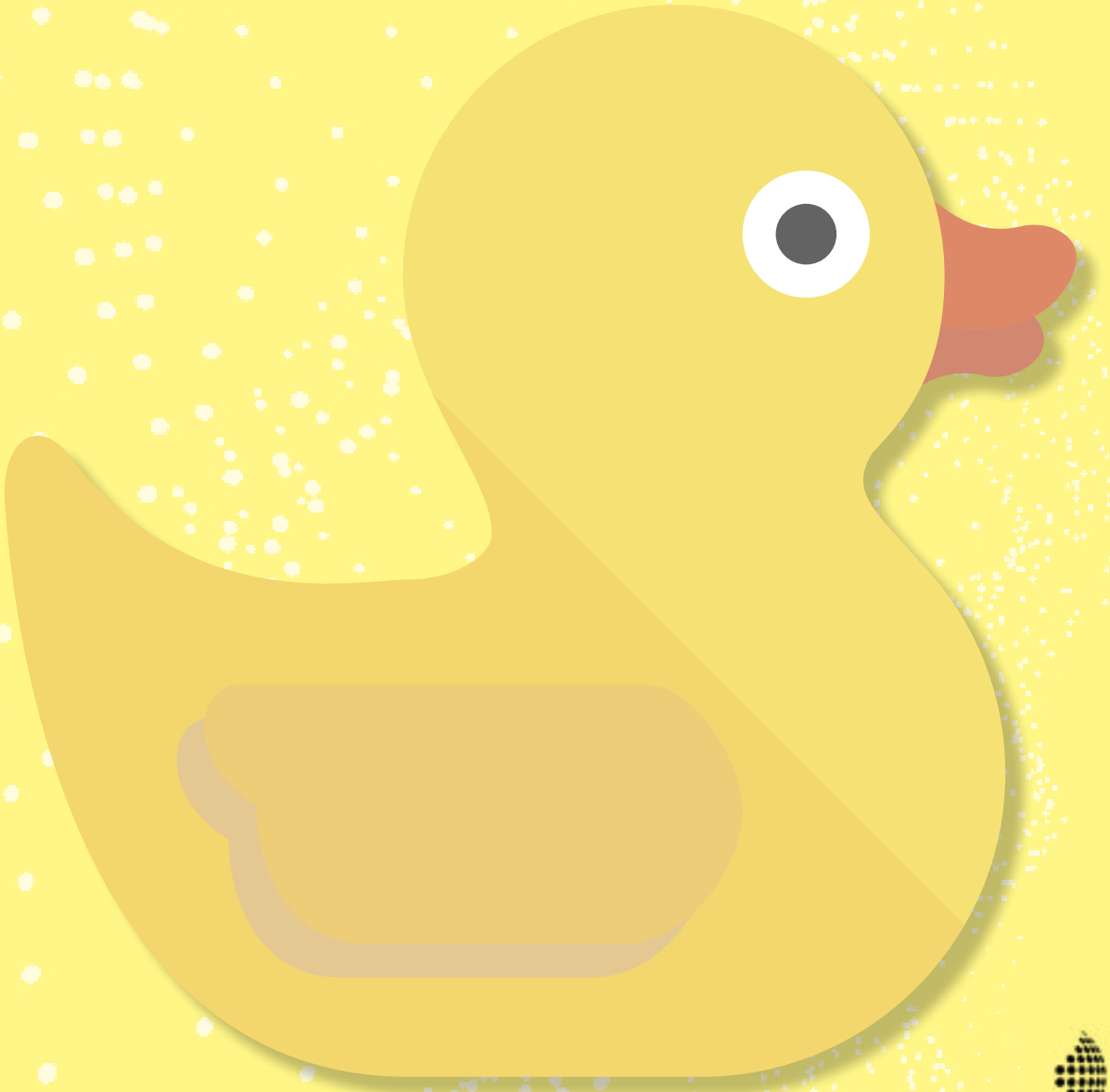
# The 7-Point Security Check

## Is Your Business a Sitting Duck?



Systems Support
IT Support & Service Since 1989

# Table of Contents




Systems Support
IT Support & Service Since 1989
www.systemsupport.com

462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

**From the Desk of William MacFee**
*CEO, Systems Support Corporation*

Dear Colleague,

If you run a small or midsized business, there is a good chance cybersecurity is one of those responsibilities you know matters but do not want to turn into a second job. You have employees to lead, customers to serve, projects to finish, and a business to run. You hired an IT person or provider, invested in software, and put reasonable protections in place because that is what responsible businesses do.

After more than 35 years supporting businesses across Greater Boston, the South Shore, and Southeastern Massachusetts, we have found that the hardest security question usually is not, “Do we have security?” Most organizations do. The harder question is, “How do I know the protections I am paying for are actually working the way I think they are?”

That is what this guide is for. It is not a technical manual, a compliance checklist, or an attempt to turn you into your own security engineer. It is a short set of questions we believe a business owner or manager should be able to ask and get a clear answer to. The questions are deliberately practical. They focus on the outcomes that matter to the business: who can get in, what happens when an employee receives a convincing fraudulent request, whether serious weaknesses are being fixed, whether every device is visible, whether the business can recover, who responds to an alert, and which outsiders still have access.

You may find that you can answer all seven confidently. That is useful reassurance. You may find one or two areas where the answer is, “I am not sure.” That is useful too. A question you know to ask is much easier to solve than an assumption nobody realized needed checking.

Our aim is simple: give you enough clarity to have a better conversation with the people responsible for your technology. If that conversation confirms everything is in good shape, excellent. If it uncovers something worth a closer look, you will know where to start.

Dedicated to serving you,

William MacFee,
CEO

Systems Support
IT Support & Service Since 1989
www.systemsupport.com
462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

# 0.0: Security Problems Don't Start with One Big Mistake

A normal office already has a surprising amount of technology protecting it. Microsoft 365 or Google Workspace. A firewall. Endpoint security. Backups. Laptops and mobile devices. Cloud applications. Remote access. A payroll system. A line-of-business application. Vendors that occasionally need access. Someone inside or outside the company responsible for keeping all of it running.

None of that sounds reckless. In fact, it sounds like a reasonably well-run modern business. The challenge is that security rarely fails because one company decided to do nothing. More often, a small exception or overlooked detail sits quietly inside an otherwise sensible environment: an old administrator account without MFA, a laptop that stopped checking in, a critical application nobody realized was exposed, a backup that has never been restored, or a vendor account that outlived the project that created it.

The stakes are real, but they do not need to be sensationalized. In 2024, 14,254 people and organizations in Massachusetts reported about $338.9 million in internet-crime losses to the FBI.1

That number is not here to suggest every business is one click away from disaster. It is here because cyber risk is now an ordinary business issue. It belongs in the same family as insurance, payroll controls, physical security, and business continuity: something worth understanding well enough to ask sensible questions about.

The goal of this report is not perfect security. Perfect security is not realistic. The goal is to make sure the basics are in place, the most consequential gaps are visible, and the business is not relying on assumptions where it should have clear answers.

**WHAT NORMAL LOOKS LIKE**
Most businesses already have security tools. The real question is whether the important protections cover the whole environment, whether exceptions are visible, and whether someone can show you the evidence when you ask.

# 0.1: The Most Common Attacks

In recent years, small and medium-sized businesses (SMBs) have increasingly found themselves in the cross-hairs of cybercriminals. According to a report from the Verizon 2024 Data Breach Investigations Report, 30% of all data breaches target small and medium-sized businesses (where data on organization size was available), highlighting that these organizations are often viewed as easier targets due to limited resources and cybersecurity measures. Furthermore, a survey by the National Cybersecurity Alliance found that 60% of SMBs that experience a cyberattack go out of business within six months.

The financial impact of such breaches can be staggering. The 2024 IBM Cost of a Data Breach Report revealed that the average cost of a data breach for businesses was approximately $4.88 million in 2024, a figure that can be crippling for organizations with limited financial buffers. Additionally, Symantec's 2024 Ransomware Threat Landscape Report indicated that 58% of malware attacks specifically targeted SMBs, emphasizing the tailored tactics used by cybercriminals.

These statistics illustrate not just the frequency of attacks but also the severe consequences that can follow. As cyber threats continue to evolve, the importance of a robust cybersecurity response plan becomes increasingly urgent for SMBs looking to protect their assets and ensure their survival in an ever-threatening digital landscape.

What are the threats that SMBs are facing from cybercriminals? Understanding the most common threats will help you craft your response and educate stakeholders on what to watch out for so they're less likely to make that one fateful click.

### PHISHING:

Phishing covers a broad range of attacks that all center around deceptive communication. The goal of the attack is to get recipients to reveal sensitive information (such as login credentials) or inject malicious software into a system. Email is the most common form of phishing but more developments in technology have given rise to an explosion of *ishing attack (e.g. "vishing" for phone calls or "smishing" with text messages). More than 31% of all incidents involved a phising attack at some stage according to the Verizon 2024 Data Breach Investigations Report.

### RANSOMWARE:

Ransomware is any malicious program that encrypts a target's files or network in order to deny access until a ransom is paid. While ransomware accounted for only 20% of cyberattacks (according to the IBM X-Force Threat Intelligence Index 2024), it's ability to do massive damage to operations has marked it as the most significant threat across most industries.

### DDOS ATTACKS:

A DDoS (Distributed Denial of Service Attack) attack is when multiple sources attempt to overwhelm a target's website or network with traffic, causing it to either crash or become impossible to use - think of it like an intentional traffic jam. DDoS attacks are often used as part of an extortion campaign, blocking a business's ability to operate without necessarily having to infiltrate its network.



Systems Support
IT Support & Service Since 1989
www.systemsupport.com
462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

# 0.2: The Consequences of Inadequate Response

Failing to implement a robust cybersecurity response plan can lead to serious consequences for businesses. The repercussions of such negligence are far-reaching, affecting not only the immediate financial health of the organization but also its long-term viability and reputation. These ramifications are magnified for SMBs, which often don' have the extra capacity to absorb significant financial or operational shocks created by cyberattacks.

***Financial Implications (losses, legal fees)***

Organizations that fall victim to cyberattacks often face crippling financial losses. According to the *IBM 2024 Cost of a Data Breach Report*, the average total cost of a data breach reached $4.88 million, with small businesses particularly vulnerable due to limited resources. Costs can include ransom payments, system recovery expenses, and the investment needed to restore operations.

In the aftermath of a breach, companies may incur significant legal fees, especially if they face lawsuits from affected customers or partners. Compliance violations related to data protection regulations (such as GDPR or HIPAA) can result in hefty fines, which can further strain financial resources. A report by the Ponemon Institute indicated that organizations could face an average of $1.1 million in regulatory fines post-breach.

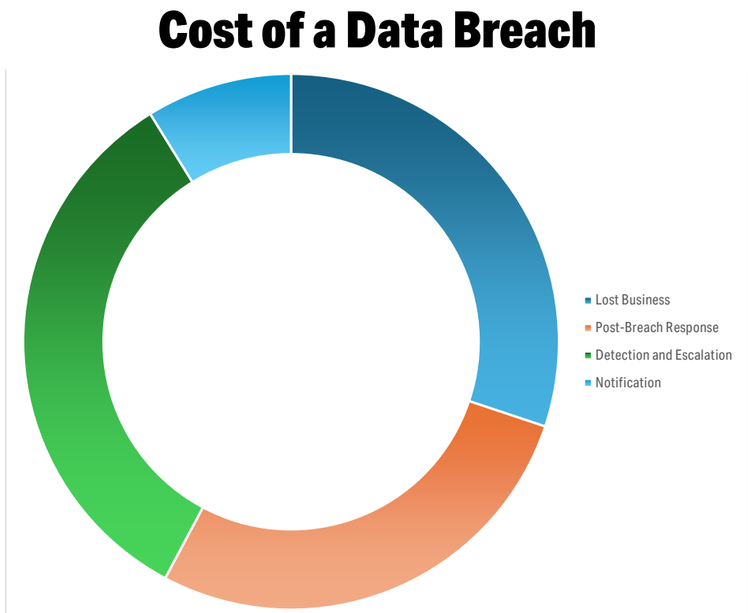
What would happen to your business if $5 million suddenly vanished from your accounts?

***Operational Disruptions (downtime, lost clients, lost partners)***

When we're talking about the impact of cyber-incidents, it's easy to focus on the bottom line figures but it's important to remember that businesses are often willing to pay all that money because the alternative is an ongoing operational disruption. What would happen at your business if the network went down? If employees were locked out of their devices? Or if your website were taken offline?

A Comparitech report estimates that organizations can experience an average of 18 days of downtime following a cyberattack, translating to lost revenue and productivity. For many small businesses, such disruptions can be catastrophic, sometimes leading to permanent closure.

The disruptions can echo long after the immediate impact of a cyber-incident. Long-term consequences of a breach might include the time and effort to sterilize or rebuild your infrastructure, or dealing with stepped up attacks because your business has been exposed as a vulnerable target.




*The average cost of a data-breach worldwide reached $4.88 million in 2024 (closer to $10 million in the United States) from $4.4 million in 2023. Lost business accounted for $1.47 million; detection and remediation cost $1.63 million; follow up, including regulatory fines, accounted for $1.35 million; and notifications cost approximately $430,000 on average.* IBM Cost of Data Breach Report 2024

***Reputational Damage (broken trust, long tail of reports)***

Perhaps the longest lasting impact of a breach is the hit to a business's reputation. Customers are increasingly concerned about how their data is handled; a breach can lead to a loss of trust that is difficult to regain. According to a 2023 PwC survey, 87% of consumers stated they would avoid a company following a data breach. For SMBs hit by an attack they could face an exodus of current clients and an uphill battle to replace them unless you make an extraordinary effort in reputation management.

A compromised reputation can also lead to strained relationships with partners and stakeholders. Trust is essential in business, and organizations may find it challenging to secure future collaborations or contracts if they are known for inadequate security practices.

With these factors in mind, it's not surprising that many SMBs will fail within six months of a significant cyberattack.

# 0.3: How to use the 7-Point Security Check

Each section starts with the same question used in the Sitting Duck Assessment. That consistency is intentional: the assessment gives you a quick gut check, while this guide gives you enough context to understand what the question is really testing.

For each point, look for three things: a clear answer, a sensible explanation, and evidence that matches the answer. You do not need screenshots of every configuration or a 50-page report. But if the answer is specific — who, what, when, how often — that is usually reassuring. If the answer is, "we should be covered" or "the tool handles that automatically," ask one more question.

The seven areas also line up closely with the practical cybersecurity fundamentals CISA emphasizes for small and midsized organizations: strong authentication, phishing resistance, software updates, logging, backups, and data protection.

**WHAT NORMAL LOOKS LIKE**
Most businesses already have security tools. The real question is whether the important protections cover the whole environment, whether exceptions are visible, and whether someone can show you the evidence when you ask.

# 1.0 Identity & MFA

**THE SECURITY CHECK**
**Are multifactor protections required for every employee, administrator, and remote access account?**

## Why this matters

Passwords get stolen. People reuse them. Phishing still works. The business question is not whether you have a strong password policy; it is whether a password by itself is enough to open an important door.

Coverage matters more than the checkbox. A company may have MFA enabled for Microsoft 365 and still have an old remote-access account, a line-of-business application, or an administrator or service account treated as an exception. The issue is not whether MFA exists somewhere. It is whether the exceptions are known, justified, and reviewed.

CISA recommends requiring MFA wherever possible, especially for remote and privileged access, and using the strongest practical method available, with phishing-resistant MFA preferred for higher-risk access.

I would also want to know what happens when roles change. New employees usually get access quickly; old access is the part that tends to linger. A clean process should remove former employees promptly, reduce privileges when someone changes jobs, and make it easy to identify who can administer important systems.

## What good looks like

- MFA is required for employees, administrators, remote access, and other important business systems.
- Administrator access is limited and kept separate from everyday user accounts.
- Former employees and stale accounts are removed promptly.
- The people responsible for security can review unusual sign-ins and identify current privileged users and approved exceptions.

**A USEFUL QUESTION TO ASK**
Can we review which accounts can still sign in without MFA and whether administrators are protected the same way as everyone else?

**A CLEAR ANSWER MIGHT SOUND LIKE**
**"Here is the current list. These two service accounts are the only exceptions, and here is why."**

# 02. Email & Phishing Protection

**THE SECURITY CHECK**
**Does your business have a consistent way to spot phishing, verify payment requests, and reduce the impact of email compromise?**

## Why this matters

No email filter catches everything. The dangerous messages are often the ones that fit the day: a payroll change just before cutoff, a supplier update during a busy job, a Microsoft sign-in notice, or an urgent request from an executive. Sometimes the message even comes from a real account that has already been compromised, so the sender name, conversation history, and business details all look legitimate.

That is why process matters as much as filtering. A change to banking information should be verified using a phone number or contact method already on file — not a number supplied in the email. An unexpected sign-in or password request should be checked through the normal support channel. Employees need an easy way to report a questionable message so IT can look for copies elsewhere and act quickly.

The aim is not to teach people to distrust every email. It is to slow down the relatively small number of requests where one rushed decision could change where money goes, expose an account, or interrupt the business.

**EASY TO OVERLOOK**
**A real mailbox can send a fraudulent message. If a vendor or customer account is compromised, an attacker may have real names, old invoices, project details, and prior email threads. For payment or account changes, verify through a trusted channel outside the message.**

## What good process looks like

- Email filtering and domain protections are configured and maintained.
- Employees know how to report a suspicious message without creating a support project.
- Payroll, banking, and vendor changes follow a verification process outside the original email.
- Unexpected sign-in activity can be identified and escalated to the people responsible for security.

**A USEFUL QUESTION TO ASK**
Can we review which accounts can still sign in without MFA and whether administrators are protected the same way as everyone else?

**A CLEAR ANSWER MIGHT SOUND LIKE**
**"Here is the current list. These two service accounts are the only exceptions, and here is why."**

# 03. Patching & Vulnerability Management

**THE SECURITY CHECK**
**Are internet-facing systems and critical software patched on a schedule that keeps serious vulnerabilities from lingering?**

## Why this matters

Most owners do not need a patch report. What matters is whether the systems that are easiest to reach are being kept current and whether known serious weaknesses are being fixed before they linger for weeks or months.

Automatic updates help, but they do not answer the whole question. Firewalls, remote-access tools, line-of-business applications, browsers, third-party software, and older servers can all fall outside the simple "Windows updated overnight" story. A good process starts with knowing what you have, then prioritizes what is exposed and what attackers are already using.

Not every missing patch carries the same business risk. What matters most is the age, severity, and exposure of the serious items. A useful conversation gets beyond a percentage such as "96% compliant" and explains what sits in the remaining four percent, which issues deserve priority, and what is being done about them.

Verizon's 2026 Data Breach Investigations Report found that 31% of breaches began with exploitation of software vulnerabilities.

## What matters most

- The organization maintains enough inventory to know which systems and software need attention.
- Internet-facing systems and known critical vulnerabilities get priority.
- Operating systems and common third-party applications are patched through a managed process.
- Vulnerability checks are used to identify important exposures that routine patching may miss.

**WHAT YOU SHOULD BE ABLE TO VERIFY**
**Which unpatched items carry the most risk right now, and are any of them exposed to the internet?**

**A CLEAR ANSWER IS SPECIFIC**
**"These are the three items we are tracking. None are externally exposed, and two are scheduled to be remediated this week."**

# 04. Endpoint Protection

**THE SECURITY CHECK**
**Can you confirm that every company laptop, desktop, and mobile device is managed, encrypted, and visible to your security tools?**

## Why this matters

A security tool is only useful on the devices it can actually see. Endpoint coverage is one of those areas that slowly drifts: a laptop is replaced but not retired, a remote employee keeps an older machine, a new hire starts on a temporary device, or a security agent stops checking in and nobody notices.

None of those situations is dramatic on its own, but together they create blind spots. A useful practice is to reconcile the list of company devices against what is actually reporting into management and security tools. That makes it possible to identify systems that are offline, unsupported, missing encryption, or assigned administrator rights that are no longer necessary.

Portable devices deserve extra attention because lost and stolen hardware is a very ordinary business problem. Encryption helps prevent a missing laptop from automatically becoming a data-exposure incident. The question is not simply, "Do we have endpoint protection?" It is, "Can you show me the devices that are outside the healthy majority, and what we are doing about them?"

**EASY TO OVERLOOK: PERSONAL DEVICES**
**Employees may access email, files, or business applications from phones and computers the company does not own. The useful question is not whether you formally allow BYOD. It is whether company information is currently sitting on devices you do not manage — and what happens to that information when a device is lost or an employee leaves.**

## What good coverage looks like

- Business computers are managed and visible to the people responsible for IT and security.
- Endpoint protection is installed and actively reporting.
- Encryption is enabled on laptops and other portable devices.
- Old, unsupported, missing, or unmanaged devices are identified and have a clear disposition.

**WORTH CONFIRMING**
**Which company devices are not currently reporting into our management or security systems, and what is the plan for them?**

**A CLEAR ANSWER MIGHT SOUND LIKE**
**"Two laptops have been offline for more than 30 days. We are confirming whether they are still in use and will remove or recover them."**

# 05. Backup & Recovery

**THE SECURITY CHECK**
**Can your business restore critical files and systems quickly because backups are tested on a regular schedule?**

## Why this matters

Most owners have heard the reassuring phrase, "We have backups." The more useful question is whether those backups have been tested and whether anyone has a realistic idea of how recovery would work when the pressure is on.

Backup is really two business questions: how much data can we afford to lose, and how long can we afford to be down? Those answers are different for every company. A file server, accounting system, practice-management application, production system, and email platform may all have different recovery priorities. The point is to decide the order before an outage forces the decision on you.

A green "backup successful" message proves that a job ran. It does not prove the data is complete, the credentials needed for recovery still work, or the business can rebuild systems in the right order. Meaningful restore tests close that gap: recover a file, mailbox, database, or application, confirm that it works, and record how long the recovery took.

Ransomware was involved in 48% of breaches analyzed in Verizon's 2026 DBIR, which is one reason recoverability deserves to be treated as a business capability rather than an IT checkbox.

**BACKUP IS NOT RECOVERY**

**A backup answers, "Do we have another copy?" Recovery answers, "Can we get the business working again, in the right order, in a timeframe we can live with?" You want both answers before an incident.**

## What recovery readiness looks like

- Critical data and systems are covered by a backup plan that reflects their importance to the business.
- Backup copies are protected from the same credentials and systems used day to day.
- Failures and capacity problems are monitored rather than discovered during an emergency.
- Restores are tested, and the business has realistic expectations for recovery before an incident.

**THE QUESTION THAT GETS TO RECOVERY**
**When was our last successful restore test, what did we restore, and how long did it take?**

**A CLEAR ANSWER MIGHT SOUND LIKE**
**"We restored a sample of production data last quarter. The test succeeded in 47 minutes, and we documented the result."**

# 06. Monitoring & Incident Response

**THE SECURITY CHECK**
**If a serious security alert appears overnight, is there a clear process for who sees it, who investigates it, and what happens next?**

## Why this matters

Buying tools is the easy part. Someone still has to notice the signal, decide whether it matters, and know what happens next. That is especially important when the office is closed and the normal chain of communication is not available.

Monitoring is useful when somebody is responsible for turning a signal into a decision. CISA's small-business guidance recommends collecting useful activity from important systems, centralizing logs where practical, setting alerts for higher-risk events, and assigning incident-response roles.6

For an owner, the practical part is escalation. If a login looks impossible, ransomware is detected, or an administrator account suddenly behaves differently, who has authority to act? Can the team disable an account or isolate a device without waiting for Monday morning? Who calls the owner? Who contacts cyber insurance, legal counsel, or a key vendor if the situation grows?

You do not need a binder full of procedures. You do want names, phone numbers, and a few decisions made in advance. A short tabletop discussion once or twice a year can expose surprisingly basic questions before the answers are needed under pressure.

## Who owns the next step?

- Important systems generate useful alerts that have a clear owner for review and follow-up.
- After-hours alerts have a defined escalation path and someone with authority to act.
- Key incident contacts and responsibilities are documented.
- The response process has been discussed or practiced so roles are familiar before a real emergency.

**A USEFUL SCENARIO TO WALK THROUGH**
**If an account were compromised at 2:00 a.m., who would know, who could act, and what would happen next?**

**A CLEAR RESPONSE MIGHT SOUND LIKE**
**"Our monitoring team gets the alert, can disable the account if the activity meets our threshold, and follows the escalation plan to contact you."**



## What Else You're Overlooking

The seven checks cover the fundamentals, but every business works a little differently. Depending on your industry, applications, workforce, customers, and contractual obligations, a few other areas may be worth keeping in the conversation with whoever helps manage your technology.

- **Personal devices and remote work:** What business information is accessible from devices the company does not own or manage?
- **Unapproved software and cloud applications:** Are employees storing files or doing business in applications nobody has reviewed, secured, or backed up?
- **Network and firewall configuration:** Who reviews the systems controlling what can enter or leave your network, and how often?
- **Employee onboarding and offboarding:** Is there a reliable process for giving people the access they need — and removing it when they leave or change roles?
- **Cloud data protection:** Which cloud services contain information you could not easily recreate, and what are the recovery options if that information is deleted, corrupted, or unavailable?
- **Cyber insurance requirements:** Are the security controls you represented to your insurer actually in place and documented?
- **Compliance and contractual requirements:** Do the type of data you handle or the customers you serve create additional security obligations?
- **Old systems and forgotten technology:** Are there aging servers, applications, accounts, or devices still connected because they are still doing a job and have never been formally retired?

**WORTH KEEPING IN VIEW**

**These do not change the 7-Point Security Check. They are common follow-up questions that may matter depending on your industry, workforce, applications, customers, and contractual obligations.**

Systems Support
IT Support & Service Since 1989
www.systemsupport.com
462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

# 07. Third-Party Access

**THE SECURITY CHECK**
**Do you know which outside vendors can access your systems or sensitive data, and is that access reviewed on a regular basis?**

## Why this matters

Most businesses depend on vendors, cloud services, contractors, and outside specialists. That is normal. The risk comes when access accumulates over time and nobody is quite sure who still has it — or why.

Your payroll provider, accountant, copier company, software vendor, outsourced specialist, or former consultant may all need some level of access. The problem is that access tends to outlive the project that justified it, especially when nobody inside the business clearly owns the relationship.

Verizon's 2026 DBIR reported third-party involvement in 48% of breaches in its dataset, which is a useful reminder that vendor access is part of your own security boundary, not somebody else's problem. A practical starting point is a simple list of the important outside parties, what they can reach, and who inside the business owns each relationship. Access should match the work being performed and be revisited when that work changes or ends.

The same principle applies internally: access should follow current responsibilities rather than accumulate indefinitely. This does not have to become a huge vendor-risk program. For most small and midsized businesses, knowing who has access, why they have it, and when it was last reviewed is already a meaningful improvement.

## Access Should Be Intentional

- Sensitive information is protected and access is based on what people actually need.
- Former employees and vendors are removed promptly.
- Outside access is documented and revisited as vendor relationships and projects change.
- Important third parties are known, along with the systems or data they need to reach.

**WORTH ASKING**
**Which vendors have active access today, what do they need it for, and when was that access last reviewed?**

**A CLEAR ANSWER MIGHT SOUND LIKE**
**"Here is the current vendor list, what each vendor can reach, who owns the relationship, and the date we last reviewed the access."**



# The 7-Point Security Check

Use this page as a conversation guide. The goal is not to grade your IT team. It is to help you advocate for the outcomes your business depends on, recognize where the answers are already clear, and identify where a follow-up conversation would be useful.

| Security Area | Yes | No | Unsure |
|---|---|---|---|
| **Identity & MFA** Are multifactor protections required for every employee, administrator, and remote access account? | ☐ | ☐ | ☐ |
| **Email & Phishing** Does your business have a consistent way to spot phishing, verify payment requests, and reduce the impact of email compromise? | ☐ | ☐ | ☐ |
| **Patching & Vulnerabilities** Are internet-facing systems and critical software patched on a schedule that keeps serious vulnerabilities from lingering? | ☐ | ☐ | ☐ |
| **Endpoint Protection** Can you confirm that every company laptop, desktop, and mobile device is managed, encrypted, and visible to your security tools? | ☐ | ☐ | ☐ |
| **Backup & Recovery** Can your business restore critical files and systems quickly because backups are tested on a regular schedule? | ☐ | ☐ | ☐ |
| **Monitoring & Response** If a serious security alert appears overnight, is there a clear process for who sees it, who investigates it, and what happens next? | ☐ | ☐ | ☐ |
| **Third-Party Access** Do you know which outside vendors can access your systems or sensitive data, and is that access reviewed on a regular basis? | ☐ | ☐ | ☐ |

**HOW TO USE THIS PAGE**
**A "Yes" is useful reassurance. "Not sure" is a prompt for a conversation. A "No" identifies an outcome the business should understand and prioritize. The objective is clarity and ownership, not a perfect score.**

Systems Support
IT Support & Service Since 1989
www.systemsupport.com
462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

## WHAT CRIMINALS WANT:

In the information age, data is a valuable currency and businesses often hold vast hoards. If you know what kinds of data criminals are looking for, you can better work to protect it inside of your system and mitigate risks.

**Personally-Identifiable Information (PII)** is the most common type of data stolen or compromised in cyberattacks. While the contents of PII will vary between industries even a home address and email can be valuable to bad actors who will in turn target victims for identity theft and other forms of fraud.

Even companies that don't collect a lot of consumer or customer data will still have **Employee PII**. Poorly secured HR systems could include demographic data, social security numbers, bank information, medical information, and even the results of background checks.

**Intellectual Property (IP)** is a prime target for attackers. It can be leveraged for all kinds of malicious purposes from selling it to competitors to extortion.

Enterprising criminals can also find opportunities with other corporate information like financial records and non-PII customer data. Don't assume that your business won't be a target just because you don't keep a lot of credit card numbers on file.

## SECURITY YOU CAN VERIFY

You hired people and invested in technology precisely so you would not have to manage every security setting yourself. That is sensible delegation. Running the business is your job; configuring security tools should not be.

Delegation works best when business leadership and the people responsible for technology share a clear understanding of the outcomes that matter. These seven questions give you a practical way to talk about those outcomes without needing to manage the underlying tools yourself.

If all seven answers are clear, you have useful reassurance. If one or two are uncertain, you have a focused place to start. And if several areas raise questions, that does not automatically mean something is wrong; it means the business would benefit from a broader conversation about priorities, ownership, and next steps.

**THE TAKEAWAY**
**You do not need to manage cybersecurity yourself. You do need to advocate for the outcomes your business depends on — and know who owns them.**

## WANT A SECOND SET OF EYES?

Systems Support helps small and midsized businesses across Greater Boston, the South Shore, and Southeastern Massachusetts keep technology secure, reliable, and understandable. From our Marshfield office, we help business leaders translate operational priorities into practical technology and security decisions — what matters most, what deserves attention now, and what can reasonably wait.

If this guide raised a question you want to explore — or you would simply like to talk through how the seven checks apply to your business — we would be happy to compare notes. A 15-minute Discovery Call is simply a conversation: tell us how your business works, what you are trying to protect, and where you would like more clarity. We can help you think through the next step and decide whether Systems Support is the right local partner to help.

**NEXT STEP**
**Book a 15-Minute Discovery Call**
**systemsupport.com/campaign/duck | 781-837-0069**



Systems Support
IT Support & Service Since 1989
www.systemsupport.com
462 Plain St, Suite 206
Marshfield, MA 02050
(781) 653-7916
info@systemsupport.com

Systems Support
IT Support & Service Since 1989