

PILLAR



How Businesses
Can Navigate
Cyber Threats
with Confidence

Security That Stays One Step Ahead

Pantheon's Advanced Security Package

Your data, your team, and your operations deserve protection that evolves with today's threats.



Cyber threats evolve every second - your protection should, too. Pantheon's Advanced Security Package delivers enterprise-grade defense designed to safeguard your business from every angle.



REAL-TIME THREAT MONITORING

Always-on visibility to detect and stop threats fast.



AI-POWERED INTRUSION DETECTION

Advanced intelligence to identify suspicious activity early.



ZERO-TRUST ACCESS CONTROLS

Limit access. Reduce risk. Protect what matters most.



AUTOMATED COMPLIANCE REPORTING

Simplify audits and stay compliant 24/7 with automated reports.



Upgrade to Pantheon's Advanced Security Package today.
Stronger protection. Smarter defense. Greater peace of mind.



More Information
www.pantheoncomputers.com



Our Phone
507-718-4288

FREE WEBINAR: **CYBERSECURITY IS A BUSINESS RISK. LEARN WHY SMBS ARE TARGETED — AND HOW TO STAY PROTECTED.**

Cybersecurity isn't just an IT issue — it's a business survival issue.

Small and mid-sized businesses are now the #1 target for cyberattacks, often because they lack the protections of larger enterprises.

In this educational webinar, our experts will break down why hackers actively target SMBs and what that means for your organization. You'll gain a clear understanding of today's threat landscape, how attacks actually happen, and the practical steps you can take to protect your business, your data, and your reputation.

Whether you're an executive, business owner, or team leader, this session will equip you with actionable insights and a straightforward approach to strengthening your security — without unnecessary complexity.

WHAT YOU'LL LEARN:

- Why small and mid-sized businesses are prime targets for cyberattacks
- The most common attack methods (phishing, ransomware, credential theft)
- The real cost of a breach — beyond just dollars
- Simple, high-impact ways to reduce your risk immediately
- How to build a practical cybersecurity strategy for your business

Date: Thursday, July 23, 2026
Time: 11:00 AM CST



In *this* Issue

Editor's Note: The Invisible Bullseye on Your Back — 5

Why small businesses and local governments are prime targets in today's cybercrime economy.

The Ease of Creating Malware in the Age of AI — 8

How AI and Malware-as-a-Service are lowering the barrier to cybercrime.

A Business Owner's Perspective on Cybersecurity — 11

Reyna Monson shares what cyber risk looks like from the owner's chair.

The Effect of AI on Spoofing and Other Cybercrime — 10

Why AI-powered scams are becoming harder to detect — and how to stay vigilant.

Your Money Is Insured. But Is It Safe? — 17

Why the FDIC treats cybersecurity as a critical part of financial safety.

Types of MFA: SMS Codes vs. Security Apps vs. Hardware Tokens vs. Biometrics — 22

A practical comparison of common multi-factor authentication methods.

The Dark Web: What Businesses Need to Know — 24

What the dark web is, why exposed credentials matter, and how monitoring helps.

Small Business Cyber Risks: Why the Colonial Pipeline Hack Matters — 25

What a major infrastructure attack taught cybercriminals about targeting smaller businesses.

Spoofing vs. Hacking: How to Tell the Difference — 29

A simple guide to understanding two common cyberattack tactics.

Social Engineering Is Not Always Obvious — 31

How attackers exploit trust, urgency, and familiarity to get inside organizations.

Cybersecurity Is Like an Onion — 35

Why strong cybersecurity depends on multiple layers working together.

Security by Layers: A Practical Cybersecurity Blueprint for Small and Medium-Sized Businesses — 36

A layered-defense framework for preventing, detecting, responding to, and recovering from attacks.

Cybersecurity Readiness Assessment: How Strong Are Your Security Layers? — 40

A practical checklist for evaluating your organization's security maturity.

How to Score Your Security Layers — 42

A guide to interpreting your readiness score and identifying priority gaps.

Your Biggest Security Vulnerability Is Already on the Payroll — 45

How employee awareness, reporting culture, and training reduce human risk.

The Deepfake That Almost Fooled Me — 50

A personal lesson on verifying unusual requests in the age of AI-generated voices.

Cybersecurity Word Search — 51

Our Core Values — 52

Client Testimonials — 53

About Us — 54

Your Go-To Cybersecurity Resource List — 56



The Invisible Bullseye on Your Back

Why small businesses and local governments are the most sought-after targets in today's organized cybercrime economy — and what you can do right now.



Editor's Note

There is a persistent myth in the small-business world — one that cybercriminals are counting on you to believe: *"I'm too small to be a target."* It is one of the most dangerous assumptions a business owner or municipal administrator can make today, and the organized criminal syndicates operating across Eastern Europe, Southeast Asia and beyond are banking on it.

The truth, documented repeatedly by the FBI's Cyber Division, is precisely the opposite. Small and mid-sized businesses are not too small to attract attention — they are **the preferred target**. Larger enterprises invest heavily in dedicated security operations and enterprise-grade defenses. SMBs, by contrast, often run end-of-life operating systems, skip monthly patching cycles, and rely on legacy antivirus software that was never designed to detect the AI-driven, polymorphic threats now deployed at scale. To a professional threat actor, that combination is an open door — and they walk through it thousands of times a day.

Hacking Is Now a Business — and You Are the Market

This is not the stuff of movie villains or lone-wolf hackers in dark basements. The cyber threat landscape the FBI describes today is one of fully professionalized criminal enterprises, complete with HR departments, tech teams that probe millions of endpoints simultaneously, and a customer-support desk to collect ransom payments in cryptocurrency — all while operating safely beyond the reach of U.S. law enforcement.

Jill Stagman
Editor-in-Chief

***Pillar
Magazine***

Their business model is simple: volume and vulnerability. They are not looking for the hardest target — they are looking for the easiest one. An SMB running Windows 10 past end-of-support, without advanced endpoint detection and response (EDR), without multi-factor authentication, without a tested backup strategy? That is not a business they have to “hack.” That is a business they simply walk into.

A Special Word to Compliance-Governed Organizations

If your organization operates under HIPAA, CJIS, FDIC, CMMC, or any other compliance framework, this conversation is even more urgent — and we understand it can feel like a trap. Many organizations quietly avoid initiating a formal audit or gap assessment because they know they are not where they should be, and they fear that surfacing those gaps will invite regulatory fines, public disclosure, or worse.

We hear that fear regularly, and we want to offer some important perspective: the fines and reputational damage that follow a breach are almost universally greater than the remediation cost of addressing gaps proactively. Regulators exist not to punish organizations that are working in good faith toward compliance, but to hold accountable those who ignore it entirely. The organization that begins its compliance journey today — that partners with a qualified MSP, documents its remediation plan, and makes measurable progress — is in a fundamentally different posture than the one that suffers a breach while still running unpatched systems.

When Your Community Loses Power, Water, or More

The cyber threat does not stop at the office door. Municipal infrastructure — water treatment facilities, electrical grid management systems, traffic and street-lighting networks, emergency dispatch — is increasingly connected, increasingly internet-accessible, and increasingly in the crosshairs. Right here in Minnesota, we have seen this play out in painful detail.

Ransomware attacks have disrupted county governments, forced cities to operate on paper for weeks, and exposed sensitive public records — from criminal justice files to public health data. In several cases, small Minnesota municipalities paid ransoms simply because they had no other path to restoring operations. The lesson is not that these communities were careless. It is that they were underprepared for a threat that has outpaced the resources of any single IT administrator working alone.

When street lights go dark, when water-pressure monitors go offline, when a county's 911 dispatch system freezes — the impact is not abstract. It is immediate, it is physical, and in the worst cases, it endangers lives. These are not hypothetical scenarios. They are documented incidents and the FBI has been explicit: attacks on critical infrastructure are accelerating, and local governments with limited IT resources are among the most exposed.

The Good News: This Is a Solvable Problem

We do not want to leave you with only a sense of alarm — because the other truth about cybersecurity in 2026 is that organizations of every size can build strong, layered defenses. They simply cannot do it alone, with one stretched IT generalist, or by relying on tools designed for a threat landscape that no longer exists.

A qualified managed services provider brings what most SMBs and municipalities cannot build internally: 24/7 monitoring, modern endpoint detection and response, current patch management programs, compliance-aligned security frameworks, and the institutional knowledge that comes from protecting dozens of organizations simultaneously. It is not a luxury. In 2026, it is the baseline.

This quarter's issue of Pillar is dedicated to giving you the clearest possible picture of the threat environment, the regulatory landscape, and the practical steps your organization can begin taking today. Read it with your leadership team. Share it with your board. And if questions arise about your own security posture, we hope you'll reach out — not with anxiety, but with the confidence that solutions exist and that you don't have to figure this out alone.



PASSWORD MANAGEMENT
Powered by Kaseya

Your Passwords Should Not Be the Weak Link.

Password Managers help your team store, manage, and share passwords securely - without sticky notes, spreadsheets, or risky sharing.

**Ask Pantheon about password
management today**

SECURE ACCESS



**Password security
made simpler.**

NO STICKY NOTES

NO SPREADSHEETS

NO RISKY SHARING

THE EASE OF CREATING MALWARE IN THE AGE OF AI

AI is lowering the barrier to entry for cybercrime. What once required deep technical expertise can now be automated, outsourced, or generated in seconds—making attacks more accessible than ever.



FROM “EXPERTS ONLY” TO “ACCESSIBLE FOR ALL”

Not long ago, creating malware required significant technical skill and time.

THEN



Advanced programming and system knowledge



Weeks or months to develop tools



Limited to skilled hackers or organized groups



NOW



AI assists with code generation, debugging, and automation



Malware-as-a-Service makes tools available via subscription



Anyone with intent can launch attacks



AI doesn't create more sophisticated hackers - it creates more hackers.

Artificial intelligence is rapidly changing the cybercrime landscape. AI has not necessarily created more sophisticated hackers, but it has dramatically lowered the barrier to entry. Combined with the growing Malware-as-a-Service economy - where underground marketplaces offer ransomware kits, phishing platforms, and credential theft tools through subscription-style services - cybercrime has never been more accessible.

HOW AI IS MAKING MALWARE EASIER, FASTER, AND MORE CONVINCING

AI makes malware operations easier mostly by lowering skill barriers, increasing speed, and improving deception, rather than by magically inventing brand-new attacks.

FASTER CODE WRITING AND DEBUGGING

Attackers can use AI to draft scripts, troubleshoot errors, port code between languages, or modify existing malware-like tooling. This can help less-skilled actors produce working components faster.

MALWARE VARIATION AT SCALE

AI can help rewrite or restructure code, change strings, generate configuration variants, or produce many slightly different samples. That can make signature-based detection harder, even when the underlying behavior is not novel.

PERSONALIZED TARGETING

Attackers can summarize public information about a victim or company and generate tailored lures, fake invoices, job messages, vendor impersonation emails, or executive-style requests.

AUTOMATED RECONNAISSANCE

AI can help summarize leaked documents, public websites, GitHub repos, job postings, and employee profiles to identify technologies, vendors, likely usernames, or weak points.



ASSISTANCE WITH EVASION CONCEPTS

At a high level, AI can suggest ways to alter behavior, packaging, wording, or delivery flows so malicious activity looks less suspicious. Defenders should assume AI can help attackers iterate quickly, even if the core techniques remain familiar.

SCAM INFRASTRUCTURE GENERATION

Generative AI can create fake landing pages, brand impersonation content, chatbot scripts, and translation/localization for campaigns. Recent reporting has noted attackers abusing AI-brand impersonation and AI-generated phishing/scam content at scale.



The real danger of AI in cybercrime is not that it replaces skilled hackers - it enables far more people to become effective ones. As artificial intelligence continues to evolve, businesses must strengthen defenses, verify identities, and stay ahead of faster, more convincing, and more accessible threats.



vCIO SERVICES

STRATEGIC TECHNOLOGY LEADERSHIP
FOR WHAT'S NEXT.

Executive-level technology leadership without the cost of a full-time CIO. We help organizations align technology with business goals, reduce risk, control costs, and plan for the future.



**REAL LEADERSHIP.
REAL RESULTS.**



REDUCE RISK

Proactive oversight and governance help prevent expensive surprises.



CONTROL COSTS

Better planning, vendor management, and cost optimization save money.



PLAN AHEAD

Roadmaps and lifecycle planning keep you ahead of the curve.



GAIN CLARITY

Scorecards and reporting give you visibility and confidence.



STRENGTHEN SECURITY

Risk management and compliance guidance keep your business protected.

WHAT YOU GET WITH vCIO SERVICES



STRATEGIC PLANNING & ROADMAPS

3-year roadmaps, quarterly reviews, and initiative prioritization aligned to your business goals.



IT OVERSIGHT & ACCOUNTABILITY

SLA oversight, escalation management, change-control governance, and executive scorecards.



AI & AUTOMATION GUIDANCE

AI governance, automation planning, business intelligence prioritization, and technology alignment.



CYBERSECURITY & RISK OVERSIGHT

Top-10 risk register, security governance, compliance readiness, and incident response planning.



BUDGETING & VENDOR MANAGEMENT

IT budgeting support, vendor reviews, renewal tracking, and cost optimization recommendations.



EXECUTIVE COLLABORATION & REPORTING

Monthly scorecards, leadership reviews, and evidence-based reporting for informed decisions.

LET'S PLAN YOUR TECHNOLOGY FUTURE.



Schedule a strategy session to learn how vCIO Services can help your organization thrive.

LET'S CONNECT.



507 - 718 - 4288



pantheoncomputers.com



contact@pantheoncomputers.com

A BUSINESS OWNER'S PERSPECTIVE ON CYBERSECURITY:

What Actually Keeps Me Up at Night

“

At some point, you stop thinking about cybersecurity as a technical checklist and start seeing it for what it is: **business survival.**



By Reyna Monson
Co-Owner & President





Cybersecurity isn't theoretical when you own a business.

It's not a question of if something will happen—it's a question of when.

And it's not really an IT problem. Because the risks aren't abstract—they're personal.

You wonder:

- Will I have to tell my clients that my company exposed their data, damaging my reputation in the process?
- Will I be staring at a ransom demand, wondering if I can even afford to get my business back?
- How long would we be down—and how much revenue would we lose while we can't operate?
- If I can't make payroll, will my team stick with me?
- Could all the time and effort I put into this business—my legacy, my retirement—end up being for nothing?

At some point, you stop thinking about cybersecurity as a list of tools the IT department uses and start seeing it for what it is: protecting your future.

That shift changes how you approach everything.

Ultimately, cybersecurity is about risk management. What level of risk are you, as a business owner, comfortable with? Recently a prospective client told me that what Pantheon is really selling is insurance. Not literal insurance, obviously – but protection, risk reduction, and the ability to sleep at night. And he wasn't wrong.

How much coverage do you want? How much inconvenience are you willing to tolerate due to cyber security tools and practices? What are you willing to spend? What will it take to make you sleep soundly at night?

Here are some of the things I've done so I'm not staring at the ceiling at 2 am:

1. I made sure my cybersecurity insurance was actually right. Not "I think it's fine"—actually right. I had a specialist review it, not my general agent. No shade on him, (he's great at what he does) but this is a different level and kind of risk. Turns out I had a strong policy. But I didn't know that before, and that's a problem. This coverage is as critical as E&O or General Liability, and it deserves that level of attention.

2. I treat vendors like a potential risk, because they are. Every vendor is a possible entry point into your business. So, I ask questions. A lot of them. What security do you have? What's your disaster recovery plan? How do you vet your people? Then I read the contracts carefully, because I don't want to be responsible for someone else's mistake. I document everything and keep it updated. "We assumed they had it covered" is not a strategy.

3. I spend time planning for risks I can't control, and there is so much that is out of my control. What happens if a major cloud provider goes down? What if backups fail? What if a major service gets hit – like the banking system or Microsoft or the electrical grid? Realistically, I can't prevent any of these from happening, but I can decide ahead of time how we will respond. We've walked through those scenarios so we're not making decisions under pressure.

In some cases, that means taking extra precautions. For example, I export and store a quarterly backup of our QuickBooks Online data on an encrypted device. Hidden.

Where is it? Nice try.

4. I've also locked down how money moves in the business. If funds are leaving my accounts, it's not happening easily. There are approvals, separation of duties, and verification steps built in. The person initiating a transaction is not the one approving it, because once money is gone, it's usually gone – and I've seen how fast that can happen.

None of these remove all my risk. None of them are foolproof.



The point is, we've thought it through - not perfectly, but intentionally.

And when the planning isn't there - or the protections you've chosen don't work - I've seen exactly what happens.

I had a client wire out \$250,000 to criminals pretending to be their boss. They were lucky (the bank flagged it and stopped most of it) but \$50,000 was gone. Another client wired \$40,000 and never recovered a dollar.

These things happen. You can't control that. There are way too many factors involved - including the human ones.

I once had to convince Target to take back a stack of Apple gift cards. I don't ever want to do that again.

Losing money is bad. Losing all control over your business is worse.

I was onboarding a client when they got hit with ransomware. We had just started working together and were in an overlap period—their previous provider was still responsible for backups. Unfortunately, those backups weren't properly protected, and the cloud backups hadn't run in months. When the attack hit, everything—including the backup—was encrypted.

They were asked to pay \$40,000 in cryptocurrency, and they felt like they had no choice.

Even after paying and getting the decryption key, it took a week to get them operational again.

They lost tens of thousands in revenue—and missed payroll. They were able to recover quickly after that, but the damage—to operations, to morale, to trust—was real.

That's not just a tech issue. That's a business crisis.

Like a lot of business owners, I have teeny-tiny control issue. So, the idea that I could lose complete control of my business is the scariest part of cyber risk for me.

Because the truth is, I can't control when or how my business might be attacked by a cybercriminal.

I hate that.

But I have to accept it. You can't own or run a business without risk. It's inherent. But accepting that risks exist is not the same as throwing up your hands. You have to move on to mitigation.

Start with the risks you can see. Review your insurance. Question your vendors. Protect how money moves. Know how you would recover if systems went down. And get help where you need it, because IT is hard and cybersecurity is harder.





Cybersecurity isn't about finding the perfect tool or checking a box. It's about layers, discipline, and consistency.

It's about doing the uncomfortable work ahead of time so you're not making impossible decisions in the moment.



Because the real risk isn't just getting hacked.

It's what happens to your business when you do.

THE EFFECT OF AI ON SPOOFING AND OTHER CYBERCRIME

Artificial intelligence is a powerful ally - but in the wrong hands, it becomes a sophisticated weapon.



WHY AI MAKES SPOOFING HARDER TO SPOT

Scams may no longer sound awkward or look suspicious. AI can make messages polished, personal and urgent - which is why verification matters more than ever.

THE THREAT

Voice manipulation can convincingly mimic family members, coworkers or trusted contacts. Victims may be pushed to send money for fuel, repairs or emergency help - sometimes under pressure or aggression.

PERSONALIZED AT SCALE

AI makes it feasible to search public posts, breached data and past details to tailor messages. A scam that names a real person, workplace or recent event feels more believable.

VOICE & VIDEO AREN'T PROOF

A familiar voice, caller ID or video clip can be faked. Hang up and reconnect using a saved number or trusted app before sending money, passwords or codes.

POLISHED PHISHING

Generative AI can remove poor grammar and awkward phrasing. Emails and texts may look professional, urgent and tailored to your account.

FALSE LEGITIMACY

AI makes it much easier to create websites, social media pages, press releases, etc. to make their scams seem more legitimate.

STAY VIGILANT

A familiar voice, caller ID or message is not enough. Pause before you respond.

- Confirm through a known number
- Use a secret code or safe word
- Never share one-time codes or passwords.



Trust your instincts.
Verify the facts.
Protect what matters.

THE BOTTOM LINE

This is an arms race: criminals use AI to deceive, while security teams use AI to defend. As scams become more realistic, protection depends on slowing down and verifying identity through a channel you control.

YOUR MONEY IS INSURED. BUT IS IT SAFE?

Why the FDIC takes cybersecurity just as seriously as it takes your bank balance - and what that means for your financial life.

Most people know that the FDIC insures their bank deposits. If your bank collapses, you get your money back - up to \$250,000. It is one of the most reassuring promises in American financial life, and it has worked reliably since 1933.

But here is something fewer people think about: What if a criminal does not need your bank to collapse? What if they can simply steal your money - or your identity - while your bank is still open and running? That is the threat that cybercrime poses to the modern banking system, and it is why the FDIC has made cybersecurity one of its most urgent priorities.



By: Josh Burston
Senior Security Analyst

BY THE NUMBERS



Financial institutions are among the most targeted organizations in the world for cyberattacks. According to federal data, the banking sector experiences many significant cyber incidents every year.

.....

A single successful attack on a mid-sized bank can expose tens of thousands of customers to fraud, identity theft, and financial loss - sometimes before anyone even realizes what happened.



Insurance Protects Your Money. Cybersecurity Protects Your Information.

FDIC deposit insurance is designed for a specific scenario: a bank that becomes insolvent and cannot pay its depositors. It is a financial safety net, and it is a good one. But it was not designed to protect you from a hacker who steals your account credentials and drains your savings, a criminal who intercepts your banking information and opens fraudulent accounts in your name, or a cyberattack that locks a bank out of its own systems for days, preventing you from accessing your money at all.

These are real, modern threats - and they require a different kind of protection. When your money is stolen via cybercrime, the FDIC will not replace it. That is why banks have cybersecurity standards that they are required to follow.



What the FDIC Requires Banks to Do

The FDIC does not just insure deposits - it examines banks regularly to make sure they are operating safely. In recent years, cybersecurity has become a central part of those examinations. Banks are now expected to maintain strong defenses against digital threats, respond quickly when something goes wrong and be transparent with regulators and customers when a breach occurs.

Specifically, the FDIC requires banks to:



Protect customer data using encryption and access controls so that sensitive information cannot be easily read or stolen.



Monitor their systems around the clock for signs of unusual or suspicious activity.



Have a tested plan in place for responding to a cyberattack - not just a document on a shelf, but a practiced, real-world response capability.



Report significant cybersecurity incidents to the FDIC within **36 hours** - one of the **strictest notification** timelines of any industry in the country.



Ensure that **outside technology companies** the bank relies on are also following strong security practices.

The last point is particularly important. Modern banks depend on dozens of outside vendors - companies that manage software, store data, and run the digital infrastructure that keeps banking working. The FDIC holds banks responsible for the security practices of those vendors, which creates a chain of accountability that extends far beyond the bank's front door.

The 36-Hour Rule

In 2022, the FDIC introduced a rule requiring banks to notify regulators within 36 hours of discovering a significant cybersecurity incident. This is one of the fastest mandatory reporting timelines in any regulated industry.

The goal is simple: get regulators involved quickly so they can help contain damage, coordinate responses, and protect customers before a bad situation becomes catastrophic.





Why This Matters to Everyday Customers

When you hand your financial information to a bank, you are placing a significant amount of trust in that institution. You trust that your account number, your Social Security number, your transaction history, and your personal details will be kept private and secure. The FDIC's cybersecurity requirements are the regulatory backbone that enforces that trust.

Without these rules, banks would face no uniform standard for how well they must protect your data. Some would invest heavily in security; other might cut corners to save money. The FDIC's oversight levels the playing field and sets a minimum bar that every insured institution must clear.

It also means that if a bank fails to meet those standards, there are real consequences - fines, required improvements, and in serious cases, regulatory action that can affect the bank's ability to operate. Those consequences create a powerful incentive for banks to take cybersecurity seriously, not just because it is the right thing to do, but because the regulator is watching.



The Bottom Line

Your bank deposits are insured against financial collapse. But in today's world, the bigger everyday risk is not your bank going out of business - it is criminals trying to access your account, steal your identity, or disrupt the systems your bank depends on.

The FDIC understands this, which is why cybersecurity is no longer a side topic in banking regulation. It sits at the center of how regulators evaluate whether a bank is truly safe. For customers, that means your bank is not just being watched for financial health - it is being held accountable for keeping your digital life secure as well.

The next time you log in to your banking app without incident, or get an alert that someone tried to access your account and was stopped, that seamless protection is not an accident. It is the result of regulations, standards, and oversight working exactly as intended.

Types of MFA:

SMS Codes vs Security Apps vs Hardware Tokens vs Biometrics

By Nick Beach

Just a quick refresher regarding multi-factor authentication. It is a security mechanism that forces users to use multiple forms to prove who they are before gaining access to an account or system.

The primary types of this are the following:



Something you know, such as passwords.



Something you have, smart phone apps, text messages, hardware token.



Something you are, like fingerprints, facial recognition or retina scans.



56%

of all compromises in Q1 of 2025 directly resulted from the theft of a valid account's credentials not using MFA.

-According to Rapid7, a global cybersecurity company

In each section I am going to go over the MFA options and give you some pros and cons. Even the worst of these will vastly improve your security over not having any but some are better than others. I think in large part it comes down to the age old issue of security versus usability where we want to make this as secure as possible but not so much that normal users can't get to what they need for their job.





SMS / Text Codes

According to a 2023 survey, 77% of people using MFA are using SMS text codes. It's easy to use, requires no installation, and works on any phone.

PROS

- ✓ Ease of use
- ✓ No additional install

CONS

- ✗ Vulnerable to passcode interception during transmission
- ✗ SIM swapping can be used by attackers to take control of the number
- ✗ Tied to a physical device that can be stolen, lost, or broken



Security Apps

Apps like Google Authenticator or DUO Mobile generate time-based passcodes when you log in.

PROS

- ✓ Encrypted tunnels and codes that change quickly
- ✓ Available offline
- ✓ Free to use
- ✓ Convenient for managing multiple accounts

CONS

- ✗ Requires smartphone or dedicated device
- ✗ If an attacker gains access to the app, it can be devastating
- ✗ Can be challenging for some users



Hardware Tokens

A physical device (USB or Bluetooth) that verifies your identity by completing a digital challenge. Great for users who don't want apps on their phones. *Monthly fee may apply.*

PROS

- ✓ Immune to man-in-the-middle attacks
- ✓ Not vulnerable to social engineering
- ✓ Works across websites and various apps

CONS

- ✗ Costs \$40-\$100+ depending on features and brand
- ✗ Loss of key can result in lockout if no backup
- ✗ Requires the physical device to be with you



Biometrics

Uses unique physical traits like fingerprints or facial recognition to verify identity. Built into many modern devices.

PROS

- ✓ Very convenient and quick to use
- ✓ Difficult to steal or replicate
- ✓ No extra device or app needed in most cases

CONS

- ✗ Not foolproof - can be spoofed with advanced tools
- ✗ May not work in all environments or with all devices
- ✗ Privacy concerns for some users



THE TAKEAWAY

There's no one-size-fits-all solution. The best MFA method balances security, usability, and your environment's needs. The key is to use something-anything-over nothing.

STRONGER AUTHENTICATION. STRONGER PROTECTION.

THE DARK WEB: WHAT BUSINESSES NEED TO KNOW

Most people have heard the term “dark web,” but it is often made to sound more mysterious than it really is. The dark web is real – and it does present risks. Understanding what it is can help you protect what matters most: your business.



1. THE SURFACE WEB

The part of the internet we use every day. These are websites and pages that search engines like Google and Bing can find.



2. THE DEEP WEB

The majority of online content – private or protected information like banking, medical portals, business systems, emails, and government resources. We use it every day without even thinking about it.



3. THE DARK WEB

A small, hidden part of the internet that requires special tools to access. It's where cybercriminals buy, sell, and trade stolen information.



WHY BUSINESSES SHOULD BE CONCERNED

Stolen credentials from phishing, malware, data breaches, or password reuse can end up on the dark web.

EXPOSED INFORMATION MAY INCLUDE:



Employee email addresses



Microsoft 365 and other account logins



VPN and remote access credentials



Banking and financial information



Business application and system accounts



Passwords

Most businesses don't know their information has been exposed until something happens. Criminals can take leaked credentials and try them against email, cloud services, financial systems, and more.

Dark Web Monitoring is not a replacement for strong passwords, multi-factor authentication, employee training, endpoint protection, or regular security reviews.

But it does give you visibility into a problem you may not otherwise know exists.

THE POWER OF DARK WEB MONITORING

Dark Web Monitoring watches for exposed credentials and sensitive information tied to your business. When a match is found, you are alerted so you can:



Be Alerted



Take Action



Reduce Risk



The dark web may be hidden, but the risk doesn't have to be.

Knowing when your information has been exposed gives you a chance to act before criminals use it against you.

SMALL BUSINESS CYBER RISKS

WHY THE COLONIAL PIPELINE HACK MATTERS

When most people think about the Colonial Pipeline hack, they remember gas shortages, long lines, panic buying, and a major piece of American infrastructure getting shut down.

And yes, that was a big deal.

But if you own a small business, the bigger lesson is what happened afterward - and how it changed the way cybercriminals thought about risk.



PREPARE. PROTECT. PREVAIL.

Strengthening today.
Securing tomorrow.



BIG ATTACKS BRING BIG ATTENTION

Colonial Pipeline was a wake up call – but not only for large companies.

In May 2021, Colonial Pipeline was hit by a ransomware attack. The company shut down operations for several days, causing fuel shortages across parts of the East Coast.

Then everyone got involved: the FBI, CISA, the Department of Justice, even the White House. Law enforcement tracked the money, recovered part of the ransom, and put serious pressure on the group connected to the attack.

That group, DarkSide, claimed it was shutting down shortly after. For the first time, there were real consequences for cyber crime. And that changed everything.

THE MESSAGE WAS CLEAR:

Big, public attacks bring heat.
And heat is bad for business.
Even criminal business.



THE STRATEGY CHANGED: **CRIMINALS ADJUSTED**

After Colonial Pipeline, ransomware groups did not suddenly decide to become productive members of society. They adjusted.

Large attacks against critical infrastructure bring investigators, headlines, pressure, and consequences. Small business attacks are different.

When a local contractor, dental office, manufacturer, law firm, or accounting firm gets hit, it usually does not make national news. To the business owner, the attack may be devastating. To the criminal, it is safer.

That is exactly the point.

SMALL BUSINESSES ARE NOT TOO SMALL

A lot of small business owners still believe they are too small to be a target.

They are wrong.

You are now a preferred target. You are being targeted because you are easier to attack, easier to pressure, and less likely to create a major public response.

Most small businesses rely on technology for everything: email, payroll, invoicing, customer records, scheduling, banking, job files, vendor portals, and cloud systems.

If those systems go down, the business feels it fast. Cybercriminals know that.

PREPAREDNESS IS SURVIVAL

Cyber threats aren't going away - but with the right strategy, tools, and awareness, your business can stay one step ahead.



ASSESS YOUR RISK

Understand your vulnerabilities and where your data lives.



STRENGTHEN YOUR DEFENSES

Implement strong security controls and keep systems updated.



TRAIN YOUR TEAM

Employee awareness is one of your strongest defenses.



PLAN FOR THE WORST

Have a response plan and backups before an attack happens.



PROTECT WHAT MATTERS

Your business. Your data.
Your customers. Your future.

Let's build a stronger
safer tomorrow - together.

TAKE ACTION TODAY

Don't wait for an attack to
expose the gaps.

Contact us to strengthen
your cybersecurity.



THE REAL LESSON

The Colonial Pipeline hack was not just a warning for big corporations and infrastructure companies. It was a warning for small businesses too.

Cybercriminals learned that major public attacks can bring serious consequences. So many shifted their attention toward smaller, lower-profile targets.

That means small business owners need to stop saying, "We are too small for anyone to care."

That mindset is dangerous.

Spoofing vs. Hacking:

HOW TO TELL THE DIFFERENCE

Cybercriminals use both tactics - often together - to compromise systems. Understanding the difference is your first line of defense.



WHAT IS SPOOFING?

A deception technique where attackers disguise their identity to appear as a trusted source - tricking you into sharing information or granting access.

COMMON TYPES:

- Email Spoofing
- Caller ID Spoofing
- Website Spoofing
- IP Spoofing

WHAT IS HACKING?

The unauthorized access to systems, networks, or data. Attackers exploit vulnerabilities to steal information, install malware, or create backdoors.

COMMON TYPES:

- Phishing
- Malware
- Brute Force Attacks
- Exploits

HOW THEY WORK TOGETHER

Spoofing is often the entry point. An attacker spoofs a trusted identity (like your CEO's email) to trick you into clicking a link - which then delivers malware or harvests credentials. Spoofing opens the door; hacking walks through it.

REAL SCENARIO:

You receive an email that looks like it's from your bank asking you to verify your account. The email address is spoofed. You click the link and enter your credentials on a fake website. Now the attacker has your login - and uses it to hack into your real account.

Category	Spoofing	Hacking
Intent	Deceive / impersonate	Gain unauthorized access
Method	Disguises identity	Exploits vulnerabilities
Target	Human trust	Systems & data
Access	Doesn't require system access	Requires breaking in
Detection	Harder to spot in the moment	Often detected after damage

HOW TO PROTECT YOURSELF

Against Spoofing:

- Verify sender identity before responding
- Don't trust caller ID alone
- Check URLs carefully before clicking
- Enable email authentication (SPF, DKIM)

Against Hacking:

- Use strong, unique passwords
- Enable multi-factor authentication
- Keep software updated
- Monitor accounts for unusual activity



Recognizing both is key to staying safe online.

Pantheon Computers



STRENGTHEN YOUR IT TEAM WITHOUT ADDING HEADCOUNT

Co-Managed IT Services from Pantheon give your team the expertise, tools, and support they need to stay ahead of today's threats.



We work alongside your team so you can focus on what matters most.

CO-MANAGED IT. REAL PARTNERSHIP. STRONGER TOGETHER.

Pantheon becomes an extension of your IT team—providing the people, processes, and technology to help you deliver more with less.



EXTEND YOUR TEAM

Get skilled IT and security experts who integrate seamlessly with your staff to fill gaps and tackle complex projects.



ENHANCE SECURITY

Strengthen your defenses with continuous monitoring, threat detection, patch management, and proven security best practices.



IMPROVE EFFICIENCY

Reduce workload and eliminate bottlenecks so your team can focus on strategic initiatives instead of putting out fires.



INCREASE RELIABILITY

Proactive support and faster response times minimize downtime and keep your business running smoothly.



CONTROL COSTS

Predictable monthly pricing helps you manage budgets while getting enterprise-level IT support.

WHY BUSINESSES CHOOSE CO-MANAGED IT WITH PANTHEON



You stay in control of your IT strategy and decisions.



We provide the expertise and support to execute and scale.



Flexible solutions that adapt as your business grows.



Clear communication and accountability every step of the way.



Stronger security posture and peace of mind for your organization.



YOU SHOULDN'T HAVE TO DO IT ALL ALONE.

Partner with Pantheon and empower your IT team to do more.

LET'S BUILD A STRONGER IT TEAM-TOGETHER.



507-718-4288



pantheoncomputers.com

Social Engineering Is Not Always Obvious

By: Angel Anderson

Hackers don't always break in. Sometimes they talk their way in.

We've all heard of social engineering by now.

Most organizations have seen the usual attempts: fake requests to change an employee's direct deposit information, smishing texts asking someone to buy gift cards, emails pretending to be from the boss, that sort of thing.

Those are the ones we tend to think about.

But some social engineering attacks are much more complicated, much more personal, and much harder to detect.

I just finished reading *Ghost in the Wires*, Kevin Mitnick's autobiography. Mitnick was one of the most famous hackers in history, and one of the things that stood out to me was how often he didn't need fancy hacking tools at all.

“
The most dangerous cyberattack doesn't look like an attack at all.”

He Didn't Hack the System. He Became Familiar.

MITNICK'S LESSON WAS NOT ABOUT CODE. IT WAS ABOUT TRUST.

In the book, he describes compromising the Social Security Administration through what he called an "elaborate social engineering attack." He researched the agency's departments, locations, managers, supervisors, and internal language. Then he called an SSA employee named Ann and pretended to be "Tom Harmon" from the agency's Office of the Inspector General.

According to Mitnick, he and Ann became "telephone buddies" for about three years. When he called, she would stop what she was doing to help him look up information.

And this wasn't harmless information. He says she helped him access Social Security numbers, birth details, mothers' maiden names, disability benefits, wages, and other sensitive records.

No hacking tools. No dramatic movie scene with green code flying across the screen.

He made a friend.

A friend who was happy to help because he was nice, familiar, and seemed to know what he was talking about. That's social engineering.

“

They don't guess anymore - they research.

SIDEBAR

Why It Worked

- He sounded like he belonged
 - He knew the agency language.
 - He became familiar over time.
 - Helping him started to feel routine.
 - Trust replaced verification.
-

Today's social engineer is patient, researched, and highly convincing.

It Works Because People Are Human.

A GOOD CON ARTIST IS NOT TRYING TO OUTSMART YOUR IQ.

I'm sure Ann was an intelligent, capable woman. Social engineering does not work because people are stupid. It works because people are human.

A good con artist is not trying to outsmart your IQ. They are trying to get you to trust them, rush for them, feel sorry for them, feel flattered by them, or feel confused enough that you stop thinking clearly.

Mitnick made sure he knew enough about the Social Security Administration to sound like he belonged there. That is what made his story believable.

And it can go even further.

Security researcher Thomas Ryan created a fake online persona named Robin Sage, who claimed to work in military intelligence as a cyber threat analyst. Over 28 days, that fake persona gathered hundreds of connections on social media, including people connected to government, military, intelligence, and large corporations.

Think about that for a second.

If someone looks legitimate online, has the right connections, uses the right language, and seems to be part of your professional world, would you automatically doubt them? Most people wouldn't. And social engineers know that.

SIDEBAR

Red Flags You Should Never Ignore



Unexpected Urgency
("Do this now")



Requests for sensitive
information



Slightly "off " email
addresses or URLs



Pressure to bypass
normal procedures



Anything that
triggers a gut feeling

**If it feels off, it
probably is.**

Confusion Is Part of the Attack.

WHEN A MESSAGE CREATES AN EMOTIONAL REACTION, STOP.

They're also very good at taking advantage of confusion. During the 2025 St. Paul cyberattack, scammers reportedly sent fraudulent invoices claiming to be from the city. People were already confused, so the criminals exploited that.

Social engineering does not always look suspicious. Sometimes it looks helpful. Sometimes it looks routine.

The best advice I've heard recently came from someone in the BCA's Financial Crimes and Fraud division. He said that if a phone call, email, text, or message causes you to have an emotional reaction, stop.

If you suddenly feel stressed, excited, confused, flattered, rushed, scared, or even happy, pay attention. Someone may be trying to get you to move before you think. It might be legitimate or it might be the next Kevin Mitnick trying to become your new best friend.

Your Best Defense? Slow Down.

Speed is the attacker's advantage - hesitation is yours.

Cybercriminals rely on urgency. They want quick reactions and minimal scrutiny.

The simplest - and most effective - defense is also the most human: Pause.



VERIFY

unexpected requests.



DOUBLE-CHECK

links before clicking.



CALL BACK

using trusted contact information.



TRUST YOUR INSTINCTS

when something feels off.



No security tool is more powerful than a skeptical human who takes five extra seconds.



FINAL WORD:

In a world of increasingly advanced cyber threats, the biggest vulnerability hasn't changed. It's human trust. And the best defense isn't just smarter technology - it's more mindful behavior.

Cybersecurity Is Like an Onion

(Yes, Really)

By: Jessica Jones



It's summer, which means grilling season is finally back. And if your house is anything like mine, nothing beats that first home-grilled burger after a long winter. For me, the one topping that takes it from good to great is a slice of sweet onion.

That's probably why I've always liked the scene in Shrek where he says, "Ogres are like onions... they have layers." Donkey argues for cake or parfaits - but Shrek sticks with onions. He's right. You can't have an onion without layers - and the same idea applies to good cybersecurity.



Healthy cybersecurity is like an onion.

Instead of focusing on specific tools, think about how protection works in layers. A single control is never enough on its own. Real security comes from multiple layers working together.

Your Home is a Good Example

A screen door lock alone wouldn't make you feel secure. Neither would just a handle lock or even a deadbolt by itself. But when you combine them - locks, an alarm system, cameras, maybe motion lights - you start to feel protected.

Each layer covers gaps the others can't.



But it only works if the layers are actually used together.



Cameras don't help much if the doors are left unlocked.



An alarm system doesn't matter if it's never armed.



LOCKS

Control access.
Keep the bad guys out.



ALARM SYSTEM

Detect threats.
Alert you and others.



CAMERAS

See what's happening.
Provide evidence.



MOTION LIGHTS

Deter activity.
Create visibility.



Cybersecurity works the same way. You don't get strong protection from one solution - you get it from multiple, intentional layers working together consistently.



No single layer is perfect, and that's the point. If one fails, the other are still there.



Strong security isn't about finding the "best" tool. It's about building the right combination of protections and using them consistently.

SECURITY BY LAYERS

A Practical Cybersecurity Blueprint for Small and Medium Sized Businesses

By: Chase Gent



For owners, operators, and IT directors, the goal is not to buy one perfect security product. The goal is to build a layered defense that can prevent, detect, respond to, and recover from real-world attacks.

Small and medium-sized businesses have a security problem that is easy to misunderstand. The problem is not simply that they lack a firewall, antivirus software, or a good backup system. The real problem is that attackers do not come through only one door.

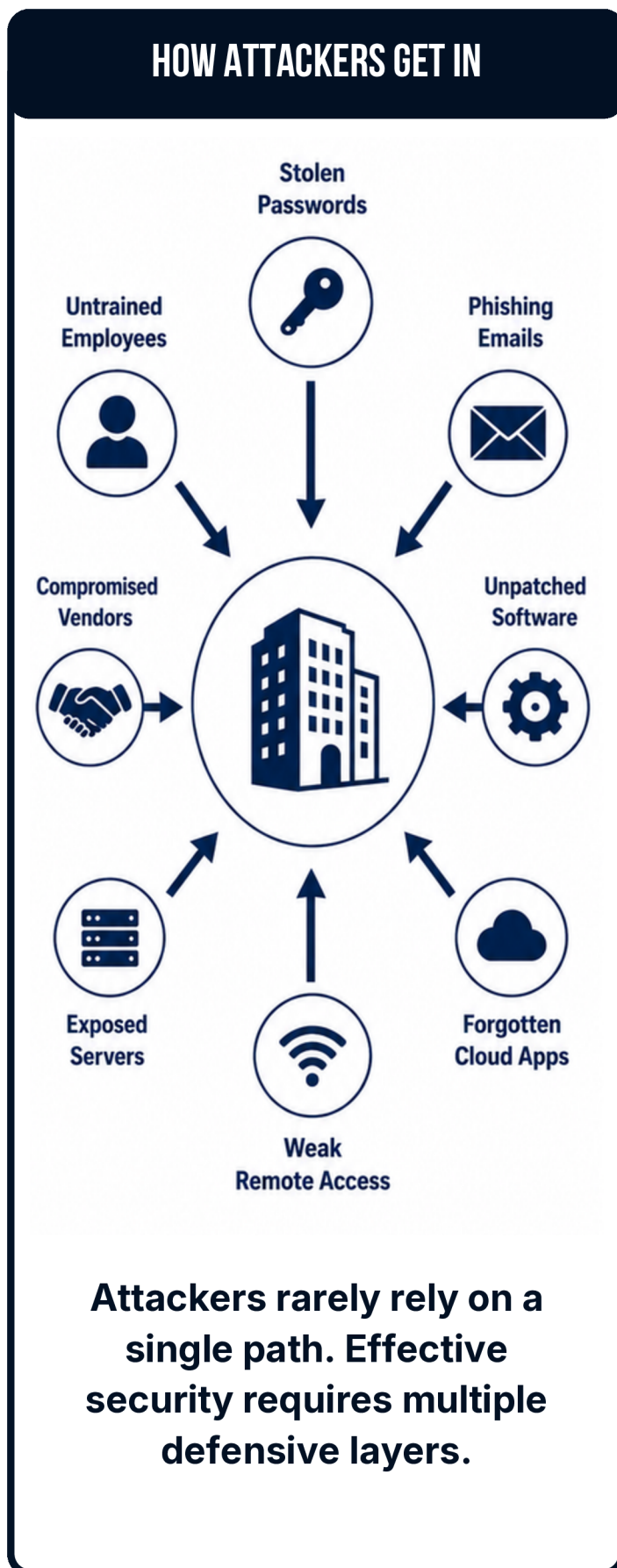
“ ***The important lesson is simple: security is not one control. It is a system.*** ”

They come through stolen passwords. They come through phishing emails. They come through unpatched software. They come through unmanaged laptops, forgotten cloud apps, weak remote access, exposed servers, compromised vendors, and employees who are trying to do the right thing but have never been trained to spot a fraudulent request.

That is why good security must be layered. A single product may block one attack path, but it will not protect the business against the full range of threats. A modern small-business security program needs to address multiple threat vectors at once: identity, email, endpoints, networks, cloud applications, data, vendors, monitoring, incident response, and recovery.

The following security tools checklist organizes this work around a practical version of the NIST Cybersecurity Framework: Govern, Identify, Protect, Detect, Respond, and Recover. NIST describes the framework as a way for organizations to manage and reduce cybersecurity risk, and its small-business guidance is designed specifically for SMBs with modest or developing cybersecurity programs.

The important lesson is simple: security is not one control. It is a system.



IDENTIFY

You cannot Protect What You Do Not Know Exists

The first layer is visibility. A business cannot secure devices, users, cloud applications, data, vendors, or public-facing systems it does not know it has. Owners and IT leaders should maintain a current inventory of workstations, servers, mobile devices, SaaS applications, domains, sensitive data locations, etc. Blind spots are where many attacks begin.

PROTECT

Build Barriers Across the Most Common Attack Paths

Protection is the layer most people think of first. Each tool addresses a different attack path, so they should not be treated as interchangeable. MFA helps when passwords are stolen, EDR helps when malware reaches an endpoint, patching closes known vulnerabilities, and email security reduces phishing exposure. The goal is not perfection; the goal is to make compromise harder, slower, and easier to contain.

DETECT

Make Sure Someone Can See Trouble Early

Preventive controls will not stop everything, so detection has to be part of the stack. SMBs should monitor alerts from all critical systems and security tools. Systems that collect data from all the security tools and SIEM can help connect events that may look harmless in isolation. Detection only works when someone is responsible for reviewing alerts and taking action. An ignored alert is not a security control.

RESPOND

Decide What Happens Before the Incident

Incident response is often the missing layer in small-business security. Every SMB should have a written response plan that identifies who makes decisions, who investigates, who communicates, who contacts outside support, and how affected systems are isolated. The plan should include specific actions to take during different types of breaches. It should also include cyber insurance contacts, legal and law enforcement contacts, and an offline copy of the plan. During an incident, confusion costs time, data, money, and trust.

RECOVER

Backups Matter Only If They Restore

Recovery is where a business finds out whether its security program works under pressure. Backups should cover all critical systems and data. They should also be protected from the same attack that hits the primary environment, which usually means immutable, offline, or separately credentialed backup storage. Restoration should be tested regularly, not assumed. A backup that has never been restored is an assumption, not a control.

THE BOTTOM LINE SECURITY IS A SYSTEM

Strong organizations are not protected by a single solution.
They are protected by multiple layers working together.



IDENTIFY

Know what you have.
You cannot protect
what you do not
know exists.



PROTECT

Build barriers across
the most common
attack paths.



DETECT

Make sure someone
can see trouble
early.



RESPOND

Decide what
happens before
the incident.



RECOVER

Backups matter
only if they
restore.

“

The companies that handle cyber incidents best are not the ones that believed they could prevent everything. They are the ones that built layers, expected failure, and prepared the business to keep operating anyway.

”

CYBERSECURITY READINESS ASSESSMENT

HOW STRONG ARE YOUR SECURITY LAYERS?



INSTRUCTIONS

For each item, rate your organization's current maturity.

SCORING GUIDE

0

Not Implemented

1

Planned

2

Partially Implemented

3

Fully Implemented

4

Fully Implemented & Regularly Reviewed



IDENTIFY

Do you know what you're protecting?

SCORE (0-3)

Asset Tracking	☐ 0	☐ 1	☐ 2	☐ 3
SaaS/Cloud App Inventory	☐ 0	☐ 1	☐ 2	☐ 3
Data Mapping	☐ 0	☐ 1	☐ 2	☐ 3
Network Mapping	☐ 0	☐ 1	☐ 2	☐ 3
Vulnerability Scanning	☐ 0	☐ 1	☐ 2	☐ 3
External Attack Surface Monitoring	☐ 0	☐ 1	☐ 2	☐ 3



PROTECT

Have you built barriers across common attack paths?

SCORE (0-3)

Endpoint Protection / EDR	☐ 0	☐ 1	☐ 2	☐ 3
Patch Management	☐ 0	☐ 1	☐ 2	☐ 3
Firewall / Router Security	☐ 0	☐ 1	☐ 2	☐ 3
Secure Wi-Fi & Guest Network	☐ 0	☐ 1	☐ 2	☐ 3
Secure Remote Access (VPN / ZTNA)	☐ 0	☐ 1	☐ 2	☐ 3
Encryption at Rest	☐ 0	☐ 1	☐ 2	☐ 3
Encryption in Motion	☐ 0	☐ 1	☐ 2	☐ 3
MFA / Phishing-Resistant MFA	☐ 0	☐ 1	☐ 2	☐ 3
Password Management	☐ 0	☐ 1	☐ 2	☐ 3
SPAM Filtering	☐ 0	☐ 1	☐ 2	☐ 3
Click Protection / URL Rewriting	☐ 0	☐ 1	☐ 2	☐ 3
Email Authentication (SPF, DKIM, DMARC)	☐ 0	☐ 1	☐ 2	☐ 3
Email Encryption	☐ 0	☐ 1	☐ 2	☐ 3
DNS Filtering	☐ 0	☐ 1	☐ 2	☐ 3
Application Whitelisting	☐ 0	☐ 1	☐ 2	☐ 3
Mobile Device Management (MDM)	☐ 0	☐ 1	☐ 2	☐ 3
USB Port Controls	☐ 0	☐ 1	☐ 2	☐ 3
Data Loss Prevention (DLP)	☐ 0	☐ 1	☐ 2	☐ 3
End User Education / Security Awareness	☐ 0	☐ 1	☐ 2	☐ 3
Phishing Tests	☐ 0	☐ 1	☐ 2	☐ 3



DETECT

Can someone see trouble before it becomes a crisis?

SCORE (0-3)

Centralized Logging / SIEM

☐ 0 ☐ 1 ☐ 2 ☐ 3

Alert Monitoring

☐ 0 ☐ 1 ☐ 2 ☐ 3

MDR/SOC Service

☐ 0 ☐ 1 ☐ 2 ☐ 3

Vulnerability Monitoring

☐ 0 ☐ 1 ☐ 2 ☐ 3

Dark Web Monitoring

☐ 0 ☐ 1 ☐ 2 ☐ 3



RECOVER

Can someone see trouble before it becomes a crisis?

SCORE (0-3)

Immutable / Offline Backups

☐ 0 ☐ 1 ☐ 2 ☐ 3

Backup Restoration Testing

☐ 0 ☐ 1 ☐ 2 ☐ 3

Cloud Backups

☐ 0 ☐ 1 ☐ 2 ☐ 3

Incident Response Plan

☐ 0 ☐ 1 ☐ 2 ☐ 3

Business Continuity Plan

☐ 0 ☐ 1 ☐ 2 ☐ 3

YOUR CYBERSECURITY READINESS SCORE

1. TOTAL POINTS EARNED

Add up all your points from the checklist.

2. MAXIMUM POSSIBLE POINTS

108

(36 ITEMS X 3 POINTS)

3. CALCULATE YOUR PERCENTAGE SCORE

Total Points Earned
108 X 100

= %

4. YOUR SECURITY LAYER RATING

See the key below to interpret your score.



**BELOW 40%
CRITICAL /
IMMATURE**

Substantial exposure.
Immediate action
required.



**40-59%
POOR /
FRAGMENTED**

Several important
controls missing or
informal.



**60-74%
MODERATE /
DEVELOPING**

Some security in
place, but layers are
uneven.



**75-89%
GOOD /
OPERATIONAL**

Strong foundation
with some gaps to
address.



**90 - 100%
STRONG /
MATURE**

Comprehensive
security program and
continuously
improving.

ASSESSMENT TAKEAWAY

Organizations rarely fail because of a single missing security tool. Most incidents occur when multiple gaps align. The strongest businesses build layers across Identify, Protect, Detect, Respond, and Recover - and regularly test those layers before a crisis occurs.



HOW TO SCORE INDIVIDUAL SECURITY LAYERS

Now that you have your Total Cybersecurity Readiness Score, it is helpful to score each layer individually. This helps point out which layers are your strengths and which ones you should focus on.

1. LAYER-BY-LAYER SCORING

Using the scoring key that was used to determine the total score, assign a score to each individual security layer.

 Identify	$\frac{\text{Total Points Earned}}{6} \times 100 =$
 Protect	$\frac{\text{Total Points Earned}}{20} \times 100 =$
 Detect	$\frac{\text{Total Points Earned}}{5} \times 100 =$
 Recover	$\frac{\text{Total Points Earned}}{5} \times 100 =$

2. SECURITY LAYER OVERVIEW

The following outlines and defines each security layer that will be evaluated and scored individually as part of the assessment.

 Identify Score	Measures whether the business knows what devices, users, systems, vendors, data, and risks exist.
 Protect Score	Measures whether the business has safeguards in place to reduce the likelihood and impact of attacks.
 Detect Score	Measures whether the business can see suspicious activity early enough to act.
 Recover Score	Measures whether the business can restore operations after disruption.

WHAT YOUR SCORE MEANS

Overall Security layer Rating



90-100%

STRONG / MATURE

The business has strong cybersecurity layers in place across identity, email, endpoints, network, cloud systems, data protection, monitoring, response, and recovery. Security controls are not only deployed, but also reviewed, tested and maintained. Backups are tested, alerts are monitored, users are trained, access is controlled, and there is a documented incident response plan. A business in this range is not immune to cyberattacks, but it is much better positioned to prevent common attacks, detect suspicious activity, contain incidents, and recover without major disruption.



75-89%

GOOD / OPERATIONAL

The business has many important controls in place and is ahead of many SMBs. Core protections such as MFA, endpoint protection, patching, backups, email filtering, and access controls are likely implemented. However, some areas may still be incomplete, informal, or untested. This is a solid position, but the business should focus on closing gaps in detection, response, and recovery.



60-74%

MODERATE / DEVELOPING

The business has some meaningful security controls, but the layers are uneven. Certain areas may be reasonably protected while others remain exposed. This score suggests the company has started building a security program but may still be vulnerable to common attacks such as phishing, ransomware, credential theft, and business email compromise. Improvement should be prioritized around the highest-risk gaps first.



40-59%

POOR / FRAGMENTED

The business has several controls missing or only informally handled. Security may depend heavily on individual judgment, basic tools, or assumptions that have not been tested. A company in this range has a higher likelihood of suffering a serious disruption from a routine cyberattack. Immediate remediation is recommended.



BELOW 40% CRITICAL / IMMATURE

The business does not have adequate security layers in place. Key controls are missing, undocumented, unmonitored, or untested. This level indicates substantial exposure to ransomware, account compromise, data loss, vendor-related incidents, and operational disruption. The business should treat cybersecurity improvement as an urgent operational risk, not a future IT project. The first priorities should be MFA, endpoint protection, patching, reliable backups, basic logging, employee training, and an incident response plan.

HEALTHCARE CYBERSECURITY ALERT

HIPAA *Just Got* Teeth.

The 2026 Security Rule closes the “addressable” loophole for good. **Encryption, MFA, EDR, SIEM,** and **annual penetration testing** are now **mandatory** for every covered entity.



\$7.42M

AVG. BREACH COST
(IBM 2025)



**197
DAYS**

ATTACKERS HIDE
UNDETECTED, AVG.



82%

HEALTHCARE VICTIMS
WHO PAID RANSOM



**180
DAYS**

TO COMPLY ONCE
RULE IS FINALIZED

WHAT'S NOW MANDATORY — NO EXCEPTIONS

- ✓ **Encryption** — at rest and in transit on all ePHI systems.
- ✓ **MFA** — required on every system touching ePHI.
- ✓ **EDR/MDR Endpoint Protection** — antivirus alone is no longer sufficient.
- ✓ **Annual Penetration Testing** — by a qualified third party.
- ✓ **SIEM / Log Monitoring** — 24/7 detection with active alert response.
- ✓ **Annual Written Risk Analysis** — documented every year.
- ✓ **Workforce Training + Phishing Simulations** — documented annually.
- ✓ **Asset Inventory + ePHI Network Map** — a full picture of where data flows.

PANTHEON HIPAA SECURITY AUDIT

Find Out Exactly Where **You Stand.**

We evaluate your environment against the current Security Rule and 2026 requirements — delivering a written report with risk ratings and a prioritized remediation roadmap before enforcement begins.



**We don't just find gaps.
We help close them.**



FREE HIPAA GUIDE AVAILABLE

We've created a practical HIPAA Compliance Guide to help you navigate the 2026 Security Rule.
Let us know if you'd like a copy!



CONTACT PANTHEON
(507) 718-4288

contact@pantheoncomputers.com
pantheoncomputers.com



**SERVING HEALTHCARE
SINCE 1997**

Locally & Woman-Owned
Waseca • Mankato
Faribault • Rochester



**Don't wait for the deadline —
every day of exposure
is a day of risk.**

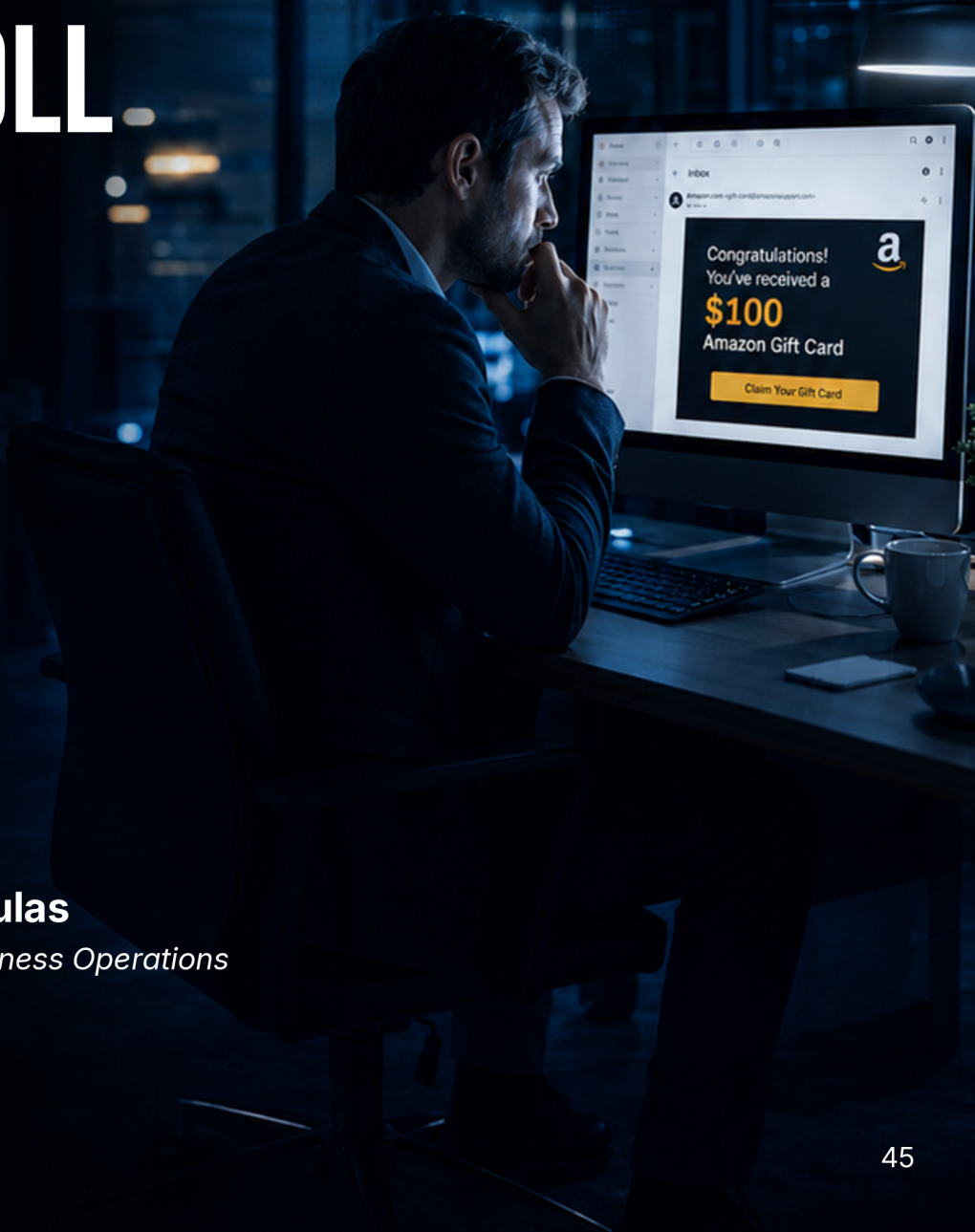
Sources: IBM Cost of a Data Breach Report 2025 • HHS HIPAA Security Rule NPRM (Jan 2025) • Kaseya Cybersecurity Survey 2024

YOUR BIGGEST SECURITY VULNERABILITY IS ALREADY ON THE PAYROLL

You have invested in firewalls, endpoint protection, and MFA. Now let's talk about the part no software can fully patch.



By: Nikki Dulas
Director of Business Operations



Imagine you have built a fortress. Thick walls. Reinforced gates. Your IT team has patched every vulnerability, your firewall rules are immaculate, and your endpoints are locked down tight.

Then Dave in Accounting clicks a link promising a free Amazon gift card.

THIS IS NOT A HYPOTHETICAL.

THIS IS A TUESDAY.

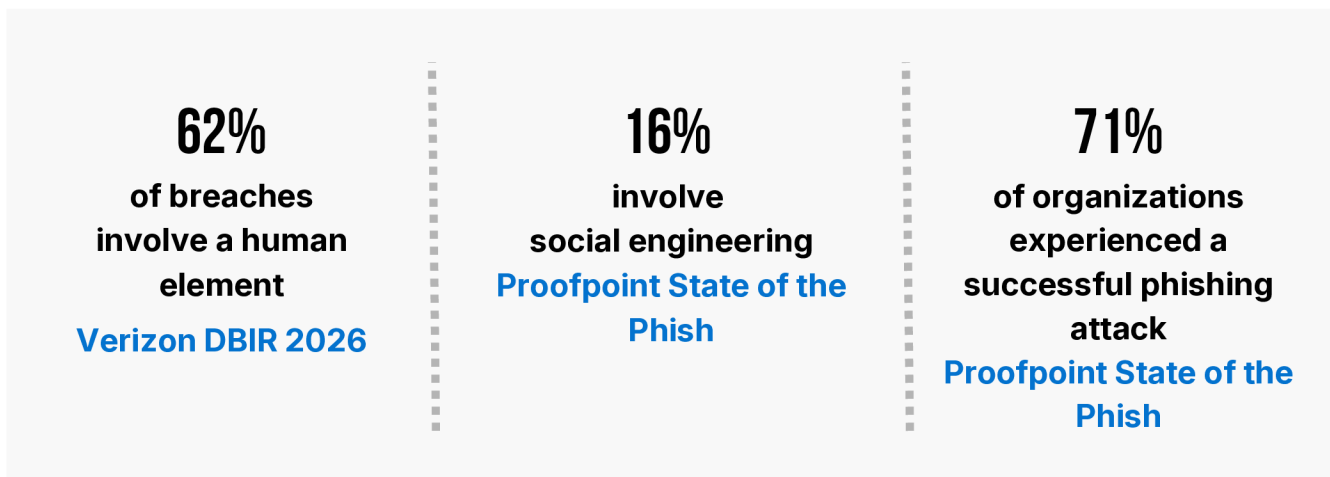
Organizations invest heavily in securing their infrastructure, and they should. Firewalls, endpoint protection, patch management, identity controls, monitoring — all of it matters. But no software subscription can fully account for the most unpredictable variable in the equation.

People.

Creative, well-meaning, deadline-driven people whose best qualities are exactly what attackers are counting on.

The attackers figured this out a long time ago. Most organizations are still catching up.

Your next breach may not start with advanced malware. It may start with a person making a perfectly human mistake.



THE NUMBERS DON'T LIE, BUT THE HACKERS SURE DO.

The 2026 Verizon Data Breach Investigations Report puts it plainly: 62% of breaches still involve the human element — social engineering, errors, misuse, stolen credentials, or other human-driven exposure. That is not a side issue. It is the majority of breach activity.

Social engineering remains one of the most reliable ways attackers get in. Verizon reports that it accounts for **16% of breaches**, and mobile-centric phishing (voice, SMS, and callback-style attacks) produces **40% higher median click rates than email phishing simulations**.

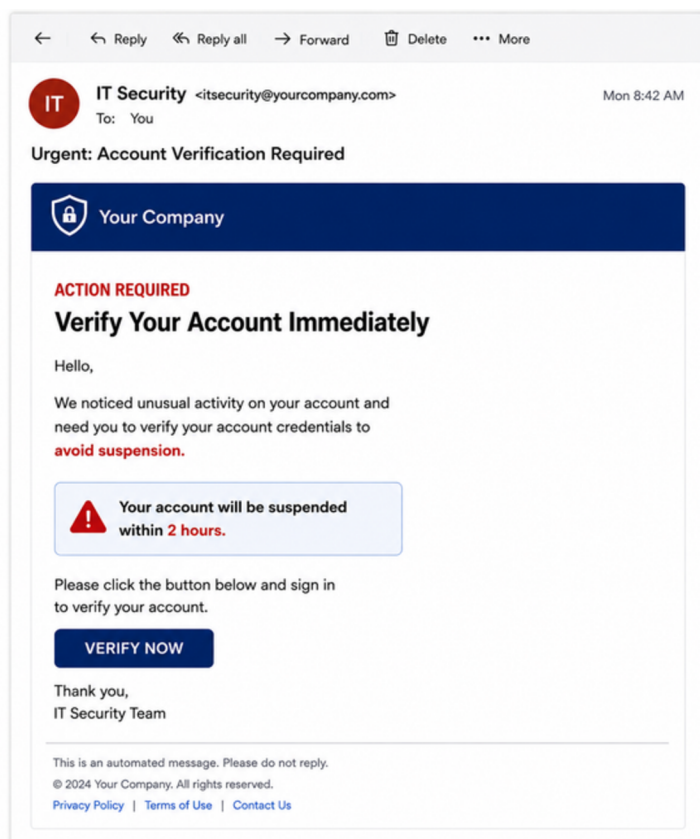
Proofpoint's latest comparable State of the Phish data found that **71% of surveyed organizations experienced at least one successful phishing attack** in the prior year. And in Proofpoint's 2024 simulation data, users still failed phishing tests at an average rate of **4.93%** across all campaigns.

Small percentage. Large consequences.

Do the math on your own headcount. One click, one credential submission, one convincing phone call — that is all an attacker needs.

The average employee receives **121 emails per day**. Expecting perfect threat detection on every single one is not a security strategy.

People make judgment calls under time pressure all day long. Occasionally, they will make the wrong one. The goal is not perfection. The goal is to build habits and systems that make mistakes harder to make, easier to catch, and faster to report.



ATTACKERS MANUFACTURE CONTEXT

They add urgency ("Your account will be suspended within 2 hours.")



THEY INVOKE AUTHORITY

They use titles and departments people trust ("Message from IT Security - Action required.")



THEY REPLICATE FAMILIARITY

They mimic branding and logos well enough to pass a quick glance



THEY TIME THEIR ATTACKS

Monday mornings, Friday afternoons. When attention is elsewhere and people are moving fast.

SO WHAT DO YOU ACTUALLY DO ABOUT IT?

Here's what the research actually supports.

1



CONSISTENT SECURITY AWARENESS TRAINING

Not annual. Not a one-time event you can set and forget. Training needs to be regular, short, varied, and tied to current threats. Industry research consistently shows that organizations running ongoing programs can significantly reduce phishing click rates over time.

2



SIMULATED PHISHING CAMPAIGNS

Controlled phishing tests serve two purposes. They show you who needs more support before a real attacker finds them, and they build a healthy skepticism that training alone does not create. The key is using the results to coach and strengthen, not to shame or single people out.

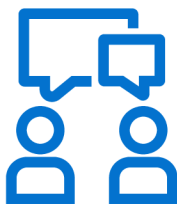
3



A CULTURE WHERE PEOPLE REPORT THINGS

This one costs nothing and gets overlooked constantly. Employees who feel safe saying, "I think I clicked something I should not have," become your fastest incident response system. Organizations that punish or embarrass those employees get silence instead — and a breach that festers undetected.

4



CONSISTENT FOLLOW-UP

If someone does not complete their awareness training or repeatedly falls for simulated phishing emails, you need to follow up. Assign additional training. Talk with them so they understand why it matters. And, if necessary, put disciplinary consequences in place for repeat negligence. Accountability matters, but it should come after coaching, not instead of it.

YOUR BEST SECURITY ASSET IS ALREADY ON THE PAYROLL

Every person with a login is part of your security posture. Keeping that posture strong is everyone's responsibility, not just IT's.

Your employees are the most targeted part of your infrastructure, and they deserve to be set up for success.

Getting this right does not mean your people never make mistakes. It means your organization is built to handle it when they do.

Because somewhere out there, an attacker is crafting a very convincing message to Dave.

Make sure Dave is ready for it.

THE TAKEAWAY



TRAIN CONTINUOUSLY

Keep security awareness fresh, relevant, and engaging.



BUILD A STRONG CULTURE

Create a safe environment where people speak up.



PREPARE. TEST. IMPROVE.

Use data and feedback to strengthen your human firewall.



SOURCES: Verizon 2026 Data Breach Investigations Report |
Proofpoint 2024 State of the Phish

The Deepfake That Almost Fooled Me

LESSONS FROM THE SALES & MARKETING LEAD ON
STAYING ONE STEP AHEAD



By Kelsey Kahnke



I get a lot of unusual requests from my boss.

Sometimes they are work-related. Other times, they are more personal or random, like helping drop something off at her kids' school. So when I got a strange call that sounded like her asking me to do something out of the ordinary, I did not immediately question it.

That is what almost made it work.

Her voice sounded right. The tone, the pace, even the urgency felt familiar. The request was odd, but not odd enough to seem impossible. My first thought was not, "Is this really her?" It was, "How am I going to fit this into my day?"

But something felt slightly off.

The timing of her responses seemed strange, and the way she answered one of my questions did not sound exactly like her. It was close, but not quite right. Instead of acting on the request, I messaged her separately to confirm.

She had not called me.

That was when I realized I had almost been fooled by a deepfake voice.

What scared me most was not that it sounded perfect. It was that it sounded familiar enough. The scam worked because it fit into a pattern I already knew: my boss sometimes asks for unexpected things, and I usually try to help quickly.

This experience taught me that deepfakes are not just about fake celebrity videos or viral clips online. They can show up in ordinary moments, using familiar voices, relationships, and routines to get people to act before they think.

Now, when something feels urgent or unusual, I pause and verify it another way. A quick text or message can prevent a big mistake.

In the age of deepfakes, sounding real is not enough. Before we act, we have to make sure it is real.

CYBERSECURITY WORD SEARCH



Find the hidden cybersecurity terms in all directions.

I	D	C	N	L	O	G	G	I	N	I	M	I	G
E	E	H	K	C	A	T	T	A	R	E	B	Y	C
B	F	W	R	O	T	C	A	F	I	T	L	U	M
T	E	R	A	N	S	O	M	W	A	R	E	E	I
P	N	E	V	P	N	Y	P	P	A	T	C	H	E
B	D	E	S	T	D	R	O	W	S	S	A	P	O
O	E	S	T	W	T	A	M	E	I	S	T	U	F
T	R	O	N	O	T	P	H	I	S	H	I	N	G
N	N	C	R	B	B	A	C	K	U	P	T	C	T
E	T	T	A	E	R	H	T	C	H	P	O	I	I
T	H	M	W	M	O	N	I	T	O	R	I	N	G
M	A	L	W	A	R	E	O	T	O	O	A	R	G
A	U	T	H	E	N	T	I	C	A	T	I	O	N
L	L	A	W	E	R	I	F	E	O	O	A	D	H

PHISHING
 LOGIN
 RANSOMWARE
 MALWARE
 BOTNET
 CYBERATTACK
 AUTHENTICATION
 VPN
 MONITORING
 FIREWALL
 THREAT
 SIEM
 DEFENDER
 SOC
 PASSWORD
 BACKUP
 MULTIFACTOR
 PATCH

Answer Key
from Issue 1:

Across:
4 Robotics
5 Cache
6 API

7 Pixel
8 Chatbot
10 Autonomous

11 Keyboard
12 Dataset
13 Hypervisor

14 GPT

Down:
1 Firewall
2 Database
3 Encryption

4 Cloud
5 Bandwidth

Our Core Values

Pantheon Computers believes that everything we do is rooted in relationships. It is the nature and character of that relationship that forms our core values. In our relationships with each other and our clients we are committed to:

1. Being an Invested Partner
2. Doing the Right Thing
3. Being Accountable
4. Striving for Transformative Growth



Invested Partner

Pantheon takes the time to learn about your business and what success means to you. We want to understand your goals and concerns so that we can provide you with the information and support you need to make decisions that move your business forward. Every person at every level of Pantheon is involved so we can provide multi-dimensional support. We have your best interests in mind, because we believe that your success is our success. We strive to function as an integral part of your team.

Do the Right Thing

We aim to provide excellent value for your dollar. The IT line item in your budget is significant and it is vital for that money to be an investment in your success and not just an expense. We commit to not over-selling or under-solving your problems. We take pride in knowing that we are fair and honest in our recommendations for your business and earn the trust of our clients. We genuinely care about client satisfaction. Your concerns, needs and worries are a priority for us, and we diligently seek ways to assist in addressing and alleviating those things for you. We also understand that you do not necessarily have the tools or knowledge available to make sure we are doing our jobs properly. So, we commit to doing the right thing for your business – even if that results in a loss for us.

Accountable

The truth is a lot of clients don't really understand a lot of what we do. Holding your MSP accountable can be hard. We make it easier with reporting, having frank conversations on visible accountability, and regular check-ins with your advisor to track the progress on your goals. When we make mistakes, we will own them. This is important because once we are all comfortable with accountability on the day-to-day stuff, we can move on to the fun stuff like innovation, automation and AI.

Transformative Growth

We want to help you dream and then help you get to your dream. Our senior advisors run our business, so they understand the struggles and the joys of it. They also want to talk about your strategic goals, budgeting, forecasting/road mapping, risk management, compliance, cyber security insurance plans, and new technologies. We are always looking to learn more; and then work on thinking critically and creatively on ways new technologies can benefit you.

 www.pantheoncomputers.com

 507-718-4288

 contact@pantheoncomputers.com



Kris Government

As a law enforcement professional, Information Technology is not naturally my strongest area. Through our normal everyday IT contract with Pantheon to provide City IT services, Pantheon has taken on the responsibility to guide us through all through all the complex policies we must follow to be CJIS compliant. This includes network security, policy revisions, staying updated on trainings and communicating upcoming needs. Our last BCA CJIS audit in 2023 went smoothly in part because Pantheon provided much of the information to the BCA directly. Pantheon has been able to prevent and mitigate loss and harm in the event of any attempted cyberattack breaches and provides a thorough investigation and after-action report. Working with Pantheon has allowed us to focus on public safety priorities and leave much of the IT tasks to the experts.



Vicki Services

Pantheon: Efficient, Friendly, and Dependable IT Support

The biggest benefit we've experienced since Pantheon took over our IT and put us on their managed program is the improvement in our tools—better antispam, cloud storage, and antivirus applications. They've made it easy to get support, and we know we can count on them to deliver excellent service.

Opening a ticket is as simple as sending an email, and their communication is above and beyond anything we've experienced with other IT firms. They're always dependable, responding promptly and keeping us informed every step of the way.

What really sets Pantheon apart is their team. Their IT professionals aren't just efficient—they're friendly and take the time to ensure customers understand the applications they're using.

Honestly, I think Pantheon is great. If you're looking for reliable IT support with a personal touch, they're the team to call.



Timothy Financial Services

Trustworthy and Responsive IT Support with Pantheon

When it comes to IT services, you need someone you can trust to resolve your issues quickly. That's exactly what I've experienced with Pantheon.

While I haven't worked with other IT providers to compare, Pantheon has consistently met every challenge I've brought to them. Their quick response times and dedication to solving issues have been outstanding.

What I especially value is their local presence. I can easily drive to Waseca to deliver a computer that needs attention, or if I prefer to speak with someone face-to-face, it's always an option. Pantheon's reliability and accessibility make them an excellent partner for IT support.

About Us

Pantheon is proudly owned and operated by Jill Stagman and Reyna Monson. As a locally and woman-owned business, we are deeply committed to the communities we serve. Our leadership reflects our belief in building strong, inclusive organizations that prioritize relationships, integrity, and long-term impact.

At Pantheon, our goal is to make a meaningful difference. We do this by supporting and securing businesses throughout the region, helping them operate confidently in an increasingly complex technological landscape. By providing reliable solutions, trusted guidance, and responsive service, we empower organizations to focus on what they do best — growing their businesses and serving their customers.

We believe that when local businesses are strong and secure, communities thrive. By protecting critical operations, safeguarding data, and strengthening IT infrastructure, we contribute to economic stability and opportunity across the region. Our work goes beyond technology; it is about enabling people, supporting livelihoods, and fostering environments where individuals, families, and organizations can live, work, and succeed.



507 - 718 - 4288



contact@pantheoncomputers.com



www.pantheoncomputers.com



400 15th Ave SE, Waseca, MN 56093

At Pantheon, we are not just a service provider — we are a partner invested in the long-term success of our clients and the vitality of our communities.



MANAGED SERVICE PROVIDER

Today's IT is complex and constantly evolving. Outsourcing is a cost-effective way to stay ahead.

With Pantheon's Managed IT and Advisor services, you stay in control while we provide the tools, expertise, and strategy to support your long-term success.

- Helpdesk
- Server & Network Administration
- Cybersecurity & Compliance
- Audit Preparedness
- 24/7 Monitoring
- Project Expertise



507-718-4288

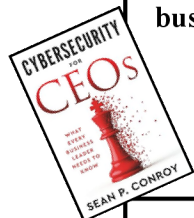


www.pantheoncomputers.com

YOUR GO TO CYBERSECURITY RESOURCE LIST

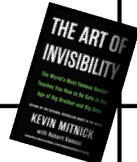
Books

Cybersecurity for CEOs: What every business leader needs to know



In today's digital world, cybersecurity is no longer just an IT issue; it's a business survival issue. Cybersecurity for CEOs is a clear, no-jargon guide explicitly designed for time-strapped business leaders who can't afford to get lost in the weeds. Whether you're running a 20-person law firm or a fast-growing SaaS company, this book will show you how to lead on security without becoming a technical expert. You'll learn why small businesses are prime targets, what the most common threats look like, and how to turn cybersecurity from a cost center into a competitive advantage.

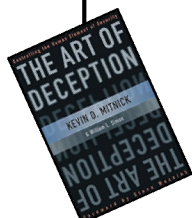
The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data



Be online without leaving a trace. Your every step online is being tracked and stored, and your identity literally stolen. Big companies and big governments want to know and exploit what you do, and privacy is a luxury few can afford or understand.

In this explosive yet practical book, Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, teaching you "the art of invisibility" -- online and real-world tactics to protect you and your family, using easy step-by-step instructions.

The Art of Deception: Controlling the Human Element of Security



The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security

Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in *The Art of Deception*, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief."

Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

YOUR GO TO CYBERSECURITY

RESOURCE LIST

Podcasts		
Darknet Diaries	Story-driven	Breaks down breaches and social engineering in ways executives and employees can actually remember.
Smashing Security	Lighthearted but informative	Very approachable for managers, operations staff, and general business users.
CyberWire Daily	Daily news brief	Short, business-friendly updates on threats, ransomware, AI risks, and regulations.





KEEP LEARNING WITH PANTHEON

Thank you for reading this issue! We hope you found valuable insights to help your organization work smarter, stay secure, and get more from technology. The conversation doesn't end here. Explore even more resources created to keep you informed, prepared, and ahead of what's next.



EXPLORE OUR MAGAZINE ARCHIVE

Missed an issue? Looking to revisit a favorite article?

Browse our complete collection of past Pantheon magazines featuring technology trends, cybersecurity insights, customer success stories, compliance guidance, and practical IT advice for today's businesses.



Scan the QR code
or visit:

[pantheoncomputers.com/
magazines](https://pantheoncomputers.com/magazines)



READ THE PANTHEON PERSPECTIVE BLOG

Our blog is updated regularly with expert insights on cybersecurity, managed IT, compliance, Microsoft 365, AI, productivity, and the technology issues that matter most to businesses today.



Scan the QR code
or visit:

[pantheoncomputers.com/
pantheon-perspective-
blog-posts/](https://pantheoncomputers.com/pantheon-perspective-blog-posts/)



STAY CONNECTED

Follow us online for fresh content, announcements, and new resources throughout the year.





THE CONVERSATION DOESN'T END HERE

Technology is always evolving—and so are we.

Whether you prefer live discussions, on-demand learning, or expert insights, Pantheon offers resources designed to help you navigate today's technology landscape with confidence.



WATCH OUR WEBINAR SERIES

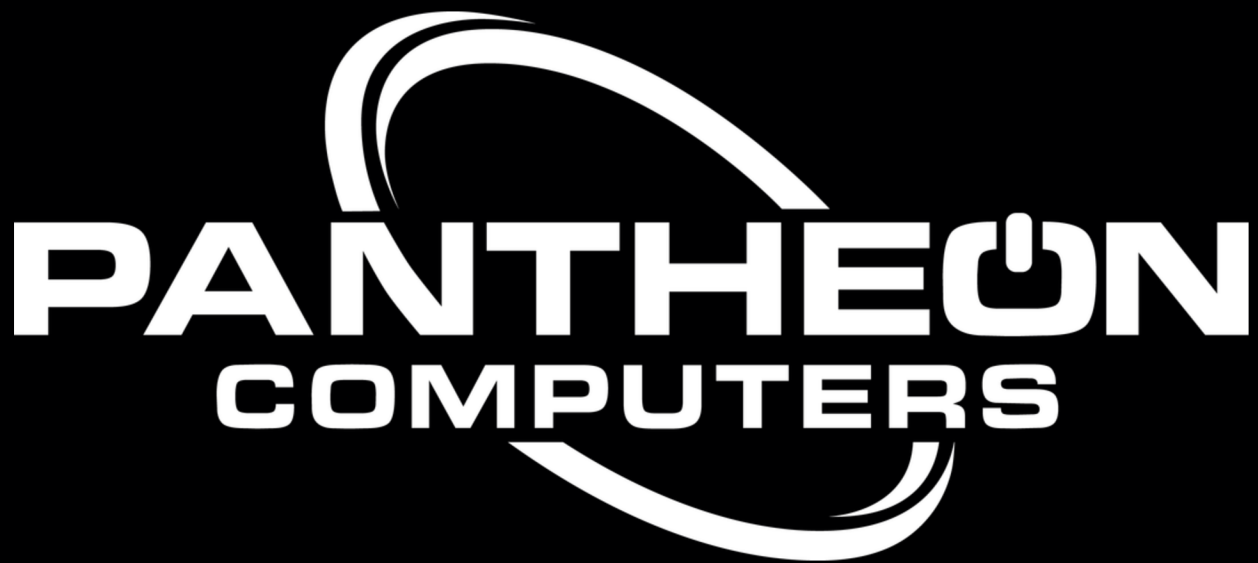
Our webinars feature practical conversations with technology experts covering cybersecurity, compliance, AI, Microsoft 365, IT strategy, and emerging business technologies.



pantheoncomputers.com/webinars/



Subscribe to
PILLAR



507 - 718 - 4288



contact@pantheoncomputers.com



www.pantheoncomputers.com