

Cybersecurity Essentials

for Business Owners



What a small or mid-sized business should
have in place, in plain language – and how to
tell whether it does.

LONG ISLAND AND NEW YORK CITY • 2026 EDITION

Before you read this

You already know the risk is real. You have had the phishing email. Someone you know has paid a ransom, or wired money to a stranger who sounded exactly like their boss. What you may not have is a plain list of what a business like yours should have in place, in what order, and how to check whether it does. That is this booklet.

I have kept the frameworks in – NIST and CIS – because your insurer, your auditor and your larger customers speak that language, and you should recognize it when they do. But every control is written in ours, with the minimum a small business should actually do, and one honest line about how we do it for our clients.

Two requests. Read the scorecard on page 22 first; it takes ten minutes and tells you which pages matter for you. And if an answer surprises you, reach out. Not because we sell the fix – though we do – but because most of what is in here costs less to do than to keep explaining.

Mariusz Sztanga
Chief Guru, Interactive AV-IT
Hauppauge, New York



Mariusz Sztanga, Chief Guru

How to read this

- Each of the eighteen controls has three parts: why it matters to you, the minimum to put in place, and how we do it.
- The controls come from a published checklist, the CIS Controls. Its starting level, called IG1, is the 56 basics every business should have regardless of size. Page 8 explains it.
- Every statistic carries its source and year. If a number here is more than two years old when you read it, ask us for the current one.

Five words we could not avoid

- **MFA** – a second step at sign-in, such as a code from an app on your phone, so a stolen password alone is not enough.
- **CIS Controls** – a checklist of eighteen security practices maintained by the Center for Internet Security. IG1 is its starting level.
- **NIST** – the US government's standards body. Its Cybersecurity Framework is the yardstick insurers and auditors use.
- **Patching** – installing the updates software makers release to close holes attackers already know about.
- **Administrator rights** – the level of access that can install or change anything on a computer. Attackers want it, so day-to-day work should not have it.

If you only read one page

The whole booklet in six lines, for the owner with ten minutes. Each one points to the page that backs it up.

- 1 Money leaves by wire because somebody believed an email.** Business email compromise cost \$3.0 billion last year. The fix is a call-back rule on a number you already had, not a product. **Page 6**
- 2 The leading way in is now a computer nobody updated.** Three breaches in ten started with a hole that an update would have closed. Automatic updates, and nobody doing daily work with administrator rights, close most of that door. **Pages 9 to 17**
- 3 Fifty-six basics are the floor for every business, whatever its size.** They are the starting level of a published checklist, the CIS Controls, that insurers and auditors work from. Pages 9 to 17 put all of it in plain language, with what we do for you on each. **Page 8**
- 4 Your insurer already holds the checklist.** A second step at every sign-in, someone watching every computer around the clock, backups kept out of reach and tested, staff who have been trained. A "yes" on the application that is not true is a claim that is not paid. **Page 18**
- 5 New York's rules reach further than most owners think.** The SHIELD Act reaches any business holding a New York resident's data; the finance, healthcare and defense-contracting rules reach by sector. **Page 19**
- 6 AI is a data question before it is a tool question.** Decide what may never go in, fix the shared drive first, and come to us before you switch it on. **Page 20**

Do you need to read on? Three questions.

- Does every sign-in to email, remote access and administrator accounts need a second step, such as a code from an app, and not only a password?
- Has anyone restored a file from your backup in the last three months?
- If one of your computers raises an alarm at three in the morning, does a person act on it?

Three yeses: skip to the scorecard on page 22 and confirm the rest. Any no: start at page 9.

If at any point this feels like more than you want to take on alone, stop and reach out. We go through it with you – set it up together, or book fifteen minutes and start there.

CONTENTS

Last year, by the numbers	4	AI at work, before you switch it on	20
How it actually happens	6	The first hour	21
Two frameworks, one page	8	Eighteen questions – score yourself	22
The eighteen controls	9	How we work	23
What your insurer will ask	18	Reach out	24
New York rules that may already apply to you	19		

Last year, by the numbers

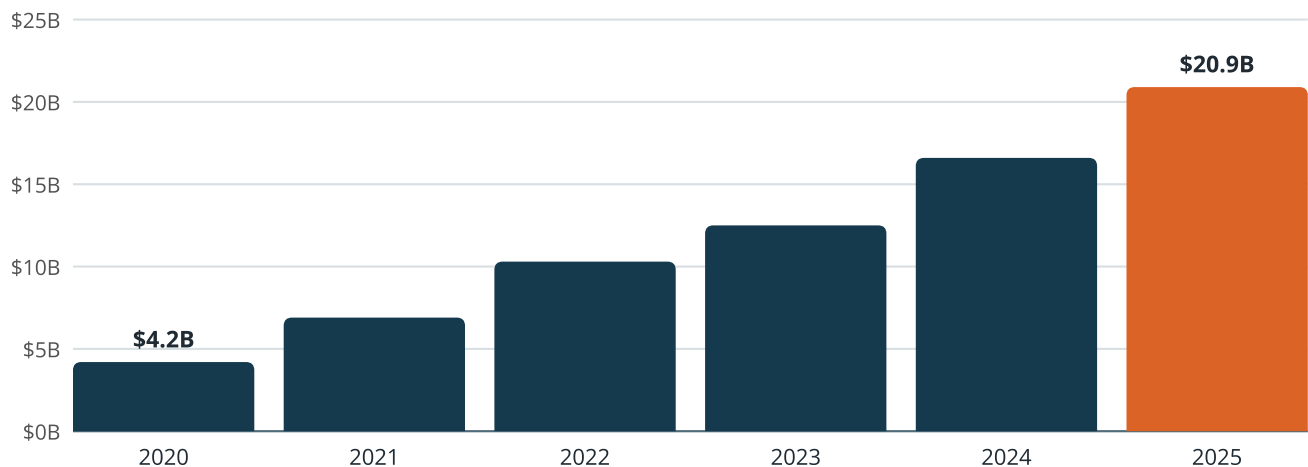


Two reports worth an owner's attention

Two reports come out every year that are worth ten minutes of a business owner's time: the FBI's Internet Crime Report and Verizon's Data Breach Investigations Report. Here is what the 2026 editions say about 2025. Every figure carries its source, so you can check it – and so you know when it has gone stale.

Losses reported to the FBI, by year

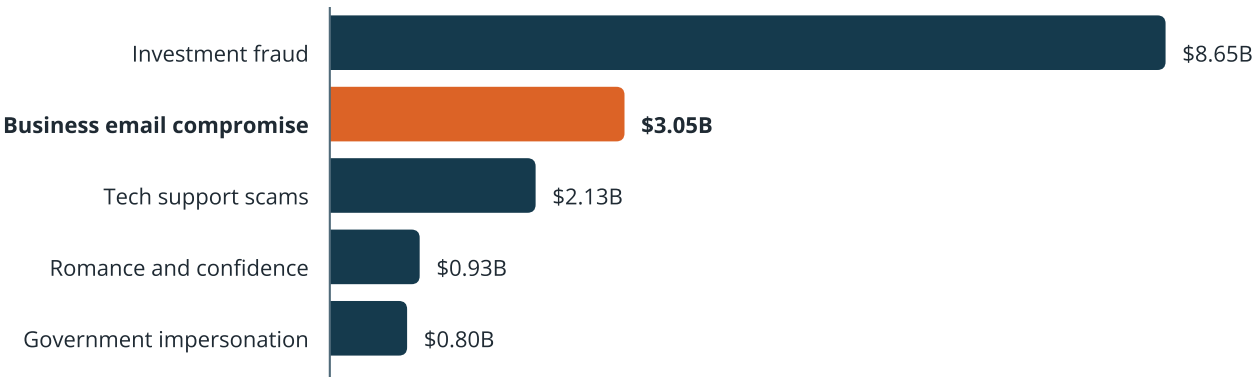
Billions of dollars – 2025 was up 26 percent on 2024



SOURCE: FBI IC3 2025 INTERNET CRIME REPORT

Where the money went in 2025

Top five cyber-enabled fraud types by reported loss, billions of dollars



SOURCE: FBI IC3 2025 INTERNET CRIME REPORT

1,008,597

complaints the FBI received in 2025

\$30 million+

business email compromise losses
where the FBI confirmed AI was used

22,000+

confirmed breaches analyzed in
Verizon's 2026 report

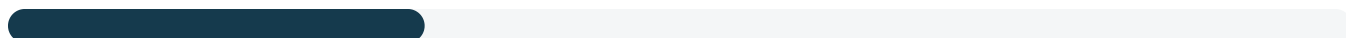
How breaches start

Share of confirmed breaches, November 2024 to October 2025

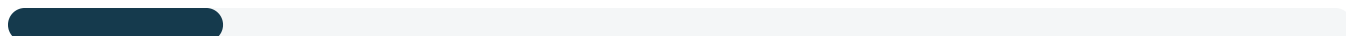
62% of breaches involved a person – a click, a reused password, a mistake



31% began with a hole that an update would have closed – now the leading way in



16% began with social engineering



SOURCE: VERIZON 2026 DATA BREACH INVESTIGATIONS REPORT

How the money leaves

24,768 complaints in 2025, over \$122,000 each on average

86% of business email compromise losses left by wire transfer or bank-to-bank (ACH) transfer



SOURCE: FBI IC3 2025 INTERNET CRIME REPORT

What this means for a business on Long Island

Two of those numbers matter more than the rest. Money leaves by wire because somebody believed an email. That is a process problem before it is a technology problem, and it is fixed with a phone call to a number you already had. And the leading way in is now a system nobody patched. That is a maintenance problem. Maintenance is boring, which is why it gets skipped, which is why it works for the attacker.

One number we left out on purpose: the size of the average ransom. It changes by the quarter and every vendor quotes a different figure. Ask us for the current one.

How it actually happens



Six patterns, and what stops each one

Older guides list categories of virus. This is how a small or mid-sized business actually loses money or data in 2026, what it looks like from your desk, and which controls stop it. The controls are numbered and named as they are on pages 9 to 17, with the page each one sits on.

1 The invoice that changed its bank details

Business email compromise

What it looks like: a supplier emails new remittance details. Or the owner emails the bookkeeper from the road asking for an urgent wire. The email is real, or nearly – the attacker has been reading the mailbox for weeks and knows the names, the tone and the timing.

What stops it: a call-back rule for any change in payment details, made to a number you already had. A second step at sign-in (MFA) on every mailbox. Monitoring that catches the sign-in from the wrong country and the mailbox rule that hides the replies.

STOPPED BY [05 Accounts p. 11](#) [06 Access p. 11](#) [14 Training p. 15](#) [17 Incident plan p. 17](#)

2 The login that was not you

Email account takeover – Microsoft 365 or Google Workspace

What it looks like: a convincing sign-in page that also asks for your MFA code and passes it straight through. Or a burst of approve-this prompts at eleven at night until someone taps Approve to make it stop. The attacker then creates a rule that hides certain replies, and starts reading.

What stops it: a second sign-in step that a fake page cannot relay – an authenticator app that asks you to match a number, or a passkey, which lives on your phone and cannot be typed into a fake page. Never a text message. Sign-in rules that block the impossible location. Identity monitoring that watches for the new rule and the odd session. And staff who know that an approve prompt they did not start is an attack, not a glitch.

STOPPED BY [05 Accounts p. 11](#) [06 Access p. 11](#) [13 Network watch p. 15](#) [14 Training p. 15](#)

3 Ransomware, with the data taken first

What it looks like: a normal Tuesday until the shared drive shows renamed files and a text file with instructions. They copied the data before they encrypted it, so a good backup does not end the conversation – it ends the outage.

What stops it: patched systems, nobody working as an administrator, detection that isolates the machine within minutes, and an offsite backup copy that cannot be altered, tested by restoring from it.

STOPPED BY [04 Config p. 10](#) [05 Accounts p. 11](#) [07 Patching p. 12](#) [10 Malware p. 13](#)

[11 Backup p. 14](#)

4 The voice that sounded like you

AI impersonation

What it looks like: a call or voice note from "the owner" or "the vendor", urgent and plausible, built from a few seconds of public audio. Sometimes a video call. The finance person does what the voice asks because the voice is right.

What stops it: a rule that no payment, credential or access change happens on the strength of a voice, a video or an email alone. A call back on a known number. A code word for the finance team.

STOPPED BY 14 Training p. 15 17 Incident plan p. 17

5 The vendor that got in first

Supply chain

What it looks like: nothing, for a while. Then the software you rely on, or the firm that manages it, is compromised, and the attacker uses their access as if it were yours.

What stops it: knowing which vendors can reach what, asking them the questions on page 23, and removing access when the contract ends.

STOPPED BY 15 Vendors p. 16

6 The password that had been out there for years

Password-stealing malware and reused passwords

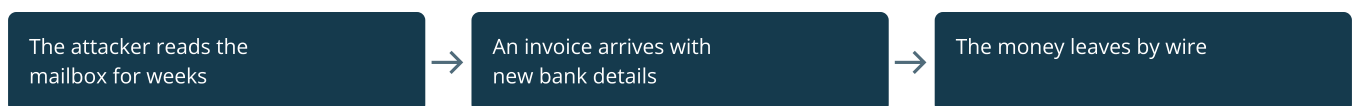
What it looks like: a personal laptop picks up a piece of malware that harvests every saved browser password. The work password was the same one. Nobody notices until it is used.

What stops it: a password manager, one password per site, a second sign-in step, and a periodic check of your domain against known breach data.

STOPPED BY 05 Accounts p. 11 06 Access p. 11 14 Training p. 15

Anatomy of pattern 1

The invoice that changed its bank details, step by step



● **What breaks the chain:** a call back on a number you already had, before any payment detail changes

Still out there

The older threats have not gone away: the macro in a spreadsheet, the infected USB stick, the worm that spreads on its own across a flat network, the file and boot-sector infectors from the old guides. They are rarer than the six above, and the controls on pages 9 to 17 cover them, but they remain a possibility – and more of one if your business does not run on Microsoft 365. Microsoft has blocked macros in files from the internet by default since 2022; Gmail and other platforms have their own protections and their own gaps. If you run on Gmail, every control in this booklet still applies. Only the tools that deliver them change.

Two frameworks, one page

NIST says what good looks like. CIS says what to do on Monday.

Six functions, one center

Govern informs the other five

The CIS implementation groups

How the 153 safeguards split



153 safeguards in three groups

Every business starts with the 56 in IG1



IG2 builds on IG1; IG3 on both. This booklet is IG1.

The NIST Cybersecurity Framework 2.0

NIST is the US government's standards body. Its framework, published on 26 February 2024, describes a complete program in six functions. It is the language your insurer, your bank and your larger customers use when they ask for evidence.

FUNCTION	IN PLAIN WORDS
Govern	Somebody owns this, it has a budget, and the rules are written down. New in 2.0.
Identify	You know what you have, where your data is, and what would hurt.
Protect	The controls that stop most things: access, training, patching, backups.
Detect	You would notice, and quickly.
Respond	You know what to do in the first hour, and who does it.
Recover	You get back to work, and you learn something.

The CIS Critical Security Controls, version 8.1

Published on 24 June 2024 by the Center for Internet Security: eighteen controls, 153 safeguards, arranged in three implementation groups.

GROUP	SAFEGUARDS	WHO IT IS FOR
IG1	56	Every business, whatever its size. CIS calls it essential cyber hygiene. It is where everyone starts.
IG2	74 more	Businesses with several departments, more sensitive data, or someone dedicated to IT.
IG3	23 more	Regulated or high-value environments with security specialists.

Where our clients sit

Every managed client of ours runs on IG1 as the floor, with the parts of IG2 their insurer or regulator asks for. This booklet describes IG1. If you need IG2 or IG3 you probably know it already, and we should talk.

The eighteen controls



01 Know what you own

CIS · INVENTORY AND CONTROL OF ENTERPRISE ASSETS

●●○○○ IG1 · 2 OF 5

Sounds familiar? *"There is a laptop somewhere with the old bookkeeper."*

Why it matters. You cannot protect a device you do not know you have, and an attacker scanning your network will find it before you do. This includes the display in the boardroom and the phones on the desks – they are on your network too.

Where to start. A list of every device that connects to your network, kept current, and a rule for what happens when an unknown one appears.

How we do it. Our monitoring agent reports every managed device, and the network gear flags anything that joins without one. The list lives in your client portal, and the monthly report shows what changed.

02 Know what runs on it

CIS · INVENTORY AND CONTROL OF SOFTWARE ASSETS

●●●○○○ IG1 · 3 OF 7

Sounds familiar? *"Somebody installed something to open a PDF and now there are four toolbars."*

Why it matters. Software you do not know about never gets patched. Software its maker no longer supports never will be. Windows 10 stopped receiving security updates on 14 October 2025; a machine still running it is a machine an attacker will find.

Where to start. An inventory of installed software, a short list of what is approved, and removal of the rest – and of anything past its support date.

How we do it. The same agent keeps the software list. Beside it sits a list of what is allowed to run on a managed machine – anything not on it does not start. Our technicians adjust that list as your needs change and watch what tries to run outside it. Unsupported versions are flagged and replaced before they become the way in.

03 Know where your data is, and who can reach it

CIS · DATA PROTECTION

●●●●●●○○○○○○○○ IG1 · 6 OF 14

Sounds familiar? *“Everyone can see everything on the shared drive. Including payroll.”*

Why it matters. Your data now lives in Microsoft 365 or Google Workspace, on laptops, on phones and with vendors. An attacker who gets in looks for it first, and once it is copied no backup brings it back. Encryption on laptops turns a stolen bag into a hardware loss instead of a breach notification.

Where to start. Know what sensitive data you hold and where it is. Limit who can open it. Encrypt every laptop. Keep data only as long as you need it, and wipe old devices properly.

How we do it. We start by finding the data, not by buying a tool: where the client files, the payroll and anything regulated actually live, and who can open them today. Then access is cut to roles – in Microsoft 365 or Google Workspace, on the file server and in the line-of-business applications – so the bookkeeper sees the books and nobody else does. Every laptop is encrypted by policy, Windows and Mac alike, with the recovery keys held in the management console rather than on a sticky note. USB storage is blocked or logged. Sharing outside the company is limited to named partners and reviewed. A retired device is wiped, and the record of the wipe is kept. Retention is written down before Copilot or any AI tool is allowed near the data – see page 20.

04 Set things up safely, then keep them that way

CIS · SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE

●●●●●●○○○○○○ IG1 · 7 OF 12

Sounds familiar? *“The Wi-Fi password is on a sticky note in reception.”*

Why it matters. Devices ship convenient, not safe: factory passwords, doors left open to the internet, features nobody uses. And settings drift – a change made to fix one problem stays forever.

Where to start. A documented standard build for laptops, servers, firewalls and switches. Default passwords changed. Screens that lock. Unused features off. The firewall on every laptop turned on.

How we do it. Every client runs on our Recommended Technology Platform – the same builds we use ourselves – so a machine leaves our bench the same way every time. We watch for drift and put it back.

05 One account per person, and fewer with the keys

CIS · ACCOUNT MANAGEMENT

●●●●○○ IG1 · 4 OF 6

Sounds familiar? *"We all use the admin login. It is easier."*

Why it matters. Most damage is done with an account that had more rights than the job needed. A shared account means nobody knows who did what, and a dormant one is a door nobody is watching. Attackers rarely break in; they log in, with a password that leaked from somewhere else or was guessed from a name and a year. The account they want is the one that can install software or reach every file, which is why the first thing malware tries is to run as the person who opened it. Give that person an ordinary account and most of what the malware wants is out of reach.

Where to start. A list of every account. Nobody works day to day as an administrator; admin accounts are separate and used only for admin work. Shared and dormant accounts removed. Long passphrases or a password manager. Passwords of at least fourteen characters, never shared between work and home. Anyone who leaves loses every account the day they leave, not at the end of the month.

How we do it. Nobody holds permanent administrator rights, our engineers included – rights are raised for a task, dropped after, and logged. Keeper for passwords. A leaver's accounts are disabled the day you tell us, and every account is reviewed quarterly.

06 Control who gets access, and take it back

CIS · ACCESS CONTROL MANAGEMENT

●●●●●○○○ IG1 · 5 OF 8

Sounds familiar? *"Does the guy who left in March still have email?"*

Why it matters. Access that was granted is rarely access that was removed. Every open account is a way in, and the one belonging to someone who left is the one nobody will notice being used. The second sign-in step matters because passwords leak: a code from an app on the person's phone means a stolen password is not enough on its own. It costs a few seconds at each sign-in and stops the most common way a business loses its email.

Where to start. A process for joiners, leavers and role changes. A second sign-in step (MFA) on every service reachable from the internet, on remote access, and on every administrator account. Access reviewed on a schedule. Prefer an authenticator app or a security key over text-message codes, which can be intercepted. Twice a year, list who can open what, and remove whatever no longer matches the job.

How we do it. Onboarding and offboarding are tickets with checklists, not memory. MFA is enforced through sign-in rules in Microsoft 365, and a leaver's access is removed across every system, not only email.

07 Patch, continuously

CIS · CONTINUOUS VULNERABILITY MANAGEMENT

●●●●○○○ IG1 · 4 OF 7

Sounds familiar? *"Updates? We click Later."*

Why it matters. The leading way in last year was a system nobody had patched – see page 4. Patching is boring, which is why it gets skipped, which is why it works. A software maker that publishes a fix also publishes, in effect, a map of the hole, and within days attackers are scanning the internet for anything still open. The firewall, the phone system and the printer count as much as the laptops: they run software too, and they are the ones most often forgotten.

Where to start. Automatic updates for operating systems and applications. A monthly cycle for everything else, firewalls included. A scan that tells you what you missed. Replace what can no longer be updated, whatever it cost when new. An unsupported machine is not a saving; it is the way in.

How we do it. Patching runs from the monitoring platform on a schedule you approve, third-party applications included. We watch what is behind and why, and chase it. The numbers are there if you ever want to see them.

08 Keep the logs

CIS · AUDIT LOG MANAGEMENT

●●●○○○○○○○○○ IG1 · 3 OF 12

Sounds familiar? *"We found out from the bank."*

Why it matters. When something goes wrong, logs are how you learn what happened, when, and whether it is still happening. Without them the response is guesswork, and your insurer's questions have no answers.

Where to start. Logging switched on for servers, firewalls and your email platform, whether Microsoft 365 or Google Workspace. Kept for at least ninety days. Clocks synchronized so the timeline lines up.

How we do it. Logs from the firewall, the servers and Microsoft 365 are kept for at least ninety days for every client, and longer where an insurer or regulator asks. Microsoft 365 audit logging is on from day one.

09 Email and the browser

CIS · EMAIL AND WEB BROWSER PROTECTIONS

●●○○○○○ IG1 · 2 OF 7

Sounds familiar? *"It looked exactly like the DocuSign email."*

Why it matters. Email is still the front door. The browser is the other one. Most of what reaches a person reaches them through one of the two. A phishing email that never arrives cannot be clicked, and a bad link that never loads cannot do harm, which is why the filtering belongs in front of the person rather than behind them. The three records matter for your own name as well: without them, anyone can send mail that looks like it came from you, to your own customers, and the first you hear of it is the complaint.

Where to start. Only supported browsers and mail programs. Web filtering that blocks known-bad sites before they load. The three email records – SPF, DKIM and DMARC – that let the world check mail really came from you. Dangerous attachment types blocked at the gateway. Turn off the old ways in that nobody uses any more, such as automatic forwarding of mail outside the company and sign-in methods that skip the second step. Check once a year that the three records are still set, because a change of email provider or website host can quietly undo them.

How we do it. DMARC set to reject for every client domain, so mail pretending to be you is thrown away before it lands – which also stops your name being used against your own customers. Web filtering on every managed device. Attachments and links scanned in Microsoft 365 before they arrive.

10 Defend against malware

CIS · MALWARE DEFENSES

●●●○○○○ IG1 · 3 OF 7

Sounds familiar? *"We have antivirus. It came with the computer."*

Why it matters. Free antivirus looks for known files. Modern attacks use the tools already on the machine. What you need is something that watches behavior, and someone who acts on what it sees at three in the morning.

Where to start. Anti-malware on every device, updating itself, with autorun disabled for USB drives. One central view of all of it.

How we do it. Huntress managed detection and response on every computer – software that watches behavior rather than known files, with human analysts behind it. Huntress's analysts watch around the clock and have the authority to isolate a machine from the network before we are awake. Monitoring is the loop we run – monitor, respond, maintain, report, review – not a feature.

11

Back up, and prove you can restore

CIS · DATA RECOVERY

●●●●○ IG1 · 4 OF 5

Sounds familiar? *"The backup runs every night. We think."*

Why it matters. A backup nobody has restored from is a hope. Attackers delete every backup they can reach, so the one that matters is the one they cannot. Ransomware crews look for the backup before they encrypt anything, because a working backup is the one thing that lets you refuse to pay. Email and cloud files need backing up too: Microsoft and Google keep the service running, but a deleted or encrypted file is your problem, not theirs.

Where to start. Automated backups of everything that matters, including your email and files in Microsoft 365 or Google Workspace. One copy offsite and out of reach. A restore tested on a schedule, not assumed. Decide in advance how much you can afford to lose, a day or an hour, and set the backup to match. Know how long a full restore takes before the day you need it, because that is how long you will be closed.

How we do it. Backups run to an offsite copy that cannot be changed or deleted for its retention period. We restore from it on a schedule, so we know it works before the day you need it.

12

Manage the network

CIS · NETWORK INFRASTRUCTURE MANAGEMENT

●○○○○○○○ IG1 · 1 OF 8

Sounds familiar? *"Guests use the same Wi-Fi as the accounting server."*

Why it matters. On a flat network one infected laptop can see everything. A firewall from 2017 with its default password is not a firewall. Every device you let onto the network is a device you trust with everything else on it: the visitor's phone, the television in reception, the thermostat. Separate networks turn one infected device into one problem instead of a company-wide one.

Where to start. Network equipment under support and kept updated. Documented. Guests, phones and AV on their own networks, separated from servers and workstations. Remote access only through a proper VPN or a managed remote-access tool, never a port opened on the firewall for convenience. A Wi-Fi password that changes when people leave.

How we do it. Ubiquiti UniFi throughout, managed from one console. Guest, voice and AV traffic on their own networks, so a visitor's phone and the conference room display never sit on the same network as the accounting server.

13 Watch the network

CIS · NETWORK MONITORING AND DEFENSE

○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ IG1 · 0 OF 11

Sounds familiar? *"Nobody noticed for three months."*

Why it matters. This control has no IG1 safeguards; it begins at IG2. That is CIS being honest about priorities: do the first twelve before this one. What it adds, once the basics are in place, is the ability to notice traffic that should not be there: a workstation talking to a server in a country you do not do business with, or a large file leaving at two in the morning. Attackers spend days inside a network before they act, and this is what shortens those days.

Where to start. Nothing required at IG1. If you are regulated, or move large sums, this is the first IG2 item worth adding. The practical first step is to know what normal looks like, which systems talk to which and when. An alert is only useful against that baseline.

How we do it. This control starts at IG2. If your insurer, your regulator or a large customer asks for it, we scope it with you before anything is bought.

14 Train people, then test them

CIS · SECURITY AWARENESS AND SKILLS TRAINING

● ● ● ● ● ● ● ● ○ IG1 · 8 OF 9

Sounds familiar? *"We sent the phishing video once. In 2021."*

Why it matters. Most breaches involve a person – six in ten, on page 4. A yearly video changes nothing. Short, regular, with simulated phishing and a word with the person who clicked, does. The goal is not to make staff afraid of email. It is to make the pause a habit, the two seconds to check the sender before the click, and to make reporting a suspicious message quick and free of blame. The person who clicked and said so within the hour has done the company a favor.

Where to start. A program, not an event: spotting phishing, handling passwords and data, what to do when something looks wrong. For every new hire, and at least yearly for everyone. Include the owner and the finance team by name; they are the ones attackers impersonate and target. A simulated phishing email every month or two shows whether the training took.

How we do it. Huntress security awareness training – short episodes every month, simulated phishing, and coaching for the person who clicked rather than a reprimand. We see who is due and who clicked, and follow up.

15 Know your vendors

CIS · SERVICE PROVIDER MANAGEMENT

● ○ ○ ○ ○ ○ ○ ○ IG1 · 1 OF 7

Sounds familiar? *"Our accountant's portal was hacked and we found out on LinkedIn."*

Why it matters. Anyone with access to your data or systems is part of your security. That includes your accountant, your software vendors, and us. A vendor's breach becomes yours when they hold your data or can sign in to your systems: the payroll service, the accountant's portal, the line-of-business application in the cloud, the IT provider with an administrator account. You cannot audit them all, but you can know who they are and ask them the questions your insurer asks you.

Where to start. A list of every service provider that holds your data or has access to your systems: what they hold, what they can reach, and who owns the relationship. Before signing with a new one, ask how they protect your data and what they would do in a breach. When a contract ends, remove their access the same week.

How we do it. We keep that list for you. We put ourselves at the top of it and answer the questions on page 23 in writing.

16 Software you had built

CIS · APPLICATION SOFTWARE SECURITY

○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ IG1 · 0 OF 14

Sounds familiar? *"The developer left, and nobody has the password to the server."*

Why it matters. No IG1 safeguards here either. But if you have had software written for you – a portal, an integration, an ordering system – it needs an owner, updates, and a plan for when the person who wrote it is gone.

Where to start. Nothing at IG1. Know what custom software you run, who maintains it, and where the credentials are.

How we do it. Much of what we install does not come in a box, because the software gets written. What we write is treated the way we treat what we buy: inventoried, patched, backed up, with the passwords and keys in a vault and not in somebody's head.

17 Have a plan for the bad day

CIS · INCIDENT RESPONSE MANAGEMENT

●●●○○○○○○ IG1 · 3 OF 9

Sounds familiar? *"Who do we call?"*

Why it matters. The first hour decides the cost. A plan is a page, not a binder – and it is on paper, because the day you need it the screens may be locked. Without one, the first hour goes on deciding who is in charge and finding phone numbers. With one, it goes on containing the problem. The plan also says who speaks for the company, so that a well-meant email to customers does not become the legal problem.

Where to start. One named person in charge. A contact list – your IT provider, insurer, attorney, bank – printed. A way for staff to report something odd without feeling foolish. Walk through it once a year with the people named in it, using a made-up incident: a locked server, a wire that went to the wrong account. Twenty minutes is enough to find the gaps.

How we do it. Every managed client has a one-page incident plan we write together at onboarding and go through at review. The first hour is on page 21.

18 Test it

CIS · PENETRATION TESTING

○○○○○ IG1 · 0 OF 5

Sounds familiar? *"We assume it works."*

Why it matters. No IG1 safeguards. Penetration testing – paying a specialist to try to break in – is for when the basics are in place. Buying it first buys a report that says "do the basics." Done at the right time, a test answers the question the scorecard cannot: not whether the controls exist, but whether they hold. It also gives your insurer and your larger customers the evidence they increasingly ask for.

Where to start. Nothing at IG1. Once IG1 is done, an external test once a year is a reasonable next step, and some insurers and customers ask for it. Ask for the findings in plain language, ranked by what an attacker would do first, and fix the top three before the next test.

How we do it. We arrange external testing through an independent partner and fix what it finds. We do not mark our own homework.

What your insurer will ask



The most useful checklist in the industry

The cyber insurance application has become the best short checklist there is, because a wrong answer voids the policy. These are the questions that appear on most applications, and where each one lands in this booklet.

THE APPLICATION ASKS	CONTROL
Is a second sign-in step (MFA) enforced on email, remote access and all administrator accounts?	05, 06
Is there attack-detection software (endpoint detection and response) on every device, monitored around the clock?	10
Are backups kept offline or unchangeable, separated from the network, and tested?	11
Is there security awareness training with phishing simulation?	14
Is email filtered, and is the DMARC record in place?	09
How quickly are critical vulnerabilities patched?	07
Do users have local administrator rights?	05
Is there a written incident response plan?	17
Is any software or operating system in use that its maker no longer supports?	02
Is there a verification procedure for wire transfers and changes to payment details?	Page 6
Are logs retained, and for how long?	08

Answer honestly. Insurers now check after a claim, and a "yes" that was not true is a claim that is not paid. If you cannot answer yes, that is where to start – not where to shade.

We fill these applications in with clients every renewal season. Bring the form.

Where the application lands on the eighteen controls

01 Assets	02 Software	03 Data	04 Config	05 Accounts	06 Access	07 Patching	08 Logs	09 Email & web
10 Malware	11 Backup	12 Network	13 Network watch	14 Training	15 Vendors	16 Custom software	17 Incident plan	18 Testing

Navy: the controls the application asks about. The wire-transfer question sits with pattern 1 on page 6.

New York rules that may already apply to you

Four sets of rules, who they reach, and which controls cover them

We are not attorneys and this page is not legal advice. It is a map of which rule tends to reach which kind of business, so your conversation with your attorney starts in the right place.

NY SHIELD Act

Reaches any business, anywhere, that holds private information about New York residents – customers, patients, employees. Requires reasonable administrative, technical and physical safeguards, scaled to the size of the business, and notification when private information is breached – within thirty days of discovery, under the amendment signed on 21 December 2024, with notice to the state as well, including the Department of Financial Services.

COVERED BY **03** Data p. 10 **05** Accounts p. 11 **08** Logs p. 12 **14** Training p. 15 **17** Incident plan p. 17

NYDFS Cybersecurity Regulation, Part 500

Reaches businesses licensed by the New York Department of Financial Services: banks, insurers, insurance agencies and brokers, mortgage lenders and brokers, money transmitters. Amended on 1 November 2023, with the last requirements in force from 1 November 2025: MFA for everyone who accesses its systems, with very few exceptions; a written asset inventory; notice of an incident within 72 hours; notice of any ransom payment within 24 hours; and an annual certification signed by the chief executive and the security officer, due each 15 April.

COVERED BY **01** Assets p. 9 **05** Accounts p. 11 **06** Access p. 11 **08** Logs p. 12 **17** Incident plan p. 17

HIPAA

Reaches medical, dental and mental-health practices, and every vendor that touches their patient data as a business associate. The Security Rule asks for a risk analysis, access controls, audit logs, encryption and breach notification. An update proposed in January 2025 would make MFA and encryption mandatory rather than "addressable". It was still not final when this booklet went to print. Expect it.

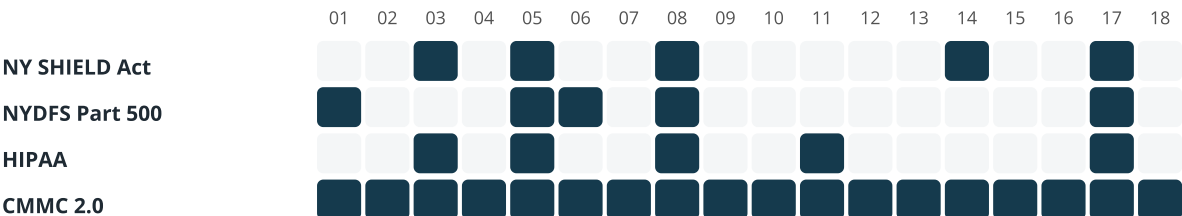
COVERED BY **03** Data p. 10 **05** Accounts p. 11 **08** Logs p. 12 **11** Backup p. 14 **17** Incident plan p. 17

CMMC 2.0

Reaches Department of Defense contractors and their subcontractors – including the machine shops, engineering firms and consultants on Long Island that never think of themselves as defense companies. Level 1 is fifteen requirements with an annual self-assessment, for federal contract information. Level 2 is 110 practices from NIST SP 800-171, mostly assessed by a third party, for controlled unclassified information. The program rule took effect on 16 December 2024 and the contract clause on 10 November 2025. IG1 covers a good part of Level 1. Level 2 is a project – and one to start before the contract that requires it, not after.

Compliance pages for each of the four are on our website, with what an engagement looks like.

Which controls each rule leans on CMMC Level 2 reaches all eighteen; the others map to the IG1 controls shown



Come to us before you implement AI. Not after.

AI AT WORK, BEFORE YOU SWITCH IT ON

The tool is not the risk. The data that goes into it is. Four things to settle before anyone in the office opens an AI assistant with company information in front of them.

- 1 Which tools, on which account.** On ChatGPT, a personal Free or Plus account trains on what it is given unless the user turns that off; the Business and Enterprise plans and the API do not, by default. Other vendors split the same way. Check the terms of the plan you are on, not the name of the product. Decide which tools are allowed and on whose account, and write it down.
- 2 What never goes in.** Client data. Payroll. Anything covered by HIPAA, the SHIELD Act or a contract. Anything you would not paste into an email to a stranger.
- 3 Permissions first.** Copilot in Microsoft 365 shows a person everything they already have access to. On most shared drives that is far more than it should be. Fix the drive before the assistant reads it – Control 03.
- 4 The verification rule.** No payment, credential or access change on the strength of a voice, a video or an email alone. AI made impersonation cheap. A call back on a known number makes it worthless.

How we do it. Our AI work is advisory before it is anything else: a conversation about what you want the tool to do, what data it would need, what the vendor's terms say, and what has to be true in your Microsoft 365 before it is safe. Then, if it still makes sense, the rollout.

PERSONAL ACCOUNT – FREE OR PLUS

Trains on what it is given

unless the user turns it off

SOURCE: OPENAI, HOW YOUR DATA IS USED TO IMPROVE MODEL PERFORMANCE. OTHER VENDORS SPLIT THE SAME WAY.

BUSINESS, ENTERPRISE OR THE API

Does not train on your data

by default – check the plan you are on

The first hour

If you think something is wrong. In this order.

- 1 **Disconnect, do not power off.** Pull the network cable or turn off Wi-Fi on the affected machine. Leave it running. Memory holds evidence that a restart erases.
- 2 **Call your IT provider.** Say what you saw, when, and on which machine. Our number is on the back cover.
- 3 **Do not pay, negotiate or reply to the attacker.** Not yet, and not without your attorney and insurer.
- 4 **Change the passwords that matter, from a clean device.** Email administrator, Microsoft 365 administrator, banking. Sign out every active session.
- 5 **Call your bank if money moved or was requested.** A wire can sometimes be recalled within hours. Rarely after.
- 6 **Notify your insurer.** Most policies require notice before any spending on the response.
- 7 **Write down what happened as it happens.** Times, names, what was clicked, who was told. This is the record your attorney, insurer and regulator will ask for.
- 8 **Do not announce it yet.** Notification obligations run on clocks. Your attorney decides what is said, to whom, and when.
- 9 **Report it to the FBI at ic3.gov.** It helps. In 2025 the FBI's Recovery Asset Team froze \$679 million of fraudulent transfers, a 58 percent success rate – when it was told in time.

Keep this page printed, with your provider's number, your insurer's claim line and your attorney's number written on it.

OUR IT PROVIDER

INSURER CLAIM LINE

ATTORNEY

Interactive AV-IT • 631.251.6300

Eighteen questions – score yourself

Ten minutes. One question per control. Tick the box when the answer is yes.

- 01 ☐ Do you have a list of every device on your network, updated in the last month?
- 02 ☐ Do you know every application in use, and is all of it still supported by its maker?
- 03 ☐ Is every laptop encrypted, and do you know where your sensitive data lives?
- 04 ☐ Do your firewall, Wi-Fi and servers have documented settings, with no default passwords left?
- 05 ☐ Does everyone work day to day without administrator rights?
- 06 ☐ Is a second sign-in step (MFA) required on email, on remote access, and on every administrator account?
- 07 ☐ Are operating systems and applications patched within a month of release, automatically?
- 08 ☐ Are logs for email, firewall and servers kept for at least ninety days?
- 09 ☐ Does your email domain tell the world to reject mail pretending to be you (DMARC at reject), and is web filtering on every device?
- 10 ☐ Is there attack-detection software on every computer, with someone acting on its alerts at night?
- 11 ☐ Have you restored a file from backup in the last three months, and is one copy out of reach?
- 12 ☐ Are guests, phones and AV on a separate network from servers and workstations?
- 13 ☐ Would anyone notice unusual traffic leaving your network? *(A second-level control – an empty box here is normal.)*
- 14 ☐ Has everyone had security training in the last twelve months, with simulated phishing?
- 15 ☐ Do you have a list of every vendor with access to your data, and what each can reach?
- 16 ☐ If you run software built for you, do you know who maintains it and hold the credentials? *(Tick it if you have none.)*
- 17 ☐ Is there a one-page incident plan, on paper, with the numbers to call?
- 18 ☐ Has anyone outside your team tested your defenses in the last year? *(A second-level control – an empty box here is normal.)*



Prefer your phone?

The same eighteen questions are on our website, with the counting done for you. Scan the code, or go to interactiveav.it.com/scorecard.

Feeling overwhelmed?

That is a normal reaction to eighteen questions. Reach out and we do this together – we set it up with you, or you book fifteen minutes and we start from your score.

What the count means

16 to 18 ticks. The basics are in place. What is left is specific to you: what your insurer asks for, what a regulator requires, or the second level of controls if you move large sums or hold sensitive data. That is a conversation, not a project.

10 to 15 ticks. Partly covered. Every empty box is an open door, and each one names a control. Turn to that control's page for the fix. Most businesses start here, and most of these fixes are settings and habits, not purchases.

Under 10 ticks. The doors are open. Do not try to close all eighteen at once. Four controls stop most of the money leaving: accounts (05), access (06), backup (11) and training (14). Do those first, in that order. It is a defined piece of work, not a permanent condition – and it is the situation we see most often.

How we work

Small on purpose

Interactive AV-IT has planned, built and managed technology for Long Island and New York City businesses since 2004. We support more than 950 people. Every new client gets a proper start, and clients stay – our longest client relationship goes back to 2002. Clients know their engineers by name.

Every client runs on our Recommended Technology Platform – the tools we use ourselves and know inside out. A managed service is not a project; it is a loop that runs every month: monitor, respond, maintain, report, review. We watch all of it – patching, the tested restore, who is due for training – and act on it. The numbers are there whenever you want them. Most clients would rather we simply handled it, and we do.

The name is the offer. The network, the security, the phones and the boardroom, supported by the same engineers. No vendor pointing at another vendor.

2004

in business since

950+

people we support

2002

our longest client
relationship, since

60

days to decide

Sixty days. Then decide.

If you are not satisfied after the first two months, tell us. We will refund your entire initial investment immediately – and pay you an additional \$1,000 for your time. No fine print. No questions.

Eight questions to ask any provider – including us

1. Who, by name, will work on my account, and how many clients do they carry?
2. Do you use MFA and a password manager internally, and can I see your own last phishing-test results?
3. What exactly do you back up for me, where does the offsite copy live, and when did you last restore from it?
4. What happens, step by step, at two in the morning on a Sunday when an alert fires on one of my machines?
5. What is not covered by the monthly fee? *Our answer: project work. It is quoted separately, every time.*
6. When did one of your clients last have an incident, and what did you change afterward?
7. What do you need from me every month for this to work?
8. How do I leave? What do I get back, and in what format?

A provider who cannot answer the last one quickly is telling you something.



interactive AV-IT
EMPOWERING THROUGH STRATEGIC TECHNOLOGY

Reach out

631.251.6300

hello@interactiveavit.com

interactiveavit.com

Interactive AV-IT
175 Commerce Drive, Suite O
Hauppauge, NY 11788

CYBERSECURITY ESSENTIALS FOR BUSINESS OWNERS · 2026 EDITION

Sources: FBI Internet Crime Complaint Center, 2025 Internet Crime Report (April 2026). Verizon 2026 Data Breach Investigations Report. NIST Cybersecurity Framework 2.0 (February 2024). CIS Critical Security Controls v8.1 (June 2024). Microsoft Learn, Windows 10 lifecycle and Office macro-blocking pages. New York Senate bill S2659B (2024). NYDFS 23 NYCRR Part 500, as amended 2023. HHS HIPAA Security Rule proposed rule (January 2025). 32 CFR Part 170 and DFARS 252.204-7021. OpenAI, How your data is used to improve model performance. The CIS Controls are a trademark of the Center for Internet Security; the control names are quoted, and everything else on those pages is ours.

This booklet is general information, not legal, insurance or accounting advice.