

EXAMPLE SECURITY PARTNERS

BOARD BRIEFING

Cybersecurity Baseline Assessment

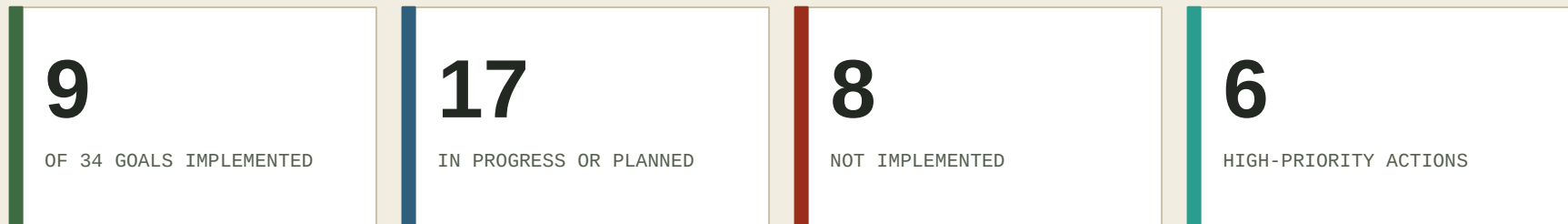
Measured against CISA's Cybersecurity Performance Goals 2.0

Sample Dental Group (made up)

October 16, 2026 · Presented by Alex Sample, CISSP

THE BOTTOM LINE

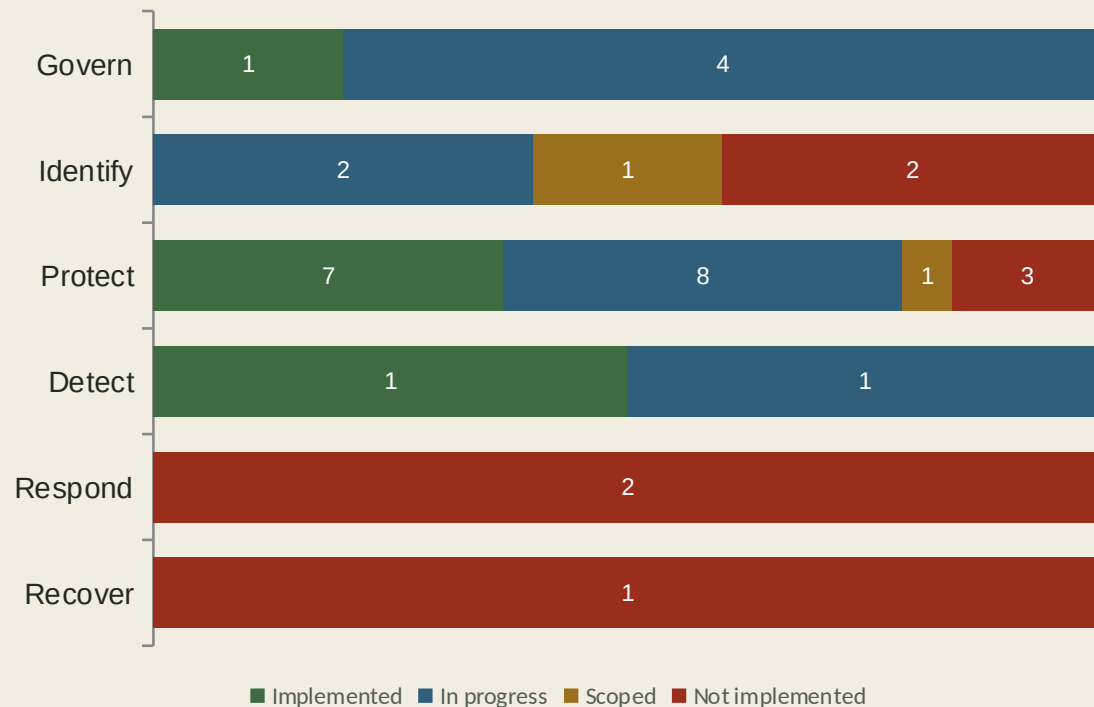
26% of essential security practices are in place



The basics most often tied to HIPAA are in place: a signed policy, training for every staff member, encrypted devices, separate admin accounts and tested backups. The gaps are the controls that stop an email takeover or ransomware from spreading: MFA is incomplete, the network is flat, logs are not collected, and the incident plan has never been approved or rehearsed.

WHERE WE STAND

Results by security function



WHAT STANDS OUT

Protect and Detect are the strongest functions, and Identify, Respond and Recover the weakest. Most gaps can be closed by the IT provider within its current agreement; network separation and log collection are the only items that need new spending.

TOP PRIORITIES

Five actions that reduce the most risk

1

Finish and approve the incident response plan, with the insurer's breach line and the HHS notice steps, and...

1.C Manage Incident Response Plans

HIGH

30 days

2

Give each staff member their own imaging login and retire the shared accounts.

3.C Create Unique Credentials

HIGH

30 days

3

Turn on Microsoft 365 risky sign-in and failed-login alerts and send them to the IT provider and the...

3.E Monitor Unsuccessful (Automated) Login Attempts

HIGH

30 days

4

Enforce MFA on every mailbox and on the remote-support tool this month; use number matching or security keys.

3.F Implement Multi-factor Authentication

HIGH

30 days

5

Limit the scanned-forms share to the front desk and office manager, and move forms into the PMS where...

3.K Utilize Strong Encryption

HIGH

30 days

THE PLAN

90 days to a stronger baseline

DAYS 0–30

Quick wins · 6 actions

- Finish and approve the incident response plan, with the insurer's...
- Give each staff member their own imaging login and retire the shared...
- Turn on Microsoft 365 risky sign-in and failed-login alerts and send...
- Enforce MFA on every mailbox and on the remote-support tool this...
- Limit the scanned-forms share to the front desk and office manager,...

+ 1 more in the full report

DAYS 31–60

Foundations · 16 actions

- Set a yearly policy review date and add a 15-minute security update...
- Add a 72-hour security incident notice term to the IT provider's...
- At renewal, ask the IT provider to confirm MFA on its remote-support...
- Have the IT provider reconcile the device list each month and add...
- Update the firewall now, then run a quarterly external vulnerability...

+ 11 more in the full report

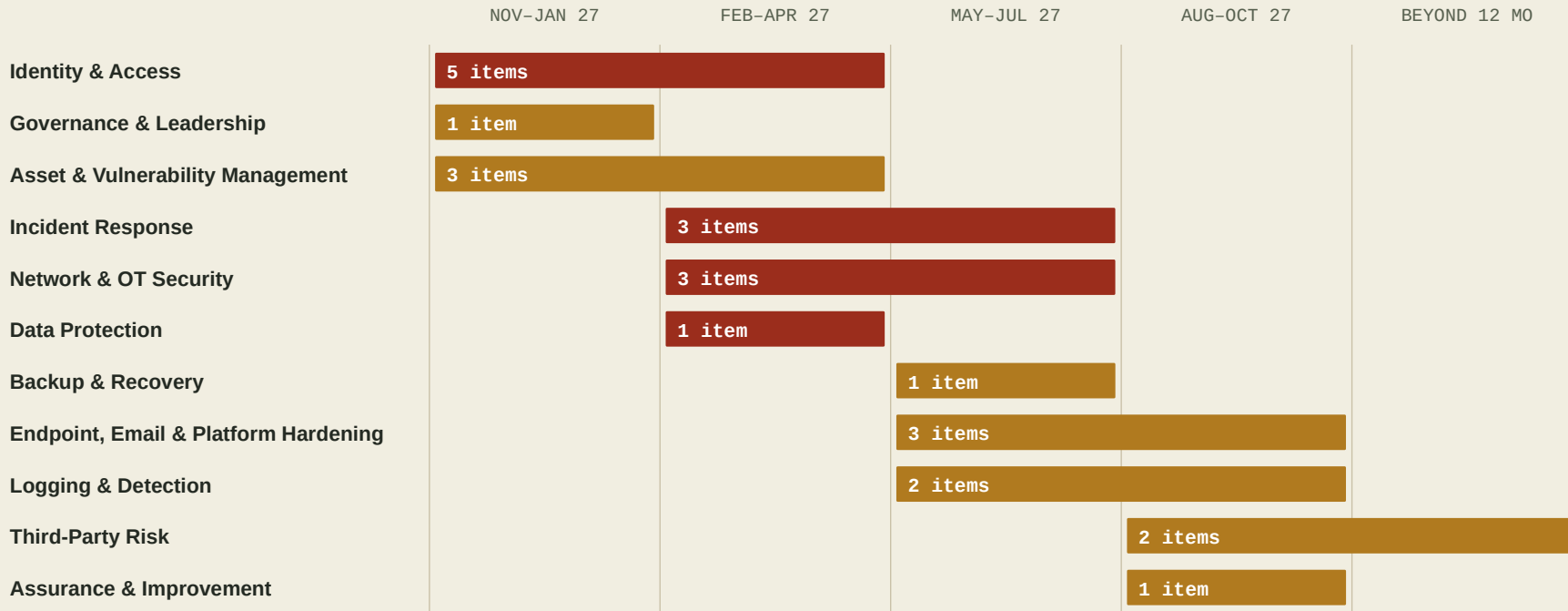
DAYS 61–90

Maturity · 3 actions

- Separate the imaging server and devices, staff PCs and phones onto...
- Publish a security contact and a security.txt file when the website...
- Raise the minimum to 16 characters at the next password change and...

THE ROADMAP

Twelve months, sequenced by priority



DECISIONS REQUESTED

What we need from the board

1

Endorse the 90-day plan

Confirm owners and dates for the 25 actions in the report.

2

Resource the quick wins

Most Days 0–30 actions need staff time more than new spending.

3

Set a reporting cadence

A short progress update to the board each quarter.

4

Schedule a reassessment

Measure progress against the same goals in six months.

ASSESSOR'S RECOMMENDATION

Approve about \$14,000 over 12 months for network separation, log collection and an outside test, and ask the IT provider to accept security terms at its contract renewal.

Questions

Alex Sample, CISSP

vCISO · Security Consultant · Incident Response Advisor

hello@example.com · example.com

The full assessment report contains detailed findings, evidence, and methodology.