04

2026 BEST PRACTICES · VOLUME 04

Healthcare Cybersecurity

A 2026 playbook for clinics and practices: protecting electronic health information, preserving care during outages, and managing the vendors that touch patient data.

CONTENTS

How to use this guide

Fourteen pages, no filler. Read the executive summary and the scenario first; use the checklist when you need to act.

01 Executive summary 03
02 The 2026 threat landscape 04
03 Identity, cloud and the insider 05
04 Twelve controls that matter 06
05 Controls in practice 07
06 The 2026 picture for healthcare practices 08
07 Scenario, priorities and quick wins 09
08 Your first 90 days and the budget 10
09 Incident response 11
10 Ransomware, communications and training 12
11 The 2026 checklist 13
12 Frameworks, sources and next steps 14

Who this is for

Healthcare Practices — Clinics & practices. Written for owners, directors, clerks, IT leads and anyone who has to make the security decision without a security department.

How to read it

Pages 3–5 explain what changed.
Pages 6–7 are the twelve controls.
Pages 8–9 are your sector.
Pages 10–12 are the plan.
Pages 13–14 are for doing.

Every recommendation maps to a recognised framework. Sources are listed on page 14. Nothing here requires a large budget to begin.

THE THREE QUESTIONS THIS GUIDE ANSWERS

Where are we exposed?

The threat landscape on pages 4–5 and the sector picture on page 8 rank the risks that actually apply to healthcare practices.

What do we fix first?

Twelve controls on pages 6–7, sequenced into a 90-day plan on page 10, with a budget frame that fits a small team.

What if it goes wrong?

A short incident plan on pages 11–12, including the first 48 hours of a ransomware event and who says what to whom.

EXECUTIVE SUMMARY

The floor has moved up

Most incidents are not sophisticated. They are ordinary attacks against ordinary routines — a password reused, a backup never tested, a payment change nobody questioned. 2026 makes those routines more expensive.

Three shifts define the year. First, **phishing became fluent**: generative tools produce targeted messages in perfect register, and voice cloning is used to authorise payments by phone. Second, **ransomware became an extortion business**: data is stolen before systems are encrypted, so a clean restore no longer ends the incident. Third, **identity became the perimeter**: remote work, SaaS and vendor access mean the stolen session matters more than the stolen laptop.

For healthcare practices, the practical consequence is that the basics are no longer optional. Multi-factor authentication, a tested backup and a payment-verification rule prevent more loss than any single product. The twelve controls in this guide are the ones that consistently change outcomes for organisations of your size.

This is not a compliance manual. It is a plan you can start on Monday, with a 90-day sequence, a budget frame and a checklist you can hand to a colleague.

What you will have by the end

Twelve prioritised controls, a sector-specific threat picture, a tested recovery approach, an incident plan short enough to use, and a checklist with owners and dates.

AT A GLANCE

Highest risks for healthcare practices

- MFA for EHR, email, remote access and administrators.
- Immutable, off-site backups plus a documented downtime procedure.
- Business associate inventory, agreements and access review.
- Encryption on every device that can hold PHI.
- Audit logging and access reviews in the EHR.

The one-sentence version

Prove who is asking, keep a copy you can restore, and know who to call — then make sure the whole organisation can do those three things without you.

THREE SHIFTS, IN ONE LINE EACH

Phishing is fluent

AI writes in your organisation's voice. Verify money and access requests out-of-band, every time.

Ransomware is extortion

Data leaves before encryption starts. A restore recovers systems, not the notification duty.

Identity is the perimeter

The stolen session is worth more than the stolen laptop. Protect accounts before devices.

THREE OBJECTIONS WORTH ANSWERING

"We're too small to be targeted."

Automated attacks do not check revenue. Small organisations are chosen because they are reachable and recover slowly.

"We can't afford a programme."

The first 30 days in this guide cost time, not money: MFA, a tested backup and a payment rule are configuration and process.

"Our IT provider handles it."

Ask which of the twelve controls they own, in writing. Co-management works when the split is documented.

14 PAGES · 12 CONTROLS · 90-DAY PLAN · 50-POINT CHECKLIST

THREAT LANDSCAPE · 01

What is actually attacking you

Six external patterns account for most of the loss we see in organisations of this size. None requires a nation-state; each exploits a normal business process.

AI-assisted phishing and business email compromise

Generative tools produce fluent, context-aware messages that reference real projects, colleagues and invoices. Voice cloning is used to authorise payments by phone. The defence is procedural: verify any money or access request out-of-band, and never trust a single channel.

Internet-facing and edge devices

VPN concentrators, firewalls, remote-management agents and web portals are scanned continuously. A missing patch on one appliance can bypass every control behind it. Inventory these devices, remove what you do not need, and patch them faster than everything else.

Credential theft and session hijacking

Infostealers harvest cookies and tokens, so a stolen session can outlive a password reset. Phishable MFA is not enough on its own. Prefer passkeys or security keys for administrators and high-value accounts.

Ransomware and double extortion

Crews steal data first and encrypt second. Restoring from backup does not remove the obligation to notify regulators, clients, patients or students. Assume any endpoint can be the entry point, and design recovery so it does not depend on the credentials the attacker has already taken.

Supply chain and vendor access

An MSP, SaaS platform or integration can be a trusted path into your data. Ask what each vendor can reach, how their own staff authenticate, how they notify you of an incident, and what happens to your data when the contract ends.

Help-desk and identity impersonation

The quickest way past MFA is to ask the help desk to reset it. Callers impersonate executives, new starters or contractors. Put a documented identity check in front of every MFA reset and privileged account change.

THE COMMON THREAD

Attackers target **trust and routine**, not exotic technology. The response is therefore procedural as much as technical: verify out-of-band, require a second person, and make the safe path the easy one.

THREAT TO FIRST MOVE

THREAT	FIRST MOVE THIS QUARTER	CONTROL
AI-assisted phishing and BEC	Publish SPF, DKIM and DMARC at enforcement; add an external-sender banner.	07
Ransomware and extortion	Prove one full restore from an offline copy, and time it.	04
Internet-facing and edge devices	Inventory every public service and patch critical ones within seven days.	02
Supply chain and vendor access	List every vendor with admin access; revoke the ones you no longer use.	10
Credential theft and session hijacking	Move administrators and finance to passkeys or security keys.	03
Help-desk impersonation	Add a callback step to every MFA reset and privileged change.	06

THREAT LANDSCAPE · 02

Identity, cloud and the insider

External attackers rarely arrive through the front door. They use the access your own systems, devices and people already have.

Cloud and SaaS misconfiguration

Public file links, over-broad sharing and stale guest accounts expose data without any attacker effort. Harden the platforms you already pay for before buying another tool.

Privileged access sprawl

Shared administrator logins, permanent admin rights and orphaned accounts make every phishing email more dangerous. Privilege should be small, temporary and reviewed.

Mobile and remote work

Personal phones, unmanaged laptops and home routers extend your perimeter into places you do not control. Require device compliance for email and applications, and encrypt everything that leaves the building.

Data sprawl and retention

Sensitive records accumulate in mailboxes, shared drives and chat. The safest data is deleted data; define retention and apply it.

Shadow AI

Staff paste contracts, student records or patient notes into consumer chatbots. Approve a tool, set rules, and monitor for data leaving through unapproved services.

Physical and operational gaps

Tailgating, unlabelled backup media, exposed wiring and an uninterruptible power supply that has never been tested are still common causes of outages and loss.

Highest-leverage internal fixes for healthcare practices

- MFA for EHR, email, remote access and administrators.
- Immutable, off-site backups plus a documented downtime procedure.
- Business associate inventory, agreements and access review.

WARNING SIGNS IN YOUR OWN ENVIRONMENT

WHAT YOU MIGHT SEE	WHAT IT CAN MEAN	DO THIS
Repeated MFA prompts you did not start	Password already stolen; the attacker is trying to fatigue you.	Reset sessions, not just the password.
New mail-forwarding or inbox rules	Account takeover; mail is being copied to an outside address.	Remove rules, review sent items.
Files renamed with unusual extensions	Ransomware staging or a failed encryption run.	Isolate, preserve, do not wipe.
A new administrator outside change control	Privilege escalation or a compromised admin account.	Disable, review audit logs.
Bulk exports from a records system	Data theft or an unapproved workflow.	Confirm with the data owner.
Urgent password-reset emails	Help-desk impersonation and credential harvesting.	Verify by phone using a known number.

CONTROLS · 01

Twelve controls that matter

Prioritised for impact and feasibility. If you only do six things this year, do these.

01 **Know what you own**

You cannot protect, patch or recover a device you have not recorded. Most incident responders lose their first day reconstructing an asset list.

- Maintain one register of hardware, software, cloud services and who owns each.
- Record the data each system holds: payment, health, student, donor or public records.
- Review quarterly; delete or archive what nobody uses.

02 **Patch the things that matter first**

Attackers exploit known vulnerabilities, not exotic ones. The gap is usually a forgotten appliance or a plugin no one tracks.

- Patch internet-facing systems and browsers on a 7-day clock; other systems monthly.
- Use a vulnerability scan you can read and act on, not a 90-page report.
- Track exceptions with an owner and an expiry date.

03 **Phishing-resistant MFA on every door**

Passwords alone no longer survive. Push and SMS codes can be phished or fatigue-spammed; passkeys and security keys cannot be replayed.

- Start with email, remote access, finance and every administrator account.
- Move priority accounts to FIDO2 keys or passkeys.
- Remove MFA bypasses, legacy protocols and stale “remember this device” rules.

04 **Back up so you can restore, not just recover**

Ransomware crews delete backups and steal data first. A backup that shares credentials or the network with production is not a backup.

- Follow 3-2-1-1-0: three copies, two media, one off-site, one offline or immutable, zero unverified restores.
- Keep backup credentials separate from the domain you are protecting.
- Test a full restore at least twice a year and record how long it took.

05 **Endpoint detection that someone watches**

Antivirus signatures miss fileless and hands-on-keyboard attacks. Detection only helps if an alert reaches a human with authority to act.

- Deploy EDR on every endpoint, including the server that only the vendor logs into.
- Define who receives alerts, the response window and the escalation path.
- Practise isolating a compromised endpoint before you need to.

06 **Separate duty from convenience**

A single administrator account used for email, browsing and server changes turns one phish into a full compromise.

- Give every person their own named account; no shared logins.
- Use a separate administrator account only for administration.
- Review privileged access quarterly and remove it when a role ends.

CONTROLS · 02

Controls in practice

The remaining six controls protect the organisation once an attacker is already inside — or once someone on the inside makes a mistake.

07 Authenticate your email domain

SPF, DKIM and DMARC stop attackers sending mail as your organisation — the core of invoice, payroll and grant fraud.

- Publish SPF and DKIM records for every sending service you use.
- Move DMARC to enforcement (p=reject) with reporting.
- Block or flag external mail that claims to be internal.

08 Segment the network and the trust

Flat networks let an attacker move from a reception PC to the finance server in minutes. Segmentation buys time and limits damage.

- Separate guest, staff, student, clinical or operational networks.
- Keep operational technology (HVAC, cameras, pumps) off the business network.
- Require a jump host or VPN with MFA for administrative access.

09 Write a plan you can execute at 2 a.m.

Under pressure, people default to improvisation. A one-page plan with roles and phone numbers is worth more than a 70-page binder never opened.

- Name an incident lead, a deputy and a communications owner.
- Print a contact tree that works when email and the intranet are down.
- Run a tabletop exercise with leadership, not just IT, every year.

10 Treat vendors as part of your attack surface

An MSP, billing provider or software integration can become the way into your data — and your obligations do not end at their contract.

- Inventory every service that touches sensitive data or has admin access.
- Ask for their security attestation and breach-notification terms.
- Review access when a contract changes or ends; revoke it the same week.

11 Train judgement, not fear

Awareness programmes that only show scary slides do not change behaviour. Short, frequent practice on real-looking messages does.

- Run quarterly phishing simulations with a no-blame reporting culture.
- Make reporting one click, and close the loop with staff who report.
- Focus training on money, credentials and data — the three things attackers want.

12 Write it down and review it

Unwritten practice disappears when the person who knew it leaves. Regulators and insurers ask for evidence, not verbal assurances.

- Keep a short policy set: acceptable use, access, backups, incidents, vendors.
- Assign an owner and a review date to each policy.
- Keep evidence — training records, restore tests, access reviews — in one place.

MATURITY	WHAT IT LOOKS LIKE	EVIDENCE YOU CAN SHOW
Crawl	MFA on email and admins; nightly backup; patching when someone remembers.	MFA report, backup log, patch list.
Walk	Phishing-resistant MFA; tested restores; EDR alerts answered; access reviews.	Restore test record, alert log, review minutes.
Run	Segmented network; tabletop exercises; vendor reviews; continuous monitoring.	Exercise report, vendor register, monitoring dashboard.

SECTOR FOCUS · 01

The 2026 picture for healthcare practices

A healthcare practice cannot pause care while systems are down. Electronic health records, scheduling, imaging and e-prescribing are now business-critical, and every one of them holds protected health information. At the same time, small practices depend on vendors for almost everything: the EHR, billing, transcription, devices and IT support. Security is therefore a matter of contract, procedure and recoverability as much as technology.

WHERE THE RISK SITS	LEVEL	WHY IT APPLIES TO YOU
Ransomware and EHR downtime	CRITICAL	Care stops; recovery depends entirely on backup quality.
Phishing and credential theft	CRITICAL	Email is the front door to ePHI and billing systems.
Vendor and business-associate exposure	HIGH	Billing, transcription and IT vendors hold broad access.
Medical device and legacy systems	HIGH	Devices that cannot be patched or authenticated.
Insider and over-broad access	MEDIUM	Staff can view records beyond their role.
Lost or stolen devices	MEDIUM	Unencrypted laptops and phones holding PHI.

RULES AND FRAMEWORKS THAT APPLY

INSTRUMENT	WHAT IT ASKS OF YOU	APPLIES WHEN
HIPAA Security Rule	Administrative, physical and technical safeguards for electronic PHI.	All covered entities and business associates
HIPAA Breach Notification Rule	Individual, HHS and media notification duties after a breach.	All covered entities
NIST SP 800-66	Implementation guidance for the HIPAA Security Rule.	Recommended reference
PCI DSS 4.0.1	Controls for card payments at the front desk and online.	If card data is handled
Business Associate Agreements	Contractual security and notification obligations with vendors.	Every vendor touching ePHI

HOW TO READ THE RULES

You are not expected to satisfy every instrument at once. Start with the one that is mandatory for you, map the twelve controls to it, and keep evidence — auditors, funders and insurers ask for proof, not intent.

SECTOR FOCUS · 02

Illustrative scenario: an EHR outage during clinic hours

A receptionist opens an attachment that claims to be a lab result. Overnight, the practice management server is encrypted and the EHR is offline. The waiting room fills, appointments cannot be confirmed, and staff cannot verify allergies or prescriptions.

The practice has backups on a NAS in the same room; the ransomware crew deleted them. The vendor's support line opens at 8 a.m. The practice learns three things that day: it needed an offline copy, a downtime procedure, and a contact list that did not depend on email.

What would have stopped it

- Immutable, off-site backups with a tested restore procedure.
- MFA on email, EHR and remote access; separate admin accounts.
- A written downtime procedure for scheduling, prescriptions and paper records.
- Endpoint detection on every workstation and server.
- Business associate agreements that define breach notification timelines.

PRIORITY ACTIONS

1. MFA for EHR, email, remote access and administrators.
2. Immutable, off-site backups plus a documented downtime procedure.
3. Business associate inventory, agreements and access review.
4. Encryption on every device that can hold PHI.
5. Audit logging and access reviews in the EHR.

QUICK WINS THIS MONTH

- Confirm every business associate agreement is signed and current.
- Test the EHR restore and time it.
- Print downtime forms and store them with the front desk.
- Turn on MFA for the EHR and email.
- Disable generic and shared clinical logins where licensing permits.

QUESTIONS FOR LEADERSHIP

- How many hours can the clinic operate without the EHR?
- Which vendors can see protected health information today?
- When did we last test the restore, and how long did it take?
- Can staff access records beyond what their role requires?
- Who decides whether a breach must be reported, and how quickly?

FIVE QUESTIONS FOR YOUR IT PROVIDER OR MSP

- Which of the twelve controls do you own today — and what evidence do you hold?
- When did you last restore our most critical system, and how long did it take?
- Who receives security alerts out of hours, and what is the response window?
- Which accounts have standing administrator access, and when were they reviewed?
- How would you notify us of a breach, and what is your own MFA posture?

PLAN · 01

Your first 90 days

A sequence that respects a small team. Finish each phase before adding the next; the order matters more than the speed.

DAYS 1-30

Stabilise the basics

- Turn on phishing-resistant MFA for email, remote access, finance and administrators.
- Confirm one offline or immutable backup exists and can be restored.
- Inventory internet-facing systems and patch anything critical within seven days.
- Publish SPF, DKIM and start DMARC reporting.
- Name an incident lead and print the contact tree.

DAYS 31-60

Reduce the blast radius

- Deploy EDR everywhere and route alerts to a named responder.
- Remove shared accounts and standing admin rights; issue separate admin accounts.
- Review vendor access and terminate what is no longer needed.
- Write the one-page incident response plan and a communications template.
- Run the first staff phishing simulation with a no-blame reporting process.

DAYS 61-90

Prove it works

- Run a tabletop exercise with leadership and test the contact tree.
- Perform a timed restore of a critical system and record the result.
- Segment guest, staff and operational networks; remove default passwords.
- Complete the checklist in this guide and assign owners to every gap.
- Review cyber insurance coverage against the scenarios you now understand.

BUDGET FRAME

TIER	SPEND	WHAT IT BUYS
Baseline	Existing IT spend + 10%	MFA, backup, encryption, endpoint protection, BAA review.
Target	+15–20%	Monitoring, access reviews, downtime exercises, training.
Resilient	+20–30%	Segmentation, device inventory, tabletop exercises, IR retainer.

Staffing reality

Most organisations your size cannot hire a security team. Choose one of three models and document it: **in-house generalist** with a named security owner; **managed service provider** for monitoring and patching; or **co-managed**, where internal staff own policy and the provider owns tooling and response.

Whichever you choose, the plan above stays the same. What changes is who ticks each box.

RESPONSE · 01

Incident response, without the binder

An incident is a business event, not only an IT event. The plan below is deliberately short enough to use under pressure. Adapt names and numbers, print two copies, and store one off-site.

01 Prepare

Assign the incident lead, deputy, communications owner and legal/privacy contact. Keep an offline contact tree. Decide in advance who can shut down a system and who can authorise spending.

02 Detect and confirm

Record what was seen, when, and on which system. Preserve logs before rebuilding anything. Distinguish a suspected incident from a confirmed one; both deserve a timeline.

03 Contain

Isolate affected endpoints from the network without wiping them. Disable compromised accounts and reset sessions and tokens, not just passwords. Do not power off a machine you may need to investigate.

04 Eradicate and recover

Remove persistence, rebuild from known-good images, restore data from a verified backup, and monitor closely for re-entry. Recovery is complete only when the business process works, not when the server pings.

05 Communicate and notify

Use prepared templates. Notify your insurer, legal counsel and, where required, regulators, affected individuals and law enforcement. One spokesperson, one approved message, a fixed cadence.

06 Learn

Hold a blameless review within two weeks. Record what slowed you down, what you would do differently, and the dated actions that follow. Update the plan.

ROLES TO ASSIGN BEFORE ANYTHING HAPPENS

ROLE	RESPONSIBILITY
Incident lead	Runs the response, makes the call, owns the timeline
Technical lead	Contains, eradicates and restores; keeps evidence
Communications	Staff, customers, media, regulators; one voice
Legal & privacy	Notification duties, contracts, insurer, counsel
Executive sponsor	Budget, business continuity, external relationships
Scribe	Decision log, timestamps, actions and owners

PRINT THIS PAGE. KEEP A COPY WHERE EMAIL AND THE INTRANET ARE NOT REQUIRED.

RESPONSE · 02

Ransomware: the first 48 hours

Assume encryption is only half the incident. Data theft, notification and public trust are the rest.

1. Isolate affected systems and preserve evidence before rebuilding.
2. Engage your insurer and legal counsel early; they coordinate notification duties.
3. Report to law enforcement — in the United States, the FBI (IC3) and CISA — and follow their guidance.
4. Restore from a verified, offline backup and validate data integrity.
5. Do not pay without legal advice: payment may be unlawful for sanctioned entities and does not guarantee recovery.
6. Expect public and regulatory scrutiny; communicate on a fixed cadence with facts you can verify.

Communications rules

One spokesperson, one approved message, a fixed cadence. Say what you know, what you do not know, and when you will update next. Never speculate about cause or data in public.

INSURANCE AND REPORTING

Call your insurer early — most policies require prompt notice and may provide legal counsel and negotiators. In the United States, report to the FBI (IC3) and CISA; many states and sectors impose their own notification timelines.

AWARENESS THAT WORKS

- Train on PHI handling and the minimum-necessary standard.
- Rehearse the downtime procedure with clinical staff, not only IT.
- Include front-desk staff in payment and identity-fraud training.

THE 24-HOUR TEST

Could you isolate an endpoint, disable an account and reach your incident lead within 24 hours — without email? If not, that is the first thing to fix.

THE FIRST 48 HOURS, HOUR BY HOUR

WHEN	ACTION	OWNER
T+0	Isolate affected systems, preserve evidence, call the incident lead.	Technical lead
T+1h	Notify insurer and counsel; disable accounts and reset sessions and tokens.	Incident lead
T+4h	Decide restore path; brief leadership; draft the holding statement.	Incident lead + comms
T+24h	Begin restore from verified backup; confirm notification duties; brief staff.	Technical + legal
T+48h	Validate data integrity, monitor for re-entry, update stakeholders.	Incident lead

EVIDENCE TO KEEP

- Logs from identity, email, endpoint and cloud systems, exported before rebuild.
- A written timeline with times, sources and who did what.
- Images or snapshots of affected machines where practical.
- Copies of communications, decisions and approvals.

WHEN TO CALL IN OUTSIDE HELP

- Data has left the organisation, or a ransom demand is received.
- Regulated data — health, student, financial, criminal justice — is involved.
- You have no tested backup, or the backup was reachable from the compromised network.
- Your insurer requires an approved incident-response firm.

ADAPT THESE STEPS TO YOUR REGULATOR AND INSURER. THIS PAGE IS GUIDANCE, NOT LEGAL ADVICE.

APPENDIX A

The 2026 checklist

Work through it once with a colleague. Give every unchecked item an owner and a date; that list becomes your plan.

GOVERN

- ☐ A named owner for cybersecurity, with time allocated
- ☐ A one-page incident response plan, printed and off-site
- ☐ Cyber insurance reviewed against realistic scenarios
- ☐ A short policy set with review dates and evidence
- ☐ Board or leadership briefed at least twice a year

IDENTIFY

- ☐ Inventory of hardware, software and cloud services
- ☐ Data map: where sensitive records live and who can reach them
- ☐ Internet-facing systems listed with patch owners
- ☐ Vendor list with data access and contract terms
- ☐ Risk register with owners and review dates

PROTECT

- ☐ MFA on email, remote access, finance and administrators
- ☐ Passkeys or security keys for privileged accounts
- ☐ Separate admin accounts; no shared logins
- ☐ SPF, DKIM and DMARC at enforcement
- ☐ EDR on every endpoint and server
- ☐ Patching SLA for internet-facing systems
- ☐ Backups: 3-2-1-1-0, credentials separated, tested
- ☐ Disk encryption on laptops and mobile devices
- ☐ Guest, staff and operational networks separated
- ☐ Default passwords changed; unused services disabled

DETECT

- ☐ A named recipient for security alerts and a response window
- ☐ Logging enabled on identity, email and cloud administration
- ☐ Failed-login and MFA-reset alerts reviewed
- ☐ Phishing reports reach one inbox and get triaged
- ☐ Backup jobs monitored for silent failure

RESPOND

- ☐ Contact tree includes insurer, counsel, IT, leadership
- ☐ Tabletop exercise completed in the last 12 months
- ☐ Communication templates prepared and approved
- ☐ Forensic image or log preservation procedure
- ☐ Restore test completed and timed in the last 6 months

RECOVER

- ☐ Recovery time objective agreed for critical systems
- ☐ Alternate process for payments and records if systems are down
- ☐ Post-incident review with dated actions
- ☐ Lessons fed back into training and policy

HEALTHCARE SPECIFICS

- ☐ Business associate list current, with signed agreements
- ☐ EHR audit logs enabled and reviewed
- ☐ Downtime procedure posted at reception and nurses' station
- ☐ Devices holding PHI encrypted and inventoried
- ☐ Breach risk assessment procedure documented

VENDORS AND DATA

- ☐ Vendor list with data access and contract end dates
- ☐ Signed confidentiality and data-processing terms
- ☐ Access revoked when a contract ends
- ☐ Data deletion confirmed at exit
- ☐ Annual vendor review scheduled
- ☐ Backup and incident terms in every contract

IF YOU ONLY DO FIVE THIS QUARTER

1. Phishing-resistant MFA on email, finance and administrators.
2. One verified offline backup, restored and timed.
3. Patch every internet-facing system within seven days.
4. A call-back rule for bank, payroll and grant changes.
5. A printed incident contact tree, tested once.

How to score this

Count the boxes you can evidence, not the ones you intend to do.

Under 20: start with the five above.
20–35: finish the Protect and Detect groups.
Over 35: run a tabletop and test a restore.

SCORE YOURSELF HONESTLY: EACH UNCHECKED BOX IS A TASK, NOT A FAILURE.

APPENDIX B

Frameworks, sources and next steps

You do not need to adopt every framework. Pick one as your backbone, map the controls in this guide to it, and keep the evidence.

NIST Cybersecurity Framework 2.0	Six functions — Govern, Identify, Protect, Detect, Respond, Recover — used as the backbone of this guide.
CIS Critical Security Controls v8.1	Eighteen prioritised safeguards, including inventory, patching, access and monitoring.
CISA Cross-Sector Cybersecurity Performance Goals	A short baseline of high-impact practices for small and mid-sized organisations.
CISA #StopRansomware Guide	Practical prevention and response steps for ransomware events.
NIST SP 800-63B	Digital identity guidance behind the move to phishing-resistant authentication.
NIST SP 800-40	Patch management planning and enterprise practice.
CISA K-12 and sector guidance	Sector-specific material for schools, local government and critical infrastructure.

Next steps

1. Pick three controls and assign owners.
2. Book the restore test this month.
3. Print the incident page.
4. Re-run the checklist in 90 days.

About Cybr Sec Solutions. A managed service provider specialising in cyber security training and backup/recovery solutions. With over 14 years of direct experience securing school districts and city network infrastructures.

In healthcare, availability is a safety control. Build for the day the EHR is down, and the security programme becomes part of patient care rather than an obstacle to it.

GLOSSARY

MFA — multi-factor authentication: a password plus a second proof, such as a passkey.

EDR — endpoint detection and response: software that watches devices for malicious behaviour.

BEC — business email compromise: impersonation used to redirect money or data.

Least privilege — giving each account only the access its role requires.

Phishing-resistant MFA — authentication that cannot be replayed, such as FIDO2 security keys.

DMARC — an email policy telling receivers what to do with unauthenticated mail.

Immutable backup — a copy that cannot be altered or deleted during its retention period.

Tabletop — a discussion-based rehearsal of the incident plan with leadership.

This document provides general guidance for educational purposes and is not legal, regulatory, insurance or professional advice. Requirements vary by jurisdiction, sector and contract; confirm obligations with qualified counsel and the relevant regulator before acting. Framework names are the property of their respective owners. Scenarios are illustrative and do not describe any actual organisation.