Security self-assessment summary

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

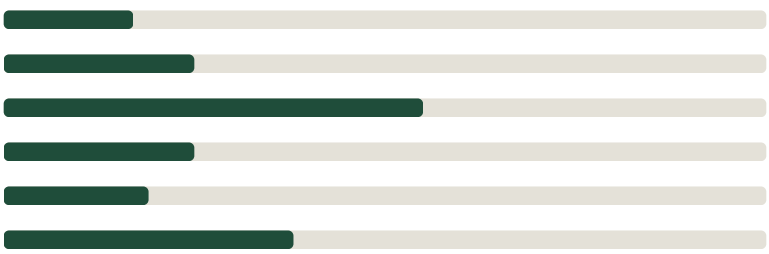
Developing

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

This is the one-page summary. The full report adds first steps and the reasoning for each priority.

Want a second opinion on your results?
Free 20-minute results review with dollop technology, led by Robert Burns (CISSP, CISM).

csf.dollop.com/contact