	
Knowing what you have	50%
Understanding your risks	25%
Learning and improving	0%
Protect	
Logins and access	25%
Staff training	25%
Protecting data and backups	75%
Keeping systems up to date	75%
Resilient networks and equipment	75%
Detect	
Spotting warning signs	0%
Monitoring	50%
Respond	
Managing incidents	0%
Investigating incidents	0%
Telling people	25%
Containing incidents	50%
Recover	
Restoring systems	50%
Recovery updates	25%

Things to find out (4)

You weren't sure about these. Questions to ask your IT provider, or whoever manages each area, and what to ask them to show you.

Logins and access

– Do people only have the access their job needs, checked at least once a year?

Spotting warning signs

– Who receives security alerts from our email, antivirus, and firewall?

– How quickly are alerts reviewed, including nights and weekends?

– Who decides when an alert is a real incident, and who do they escalate to?

Ask to see: Where alerts are sent, the agreed response times, and a recent example of an alert being handled.

Suppliers and partners

– Which suppliers hold our data or can access our systems?

– Do their contracts say anything about security or telling us about a breach?

Ask to see: A supplier list, and the security or breach-notification clauses in key contracts.

Knowing what you have

– Do you know where your important or sensitive data is kept?

Other things to improve (14)

Every other answer of “Written down” or lower, highest priority first.

List your suppliers, rank them by access and importance, and add security requirements to contracts with the critical ones.

Govern · Suppliers and partners. You answered “Not sure” to: Do you know which suppliers could hurt you if they were hacked, and do your contracts set security expectations for them?

Medium impact · Short project (a few weeks) · Owner: Operations or whoever manages vendors, with the cybersecurity owner

Missing, checking suppliers' security: Ask critical suppliers for evidence of their security, such as a certification or a completed questionnaire, before signing and at renewal.

Not sure: security terms in contracts. Worth finding out.

Already in place: knowing your critical suppliers.

Works best after: Knowing what you have

Your note: Our practice-management software vendor holds patient records. Not sure what our contract says about security.

NIST GV.SC: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

---

Scan regularly for weaknesses, track what you find, and fix the most likely and most damaging first.

Identify · Understanding your risks. You answered “Sometimes” to: Do you regularly look for weaknesses in your systems and work out which ones could cause the most harm?

Medium impact · Ongoing routine (a regular habit to keep up) · Owner: IT lead or IT provider

Works best after: Knowing what you have

NIST ID.RA: The cybersecurity risk to the organization, assets, and individuals is understood by the organization

---

Give all staff short yearly security training, including how to spot and report phishing, plus extra for sensitive roles.

Protect · Staff training. You answered “Sometimes” to: Do all staff get regular security awareness training, with extra training for people in sensitive roles?

Medium impact · Ongoing routine (a regular habit to keep up) · Owner: Cybersecurity owner, with HR or office management

NIST PR.AT: The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks

---

Write a short security policy, have leadership approve it, share it with staff, and review it every year.

Govern · Security policy. You answered “No” to: Do you have a written security policy that staff know about, and is it kept up to date?

Foundational · Short project (a few weeks) · Owner: Cybersecurity owner, approved by leadership

Works best after: Who's responsible

NIST GV.PO: Organizational cybersecurity policy is established, communicated, and enforced

---

Pick a few security measures to report to leadership regularly, and review your approach after any incident.

Govern · Checking it's working. You answered “No” to: Do leaders regularly review whether your security approach is working, and change course when it isn't?

Foundational · Ongoing routine (a regular habit to keep up) · Owner: Leadership

Works best after: Who's responsible

NIST GV.OV: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy

Write an incident response plan, practice it with a tabletop exercise, and update it with what you learn.

Identify · Learning and improving. You answered “No” to: Do you have an incident response plan, and do you learn from tests, reviews, and past problems to improve?

Foundational · Ongoing routine (a regular habit to keep up) · Owner: Cybersecurity owner

Works best after: Managing incidents

Your note: No written plan. If something happened we'd call our IT provider and hope.

NIST ID.IM: Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions

During incidents, keep a written timeline and preserve logs and evidence, then find and fix the root cause.

Respond · Investigating incidents. You answered “No” to: After an incident, do you work out what happened and why, and keep careful records and evidence?

Foundational · Short project (a few weeks) · Owner: IT lead or IT provider

Works best after: Managing incidents

NIST RS.AN: Investigations are conducted to ensure effective response and support forensics and recovery activities

Write down your most critical services, what they depend on, and which laws and contracts set security requirements for you.

Govern · Your mission and obligations. You answered “Written down” to: Do you know what your organization depends on most, and which laws, regulations, and contracts set security requirements for you?

Medium impact · Quick win (days, not weeks) · Owner: Leadership, with whoever runs IT

Your note: We have a list of key systems and know HIPAA applies, but the list hasn't been updated in two years.

NIST GV.OC: The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood

Make sure someone can quickly isolate infected devices and disable compromised accounts, day or night.

Respond · Containing incidents. You answered “Written down” to: Can you quickly stop an incident from spreading and fully remove the cause?

Medium impact · Quick win (days, not weeks) · Owner: IT lead or IT provider

Works best after: Managing incidents

NIST RS.MI: Activities are performed to prevent expansion of an event and mitigate its effects

Build an inventory of your devices, software, cloud services, and sensitive data, and keep it current.

Identify · Knowing what you have. You answered “Written down” to: Do you keep an up-to-date list of your devices, software, online services, and important data?

Medium impact · Short project (a few weeks) · Owner: IT lead or IT provider

Missing, a software and services list: List the software and online services you use, including free ones, and who manages each.

Not sure: knowing where important data is. Worth finding out.

Already in place: a device list.

NIST ID.AM: Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy

Use tools that watch for malware and suspicious logins on your computers, network, and email.

Detect · Monitoring. You answered “Written down” to: Do you monitor your networks, computers, accounts, and buildings for signs of trouble?

Medium impact · Short project (a few weeks) · Owner: IT lead or IT provider

Works best after: Knowing what you have

NIST DE.CM: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events

Write down the order to restore critical systems, and check backups are clean before restoring from them.

Recover · Restoring systems. You answered “Written down” to: After an incident, can you restore your most important systems from clean backups, in the right order, and confirm they're safe?

Medium impact · Short project (a few weeks) · Owner: IT lead or IT provider

NIST RC.RP: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents

Plan how you'll update leadership and the public during recovery, and decide who approves public statements.

Recover · Recovery updates. You answered “Sometimes” to: During recovery, do you keep leadership, affected partners, and the public informed with approved messages?

Foundational · Quick win (days, not weeks) · Owner: Leadership

Works best after: Telling people

NIST RC.CO: Restoration activities are coordinated with internal and external parties

Agree security goals with leadership and start a simple risk list that ranks each risk by likelihood and impact.

Govern · Your approach to risk. You answered “Sometimes” to: Have your leaders agreed how much cyber risk the organization is willing to accept, and how risks get compared and prioritized?

Foundational · Short project (a few weeks) · Owner: Leadership

Works best after: Your mission and obligations

NIST GV.RM: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions

How your score is worked out

Each answer is worth 0 to 4 points: No 0, Sometimes 1, Written down 2, Routine 3, Improving 4. “Not sure” counts as 0 and “Doesn't apply” is left out. Each area is the average of its topics; the overall result averages the six areas equally. Levels: Just starting (0%+), Developing (20%+), Established (40%+), Strong (60%+), Leading (80%+). The five levels are dollop technology's scoring model for this self-assessment. They aren't NIST's four CSF Tiers, which describe how rigorously an organization governs and manages cybersecurity risk. Method: questions 2026-09-28, scoring 2026-09-24.

This is a self-assessment based on your own answers, not an audit, professional advice, or an official NIST certification, and it doesn't guarantee your organization is secure. The NIST Cybersecurity Framework is owned and maintained by NIST; this tool is independent and not endorsed by NIST. Official framework: nist.gov/cyberframework

dollop technology

This self-assessment is provided free by dollop technology: fractional CISO and IT leadership, based in San Francisco and working with teams everywhere. Engagements are led by Robert Burns, CISSP, CISM, a security and technology executive with more than 20 years of experience building and running IT and security programs. We work with healthcare organizations, nonprofits, digital agencies, and companies going through M&A.

Request a free 20-minute results review: csf.dollop.com/contact · www.dollop.com