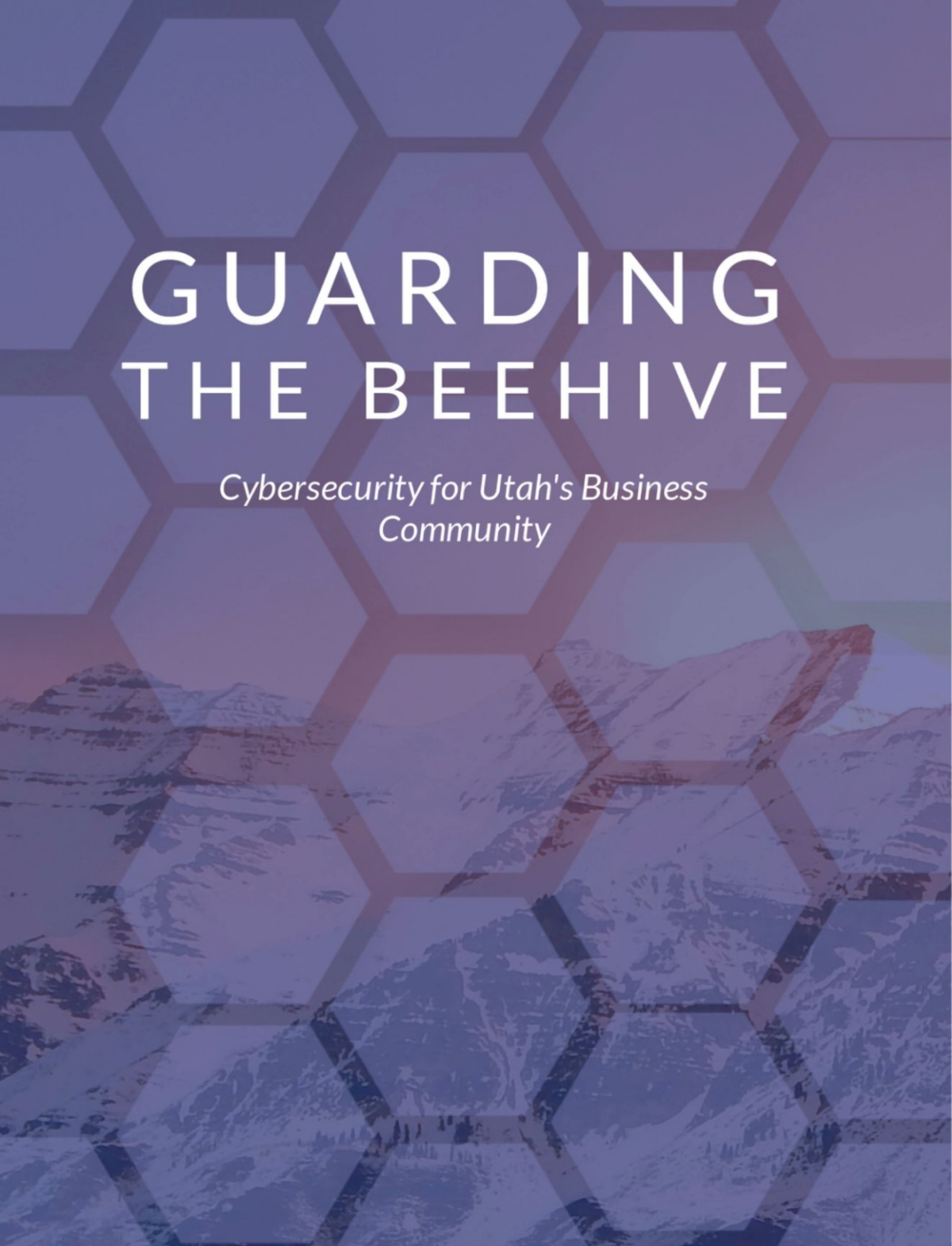
GUARDING THE BEEHIVE

Cybersecurity for Utah's Business Community



JOHN HUSTON

Guarding the Beehive

Cybersecurity for Utah's Business Community

John Huston

Founder, Brivy IT • Sandy, Utah

Brivy IT
8415 S. 700 W. Suite 7, Sandy, UT 84070
(385) 200-7323 • support@brivyit.com • brivyit.com

Printed in the United States of America
First Edition, 2025

Contents

For the business owners of Utah —
the ones who build, serve, and protect this community.

And for every IT professional who does the right thing
when nobody is looking.

CHAPTER 0

A Walgreens Parking Lot in Midvale

I'm sitting in my car in a Walgreens parking lot in Midvale, Utah. It's after hours. It's dark. And I'm about to buy bitcoin from a buddy who pulled up next to me so I can pay a ransom to a criminal I'll never meet, halfway around the world, to save a business I just learned about a few days ago.

This was years ago, before Brivy IT was even a formed idea in my mind. Back when bitcoin was still a novelty — something nerds were mining and tossing around like digital pocket change. We only really had physical wallets at the time, and the whole thing felt like something out of a movie that hadn't been written yet.

But there was nothing dramatic about the business owner I'd just met. He wasn't a character in a movie. He was a guy running a company along the Wasatch Front, and his entire world was locked up. His server — encrypted by ransomware. His business data, his books, his accounting, his intellectual property, his documents. On-premise Exchange handling all his email. Active Directory authenticating every device. Everything. Gone. Held hostage.

I watched the panic in that man's face, and it brought a new kind of reverence to what I do for a living.

Nobody thinks of the IT guy as the noble hero. We don't wear that badge, and we don't need to. But I'll tell you this — that night wasn't a fire, a flood, or a break-in through the back door. It was a burglary all the same. Someone was stealing this man's entire business and holding it for ransom, and the only way out was a check written to a buddy in a parking lot and a transfer of cryptocurrency that most people hadn't heard of yet.

We paid. The hacker gave us the keys. We restored the system.

That was an averted disaster. But it's insane to think about now, knowing what ransomware has become — a multi-billion-dollar criminal industry that hits businesses like yours every single day.

That experience stuck with me. Not just because it was dramatic, but because of what it revealed.

I've spent my entire career in the office technology space. I've worked across nearly every industry you can think of. And over those years, I developed a deep love for helping my clients solve problems in their businesses — whether that was through software, hardware, or services. Honestly, some days I think I'd keep doing what I do even if nobody paid me. I just love this work, and the people I do it for have become my friends.

But here's what I kept seeing, over and over again, at every company I worked for: technology was being treated as a pile of disconnected parts. A server here. An antivirus subscription there. A backup that nobody tested. Security treated as an upsell — something you tacked onto a proposal to bump up the monthly number, rather than something every single client needed from day one.

That never sat right with me.

I believe technology should work like a fine watch — a unified ecosystem of interworking gears, each one placed with precision and care. Not a junk drawer of tools that sort of work together on a good day. And I believe security isn't something you sell on top of that. It's woven into the fabric of everything. It's not an add-on. It's the baseline.

That belief is why I started Brivy IT.

The name “Brivy“ isn't a technical term or an acronym. Look it up in the Urban Dictionary and you'll find it means something pretty simple: cool, good, groovy. We picked it because we wanted a word that captured the feeling we want every client to have — that their technology just works, that it's taken care of, that someone is watching over it with craftsmanship and pride. Not a name that was stiff or corporate. Just something that felt right.

And that feeling is what I want this book to give you.

Who This Book Is For

This book is for every business owner along the Wasatch Front — and honestly, anywhere in Utah — who knows they should probably be doing more about cybersecurity but doesn't know where to start.

Maybe you're running a dental practice in Murray. A construction company in Riverton. A law firm in downtown Salt Lake. A growing startup in Lehi. A family business in Sandy that's been around for thirty years.

You're not a tech expert. You shouldn't have to be. You have a business to run, employees to take care of, and customers who trust you.

But here's what I need you to hear, and I'm going to say it with all the care and directness I can: if you're the business owner reading this right now, there's a very good chance that you are the biggest cybersecurity risk in your own company.

I see it constantly. The owner who tells me, “Oh yeah, everyone has MFA,“ and then I look at the admin portal and find two or three people who don't — and one of them is the owner. The owner who exempts themselves from the password policy because “I own the place.“ The owner who doesn't do the security awareness training they assigned to everyone else. The owner who has the most data access of anyone in the organization, poses the greatest risk, stands to lose the most, and yet models the worst security behavior in the building.

I'm not saying that to call you out. I'm saying it because I genuinely care about what happens to your business, and I'm not going to let you ignore the thing that could take it all away. That's just not how I'm built.

What This Book Will Give You

This book isn't meant to turn you into a cybersecurity expert. It's not filled with manufactured urgency or fear tactics designed to make you buy something.

What it will do is make cybersecurity make sense. It'll show you that most of it comes down to a handful of smart habits — things that are simple, practical, and completely within your reach. You'll understand the threats that actually target

businesses like yours. You'll learn a simple framework to organize your efforts so you're not just reacting to the latest scary headline. And you'll walk away with the right questions to ask your IT provider — because holding them accountable is one of the most important things you can do.

Take this book one chapter at a time. Don't feel like you need to overhaul everything overnight. Just pick one or two things from each chapter and start doing them. That's how habits are built. That's how real security works — not as a project with a start and an end, but as a way of operating your business with the same care and attention you bring to everything else.

I've spent my career watching what happens when businesses take shortcuts with technology. I've been in the parking lot at midnight trying to undo the damage. I've also seen what happens when people do it right — the peace of mind, the confidence, the resilience when something eventually does go wrong.

I wrote this book because I want that for you. For your business. For your employees. For the community we share here in Utah.

So grab a cup of coffee, and let's get to work.

— *John Huston Founder, Brivy IT Sandy, Utah*

PART I — The What & The Why

CHAPTER 1

What Cybersecurity Actually Is

Meet David. He runs a fifteen-person HVAC company in West Jordan. His crews are on the road every day, his office manager handles scheduling and invoicing, and he's been using the same IT setup for about five years. When I asked David what his cybersecurity plan was, he laughed and said, "We're an HVAC company. Nobody's trying to hack us." When I pulled up his company's email admin console, three accounts had no MFA, his office manager was using the same password for everything, and two former employees still had active logins — one of whom had left eighteen months ago. David's a smart guy. He just didn't know what he didn't know. That's who this chapter is for.

Let me clear up something the tech industry has worked very hard to overcomplicate.

Cybersecurity is not a piece of hardware your IT company plugs into a rack. It's not a software subscription with a fancy dashboard. And despite what the marketing would have you believe, it's not something reserved for Fortune 500 companies and government agencies.

For a typical Utah business — five people, fifty people, or a hundred and fifty — the core idea is refreshingly simple. Cybersecurity is the set of habits your organization builds to reduce the odds that something bad happens to your digital assets. Your data, your systems, your ability to keep the lights on and serve customers. That's it. The entire discipline, reduced to its essence, is about managing risk in the digital parts of your operation.

Think about how you'd approach physical security. You wouldn't leave the office unlocked at night and hope for the best. You'd lock the doors, arm the alarm, and make sure only the right people have keys. Cybersecurity applies the same common sense to everything your business does online.

Size Doesn't Make You Invisible

One of the first misconceptions I hear from business owners here along the Wasatch Front is the idea that they're too small to be worth attacking. “We're just an HVAC company.“ “We only have twelve employees.“ “Why would a hacker care about us?“

Here's the reality: the people behind these attacks aren't handpicking their targets. They're running a volume operation. They deploy automated tools that sweep across the entire internet probing for weak spots — outdated software, reused passwords, misconfigured remote access. These tools don't filter by company size. They filter by opportunity.

The statistics paint a clear picture. Nearly half of all cyberattacks land on small businesses. And of those that suffer a serious breach, six out of ten close their doors within half a year. If you're operating a twenty-person company in Sandy and you think your size keeps you off the radar, I'd gently ask you to reconsider. Automated scanning tools don't check your headcount. They check your defenses.

But here's the piece that should actually give you hope: the vast majority of these incidents aren't the result of some brilliant criminal mastermind outsmarting your technology. Industry research consistently shows that somewhere between sixty and ninety-five percent of breaches trace back to a human mistake — somebody clicking a suspicious link, reusing a compromised password, or falling for a convincing fake email.

If the root cause is that simple, the fix can be too.

Three Areas Worth Protecting

Every security decision you'll make connects back to one of three foundational areas. I think of them as pillars, and they're the lens through which we'll examine everything in this book.

Identity. This covers the people connected to your business, their login credentials, and the devices they use to access your systems. Sloppy habits here — passwords scribbled on sticky notes, former employees who still have active accounts, the owner who refuses to enable two-factor login — make everything else fragile. Getting identity right is your first and most important defensive

layer.

Data. This is the reason any of this matters in the first place. Your financial records, your client lists, your contracts, the intellectual property that makes your business yours. Understanding where this information lives, restricting who can reach it, and maintaining reliable copies that can survive a disaster — that's the safety net underneath everything.

Operations. This is the ongoing discipline. Keeping software current, watching for unusual activity, and having a clear plan for the day something goes wrong. It includes routine habits like calling to verify a vendor's bank account change before wiring funds, and bigger commitments like running regular backup recovery drills.

These three pillars support everything that follows. And the approach for each one boils down to two concepts: developing a few critical habits, and organizing those habits within a clear, repeatable plan.

The Buck Stops with You

I want to make one point emphatically, because everything else in this book depends on it.

The security posture of your company is not your IT department's responsibility. It's yours.

You'd never let your bookkeeper be the sole guardian of the company's financial well-being. That accountability rolls up to you. The digital health of your business works the same way. Your IT team or provider handles the technical implementation, but the ownership lives with leadership.

And I'll push this a step further. You can't simply assign this to someone and walk away. You have to set the example. When the owner bypasses the password policy because it's annoying, the entire team notices. When the owner ignores the security training everyone else was assigned, the message is clear: this doesn't really matter. When the owner carries the most privileged access in the company and simultaneously maintains the weakest security habits, the entire organization inherits that risk.

The tone is set from the top. Every single time. This book is here to give you the knowledge and confidence to set the right one.

> **FROM THE FIELD**
>
> Let me tell you the most common thing I find when I walk into a new client's environment for the first time. It's not a sophisticated vulnerability or a complex misconfiguration. It's an open computer. No password on the lock screen. No separate user profiles. Just a shared desktop that anyone — an employee, a visitor, a vendor rep, a cleaning crew member — can sit down at and access everything. Customer lists, financial documents, saved passwords in the browser, email accounts left logged in. I've seen this at dental offices, at law firms, at construction companies, at insurance agencies. Businesses you'd recognize. Businesses that look professional from the outside. The gap between what we assume about “well-run“ businesses and what's actually happening with their technology is one of the biggest lessons of my career.

Why Utah, Specifically

You might wonder why this book is written for Utah's business community and not just “businesses“ in general. There are a few reasons.

Utah is one of the fastest-growing states in the country, and the business landscape along the Wasatch Front is unlike anywhere else. We have the Silicon Slopes tech corridor stretching from Lehi to Draper, with companies scaling at incredible speed. We have a dense concentration of healthcare organizations — Intermountain Health, University of Utah Health, and hundreds of clinics and practices — all handling sensitive patient data under strict HIPAA requirements. We have a booming construction industry, thriving real estate and property management firms, professional services companies, manufacturing, and a proud tradition of family-owned businesses that have been here for generations.

Each of these industries has its own relationship with technology and its own blind spots. The construction company that runs everything from the owner's phone and a shared desktop in the trailer. The dental practice with an ancient server that hasn't been patched in two years. The Silicon Slopes startup that moved so fast building their product that nobody thought about securing the internal infrastructure.

Utah also has a unique business culture — one built on trust, personal relationships, and handshake deals. That's one of the best things about doing business here. But in cybersecurity, that trust can become a vulnerability. We trust our vendors, our neighbors, the people we do business with. Attackers exploit exactly that kind of trust.

This book is written with all of that in mind. The advice is universal, but the context is ours.

> **THE OWNER IN THE MIRROR**
>
> Before you turn this page, answer one honest question: Are you following every security policy that you expect from your employees? If the answer is anything but a firm “yes,“ that's the first thing to fix. Not tomorrow. Today.

CHAPTER 2

What It Costs When Things Go Wrong

Meet Rachel. She owns a small accounting firm in Draper with twelve employees. Tax season is her Super Bowl — twelve weeks where her team works sixty-hour weeks to get everything filed on time. Last March, during the busiest week of the year, one of her staff clicked a link in an email that looked like it came from the IRS. Within four hours, ransomware had encrypted the firm's entire file server. Client tax returns. Financial records. Payroll data. Everything. Rachel didn't have tested backups. She didn't have cyber insurance. The recovery took eleven days — eleven days in the middle of tax season. Between lost revenue, emergency IT costs, overtime to re-do work from paper copies, and the clients who left for another firm, the total cost was just over two hundred thousand dollars. Rachel's firm survived, but barely. She told me later that for the first three days, she genuinely didn't know if the business would make it.

So what's the actual payoff for investing in cybersecurity?

Honest answer: the return doesn't show up on a profit-and-loss statement. Not if things go right.

The real payoff is the catastrophe you never experience. It's the same logic behind insurance, fire suppression systems, and maintaining the brakes on your trucks. You spend a reasonable amount today to dramatically shrink the chances of a ruinous event tomorrow.

There's a straightforward way to think about this: **Expected Loss = How much damage an incident would cause × How likely it is to happen.**

Everything you invest in cybersecurity should be aimed at driving both halves of that equation toward zero.

Breaking Down the Real Damage

Let me put concrete numbers on what a cyber incident actually costs, because it extends far beyond whatever dollar figure flashes on a ransom demand.

Lost productivity and revenue. Picture your entire operation frozen for seventy-two hours. No orders going out, no invoices, no customer service. If your company generates ten thousand dollars a day in revenue, you've lost thirty thousand before you even start counting labor costs. Add payroll for a team that's sitting idle, plus the overtime needed to dig out of the backlog once you're running again. For a business like Rachel's accounting firm — hit during the one window where every day counts — the timing alone can multiply the damage exponentially.

Stolen funds. The most common version of this is a fraudulent wire transfer, usually triggered by a hijacked email thread. Someone impersonates a vendor or executive, convinces your accounts payable person to redirect a payment, and the money disappears into an overseas account. The FBI's Internet Crime Complaint Center reported that the average loss from a single one of these schemes is roughly a hundred and thirty-seven thousand dollars. Sit with that number for a moment. What would it mean for your business to lose that much cash in a single afternoon?

Recovery expenses. Once the attack is contained, the bills arrive. Forensic specialists to determine what happened. Lawyers to navigate your legal exposure. System rebuilding, data restoration, regulatory filings, and customer notification. For small and mid-size companies, these costs commonly range from six figures into the half-million-dollar range. For larger organizations, IBM's annual breach report puts the average north of four million dollars globally and above ten million within the United States. And roughly one in three cases now triggers regulatory penalties, with half of those fines exceeding a hundred thousand dollars.

Trust and reputation. This one is hardest to quantify but hits especially hard in Utah, where business runs on referrals and relationships. When your clients' personal data is exposed — their financial records, their medical history, their Social Security numbers — years of earned trust can collapse overnight. Rachel lost four clients in the month following her incident. They weren't angry. They were worried. Rebuilding that confidence takes far longer than rebuilding a

server.

Stack these up together and you can see how a single incident can push well into six figures of total damage. That's the math behind why so many small businesses don't recover.

I know this firsthand. I've stood next to the business owner as the scope sets in. I was the one in the Walgreens parking lot, writing a check to buy cryptocurrency because no other option existed. That company made it through. Others haven't.

Spending Where It Counts

So how do you shrink those numbers? Focus on the investments that deliver the largest, most direct reduction in risk.

Preventing account takeover. The single highest-value investment is multi-factor authentication — the second verification step when you log in, typically a code sent to your phone. It neutralizes the vast majority of attacks that rely on stolen or guessed passwords. Enabling MFA costs almost nothing compared to the six-figure wire transfer it prevents by keeping an attacker locked out at the front door.

Surviving ransomware. You need backup copies of your critical data that are tested and stored where an attacker can't reach them. This is what turns a potential weeks-long, business-killing crisis into a weekend recovery project. When everything is encrypted and a criminal is demanding payment, the difference between “we'll be operational by Monday“ and “we're seriously considering paying“ comes down to whether you have a clean, verified copy of your data that's isolated from the compromised network. Three out of four small businesses report they couldn't keep operating if ransomware hit them. A proven backup is the escape hatch.

Containing the blast radius. Modern endpoint protection tools and a disciplined approach to software updates shrink the damage when something does get through. Today's security tools don't just scan for known viruses — they watch for abnormal behavior and can automatically quarantine a compromised machine before the problem cascades across your network.

Security as a Growth Engine

Solid security practices don't just prevent losses. They can actively help you grow.

Keeping Your Insurance Valid

Cyber insurance policies now come with prerequisites. Carriers increasingly require evidence of specific controls — MFA, offline backups, endpoint protection — before they'll write a policy. More importantly, they require the same evidence before they'll pay a claim. I've heard from business owners along the Wasatch Front who faithfully paid their premiums for years, only to have their claim denied after an incident because they couldn't demonstrate basic controls were in place when it mattered.

A Word About Cyber Insurance

Cyber insurance deserves its own discussion because it's become both essential and frequently misunderstood by business owners.

First, let me be clear: cyber insurance is not a substitute for good security. It's a complement to it. Think of it like car insurance — having insurance doesn't mean you drive recklessly. You still wear your seatbelt, follow traffic laws, and maintain your brakes. But if something goes wrong despite your best efforts, insurance helps you recover financially.

Cyber insurance typically covers several categories of costs: forensic investigation (figuring out what happened and how), legal fees, customer notification costs, credit monitoring for affected individuals, business interruption losses, and sometimes the ransom payment itself in a ransomware attack.

The application process itself has become a useful forcing function. When you fill out a cyber insurance application, it essentially asks you to self-assess your security posture. The questions map closely to the habits and controls we discuss in this book. If you can answer “yes“ to everything on the application honestly, you're in good shape. If you find yourself wanting to fudge an answer, that's a red flag — both for your security and for your insurance coverage.

My recommendation: get cyber insurance. But get your security house in order first, so you can answer the application honestly and ensure your claims will be valid if you ever need to use the policy. The premiums are also significantly

lower for businesses that can demonstrate strong controls — so good security literally pays for itself through reduced insurance costs.

Winning Larger Contracts

When you can demonstrate robust security practices to a prospective client, you're signaling something important: this is a company that operates with discipline and takes stewardship of data seriously. Here in Utah, this matters more every year. Companies in the Silicon Slopes corridor routinely require their vendors to complete security questionnaires. Government contracts — and Utah has a significant concentration of them — often mandate adherence to specific frameworks. Being able to respond to those requirements with real, documented answers gives you an edge that most of your competitors simply can't match.

Standing Out Locally

Most businesses your size aren't doing this work. They're not validating their backups, not enforcing second-factor authentication, not following any organized plan. When you can demonstrate that you are — and prove it — you differentiate yourself in a market that runs on trust. In a state like Utah, where your reputation travels by word of mouth, being the company that takes this seriously builds confidence faster than any advertising campaign.

THE OWNER IN THE MIRROR

Think about that number — a hundred and thirty-seven thousand dollars gone in a single afternoon. Could your business absorb that loss tomorrow? If that thought makes your stomach tighten, keep reading. Everything in this book is designed to keep that number theoretical.

CHAPTER 3

The Playbook They Use Against You

Meet Carlos. He manages a real estate brokerage in South Jordan with twenty-five agents. One morning, his top-producing agent forwarded an email to the office manager: "Hey, the title company says they updated their wire instructions for the Morrison closing. New account info is attached." The office manager didn't think twice — they'd worked with this title company for years. She processed the wire for eighty-seven thousand dollars. The money went to a criminal's account overseas. The email hadn't come from the title company at all. The attacker had been quietly reading the agent's email for weeks, waiting for a transaction large enough to hijack. By the time anyone realized what happened, the money was gone. Carlos spent the next three months dealing with FBI reports, insurance claims, and very difficult conversations with his clients. The Morrison family's closing was delayed by six weeks. The thing that keeps Carlos up at night isn't that someone hacked his systems — it's that the attack was so simple, so human, that all the firewalls in the world wouldn't have stopped it. Only a phone call would have.

Forget everything the movies taught you about hackers. The threats facing your business don't involve dramatic countdowns or green code scrolling across a screen.

The actual picture is far more boring — and far more dangerous. The people behind these attacks think like business operators. They measure efficiency. They optimize their return on investment. They lean on a tight set of proven tactics that reliably generate revenue, and they run those plays over and over against anyone whose defenses leave an opening.

This chapter walks through that playbook. Once you recognize the patterns, you'll be in a much stronger position to shut them down.

The Utah Threat Landscape

Before we dive into specific tactics, it's worth understanding why businesses in our state face a particularly interesting risk profile.

Utah has been among the fastest-growing economies in the country for years. The Silicon Slopes tech corridor has attracted enormous investment and rapid hiring. But fast-growing companies tend to prioritize speed over everything else. When you're doubling headcount in a year, nobody pauses to audit whether the new sales rep's system permissions are scoped correctly, or whether that “temporary“ file server from three years ago is still the backbone of daily operations.

Our state also has unusually heavy representation in the industries that attackers specifically target. Healthcare blankets the Wasatch Front — Intermountain Health, University of Utah Health, and thousands of independent practices, dental offices, and clinics. Every one of them handles protected patient data that commands a premium on the dark web. Medical records contain the full package for identity theft — names, addresses, Social Security numbers, insurance details — which is why they're worth far more per record than a stolen credit card number.

Construction and real estate are booming here, and both move large sums through wire transfers during closings, equipment purchases, and project draws. A single intercepted transfer can vaporize tens or hundreds of thousands of dollars, as Carlos learned.

Professional services firms — accountants, attorneys, consultants, insurance agencies — sit on troves of client data without always recognizing themselves as high-value targets. A breached law firm doesn't just lose its own files; it potentially compromises confidential information for every client it represents.

Manufacturing and logistics outfits along the I-15 corridor increasingly depend on networked production systems. Ransomware that freezes the shop floor doesn't just hurt the manufacturer — it ripples through every customer and supplier in the chain.

The threats in this chapter aren't abstract. They're landing on businesses in your zip code, in your industry, right now.

Attacks That Target People

The majority of security incidents don't start with someone defeating a technical barrier. They start with a person making a decision — often in a split second, under the pressure of a busy workday. The 2025 Verizon Data Breach Investigations Report identified a human factor in sixty percent of the breaches it studied. Attackers understand that your people are simultaneously your greatest asset and your most exploitable surface.

Phishing and Social Engineering

The concept is as old as the con itself — trick someone into doing something against their own interest. In the digital version, this usually means persuading a person to click a harmful link, open a weaponized attachment, or hand over their login credentials.

Bulk phishing is the spray-and-pray approach. Millions of generic messages go out — fake shipping notifications, bogus account suspension warnings — banking on the law of large numbers. A tiny hit rate across a massive volume still generates plenty of victims.

The targeted variant — sometimes called spear phishing — is where things get truly dangerous. Here, the attacker invests time studying your organization. They identify the people who handle money or sensitive data, and they craft messages designed to blend seamlessly into normal business communications.

This precision targeting often evolves into what the industry calls Business Email Compromise. The attacker gains access to a legitimate email thread — or creates a convincing imitation — and waits for the right financial moment to redirect funds. That's precisely what happened to Carlos in South Jordan. The criminal had been silently monitoring his agent's inbox for weeks, waiting for a wire transfer large enough to justify the effort.

The FBI reports that BEC schemes generated nearly 2.8 billion dollars in reported losses across the United States in 2024 alone. In Utah's real estate, construction, and professional services sectors — where large payments change hands regularly — the target-rich environment is especially favorable for

attackers.

Here's the counterintuitive part: falling for these scams has almost nothing to do with intelligence. Research shows that the median interval between a phishing email arriving and the recipient clicking the link is under twenty-five seconds. People aren't being stupid. They're being human — busy, distracted, and moving fast.

The telltale signs almost always include: artificial urgency designed to short-circuit your judgment (“Act now or your account will be locked“), requests that deviate from established processes (especially with an instruction to keep things quiet), and small inconsistencies like a misspelled domain name or a link destination that doesn't match what's displayed.

> **FROM THE FIELD**
>
> I've seen phishing messages that are nearly flawless — correct logo, professional language, and the sender's name matching someone the recipient works with regularly. The only giveaway was a single letter difference in the email domain. In a busy office where someone is juggling twenty tasks, that detail slips right past. This isn't a failure of intelligence. It's a failure of process. The fix isn't “pay closer attention.“ The fix is building a verification step into your workflow that takes thirty seconds and catches a hundred-thousand-dollar mistake.

Insider Threats

This is uncomfortable territory because it involves the people you've chosen to bring into your organization.

An insider threat materializes when someone with legitimate access — a current employee, a former team member, a contractor, a business partner — uses that access in a way that harms the organization. A 2024 industry report found that nearly half of businesses surveyed had seen an increase in these incidents

compared to prior years.

Not every case involves bad intentions. An employee might forward a client spreadsheet to their personal email so they can catch up over the weekend. The intent is good. The result is company data living outside your security controls, exposed to whatever risks that personal account carries.

The deliberate version looks different. A departing employee downloads client records to bring to their next job. A contractor whose engagement ended months ago still has active credentials because nobody remembered to shut them off.

The right response isn't to distrust your people. It's to build reasonable guardrails — the same way you'd implement financial controls even if you had complete faith in your bookkeeper. Smart access management protects honest employees from accidental mistakes and the organization from intentional ones.

Attacks That Target Technology

People may be the entry point, but technology is the door they walk through. Even after an attacker tricks someone into revealing credentials, they still need a technical pathway into your systems. And they have sophisticated, automated tools hunting for those pathways around the clock.

Compromised Credentials

The usernames and passwords your team uses every day are currency in criminal markets. When a large company experiences a data breach — and these happen constantly — the stolen login data ends up for sale on underground marketplaces. Criminals purchase these databases in bulk and feed them into automated tools that methodically test each username-and-password pair against login portals across the internet, including yours.

This technique works because people reuse credentials. Studies indicate that roughly half of workers use identical passwords across multiple professional applications. If someone on your team used the same credentials for a social media account that was breached years ago and for your company's email today, that old compromise just became your current crisis.

That sounds far-fetched until you consider that compromised credentials are involved in the vast majority of web application attacks — upward of eighty-five

percent according to recent data.

How Credential Theft Plays Out in Practice

Let me walk through the mechanics, because understanding the chain makes it feel less abstract and more urgent.

First, a major company suffers a breach. Millions of username-and-password combinations are stolen. This happens regularly — dozens of significant breaches affecting hundreds of millions of accounts over the past decade, some of which go undetected for months or years.

Second, those credentials surface on underground markets, sold in bulk for a few hundred dollars. Third, a criminal loads them into automation tools that can test thousands of combinations per minute against any login page — your Microsoft 365 portal, your VPN, your CRM, your accounting platform.

Fourth, because people reuse passwords, some combinations match. The attacker is in. Fifth — and this is critical — they don't announce their presence. They log in quietly, start reading emails, study your financial workflows, and wait for the opportune moment to act. They might set up hidden forwarding rules on the compromised mailbox so copies of incoming messages flow to their own account. Weeks or months might pass before they make a move.

This is the most common attack chain against small businesses right now. And it all collapses if you have MFA enabled, use a password manager to eliminate reuse, and monitor for unusual login patterns.

Warning signs to watch for: login notifications from unfamiliar locations or odd hours, unexpected account lockouts, messages in your sent folder that you didn't write, or files showing access timestamps from periods when nobody was working.

Unpatched Software and Exposed Services

This category is growing faster than any other, grounded in a simple premise: automated tools ceaselessly probe the internet for known weaknesses. The 2025 Verizon report documented a thirty-four percent year-over-year increase in breaches where exploiting a technical vulnerability was the first step.

Two varieties dominate. The first is known software flaws. When a company like Microsoft or Google identifies a security defect in their product, they publish a fix. The instant that fix is announced, criminal operations begin scanning for organizations that haven't applied it. With over twenty-one thousand new vulnerabilities catalogued in just the first half of 2025, the supply of fresh targets never runs dry.

The second is improperly secured remote access. Tools like VPNs and remote desktop services are essential for modern work, especially along the Wasatch Front where employees might be connecting from Ogden, Park City, or their kitchen table in American Fork. But when these tools are deployed with weak credentials and no second-factor authentication, they become visible entry points that attackers can discover and exploit with minimal effort.

The math is brutally unfavorable: attackers can weaponize a newly disclosed flaw within hours, while the average organization requires roughly two months to patch even half of its critical vulnerabilities. That gap is where breaches happen.

Supply Chain Compromise

No business operates alone. You depend on software vendors, IT providers, accounting platforms, payroll services, and countless other third-party connections. A supply chain attack targets one of these trusted partners and uses that partner's legitimate access as a bridge into your environment.

The efficiency is what makes this approach so attractive to criminals. Instead of targeting a hundred small businesses individually, compromise the single software tool they all depend on and you gain access to all of them simultaneously.

These attacks have doubled in frequency since early 2025. Roughly a third of all breaches now involve a third party, and vendor access accounts for over forty percent of ransomware incidents.

In Utah, where business runs on trusted relationships and long-standing partnerships, this vulnerability deserves special attention. The security of your payroll provider directly affects your employees' personal data. A compromise at your IT provider could hand an attacker administrative control over your entire infrastructure. Your security perimeter extends to encompass every partner

you're connected to.

Attacks That Target Operations

Once an attacker has bypassed your people and your technology, the next step is converting that access into a payday. These are the threats that go directly after your ability to function, generate revenue, and serve the people who depend on you.

Malware and Ransomware

Malware is the umbrella term for hostile software — keyloggers that record every keystroke, spyware that quietly harvests data, remote access tools that let an attacker wander through your network undetected for weeks.

Ransomware is the strain that dominates headlines, and I have personal experience with it. I was the guy in the Midvale parking lot.

Ransomware is weaponized software with a revenue model. After exploring your network and identifying what matters most, the attacker deploys code that rapidly encrypts everything — files, databases, applications — and demands payment for the decryption key.

The pressure doesn't stop there. Modern ransomware operations almost universally steal a copy of your data before encrypting it, then threaten to publish everything unless you pay. This two-pronged approach appears in roughly a third to nearly half of all breach incidents.

Recognizing malware: subtle signs like unexplained sluggishness, odd pop-ups, unexplained crashes, or unfamiliar programs running in the background. It's built to stay hidden. **Recognizing ransomware:** impossible to miss. Every screen displays a demand for payment, and nothing on your system will open. Maximum disruption is the entire point.

Service Disruption Attacks

Not every attack aims to steal something. Some exist purely to cause chaos.

Picture someone arranging for a hundred callers to flood your single phone line simultaneously and continuously. Your actual customers can't get through. That's

the basic idea behind a Denial-of-Service attack — overwhelming your website or online systems with so much garbage traffic that legitimate users are shut out.

These incidents surged over forty percent year-over-year in the first half of 2025 globally. The largest documented attack reached 7.3 terabits per second, marshaling hundreds of thousands of compromised devices worldwide.

Warning signs: your website or online tools become unusually slow or completely unreachable, traffic volumes spike far beyond any normal pattern, or you receive a message demanding payment to halt the flood.

That's the playbook — seven categories of tactics that criminals deploy repeatedly against organizations of every size, across every industry, in every geography. Including the Wasatch Front.

The remainder of this book is dedicated to making sure those tactics fail when they're pointed at you.

CHAPTER 4

Follow a Framework — Your Security Blueprint

Meet Lisa. She runs a growing property management company in Orem — forty employees, about six hundred units under management. Lisa knew she needed better security after a phishing scare, so she bought an expensive email security tool. Then she heard about ransomware, so she signed up for a backup service. Then a competitor got breached, so she rushed to get cyber insurance. Each purchase made sense in the moment, but when I sat down with Lisa to look at the whole picture, we found major gaps. She had no device inventory. Nobody had tested the backup. Two employees still had admin rights they didn't need. Her email security was solid, but the rest of the program was scattered. Lisa had spent real money, but she'd been playing whack-a-mole — reacting to whatever scared her that week instead of following a plan. That's what a framework prevents.

It's easy to fall into the pattern Lisa did. A scary headline about ransomware triggers a backup purchase. A phishing story inspires a training subscription. A competitor's breach sends you scrambling for insurance. Each reaction feels productive in the moment, but without an organizing structure, you end up with scattered investments and dangerous blind spots. You've plugged some holes while leaving others wide open, and you don't even know which ones.

A recognized security framework solves this by giving you a map. Instead of reacting to the latest fear, you follow a deliberate path that ensures nothing critical gets overlooked.

NIST Cybersecurity Framework 2.0

For businesses operating in the United States — and particularly along the Wasatch Front — the framework published by the National Institute of Standards and Technology is the most practical starting point. It organizes your entire security program around six core functions: **Govern, Identify, Protect, Detect, Respond, and Recover.**

NIST is part of the U.S. Department of Commerce, and their framework has become the de facto standard for how organizations talk about security. That matters for you directly: when a larger company sends you a vendor security questionnaire — and if you're bidding on contracts in the Silicon Slopes corridor, supplying Hill Air Force Base, or working with any of the federal facilities in this state, they will — the questions almost always trace back to NIST. Fluency in this framework means you already speak their language.

The 2.0 revision introduced “Govern“ as a central function, formally acknowledging what should have been obvious from the start: security is a leadership discipline, not a technical one.

Here's each function translated into plain business terms:

Govern. Establish the rules of the road. Decide who's accountable for security decisions, define how much risk you're willing to accept, and make sure those expectations are communicated clearly. This is where policies are born and where leadership sets the tone.

Identify. Catalog everything that matters. Build a comprehensive picture of the systems, accounts, data stores, and vendor relationships that your business depends on. The principle is simple: you can't defend assets you don't know you have.

Protect. Deploy the core safeguards. Strong authentication, current endpoint protection, reliable backups, and staff awareness training all live here. This function is where your daily habits take shape.

Detect. Maintain active surveillance. Monitor your environment for anomalies, flag suspicious behavior, and catch emerging threats before they escalate into full incidents.

Respond. Have a playbook ready. Define the steps your team follows when something goes wrong so that nobody is improvising under pressure. Clear roles, communication plans, and containment procedures live here.

Recover. Restore and learn. Bring operations back to normal from clean backups, verify that the threat has been eliminated, and capture lessons that strengthen your posture going forward.

Why Structure Beats Reaction

A framework prevents you from building a lopsided program — investing heavily in one area while neglecting others. Lisa had excellent email security and zero device management. A framework would have surfaced that imbalance immediately.

It also gives you a management tool. You don't need to understand every technical detail. You just need to ask your IT provider: “Where do we stand on the 'Detect' function this quarter? Show me the evidence.“ The six functions become a straightforward scoreboard for tracking progress and enforcing accountability.

Lisa's experience is a textbook example. She was spending real money on security — that wasn't the issue. The issue was that every dollar went toward whichever threat caught her attention that week. Once she laid her existing tools against the NIST framework, the gaps became immediately visible, and she could prioritize filling them in order of actual risk rather than headline anxiety.

CIS Controls: The Prioritized Checklist

If you prefer a more prescriptive format — a ranked to-do list rather than an organizing structure — the CIS Critical Security Controls offer exactly that. Maintained by a community of security practitioners and informed by real-world attack data, CIS Controls provide a concrete sequence of actions prioritized by impact.

For small businesses, Implementation Group 1 (labeled “essential cyber hygiene“) contains fifty-six specific actions considered non-negotiable regardless of size or industry. They cluster around familiar themes: inventory your hardware and software, establish core habits like multi-factor authentication and patching, and build foundational disciplines like tested backups, basic security training, and a simple incident response plan.

NIST and CIS complement each other well. NIST gives you the architecture; CIS gives you the punch list. Pick whichever resonates with how you think, and start.

For organizations doing business internationally that need to demonstrate security to global partners, ISO 27001 certification provides a recognized standard. It's a more formal, audit-based process, but the underlying principles are consistent with everything we've discussed.

The Core Lesson

Whether you adopt NIST, CIS, or any structured approach, the critical thing is to follow something. A framework converts reactive, fear-driven spending into a deliberate program. It provides a coherent path forward, a credible story to tell customers and insurers, and an ongoing routine that replaces anxiety with process.

Everything in the chapters ahead — the specific controls, the habits, the questions to ask your IT provider — should be implemented within the context of a framework. That way, you'll always be addressing the highest-priority gap first, not just chasing whatever headline scared you most recently.

> **THE OWNER IN THE MIRROR**
>
> Have you ever purchased a security tool because a news story frightened you, rather than because an organized plan called for it? That's the reactive approach. A framework replaces fear with structure.

PART II — The Controls That Matter

CHAPTER 5

People & Identity — Starting with You

Meet Jeff. He owns a dental practice in Murray — three dentists, four hygienists, a front desk team, and an office manager. Jeff is a great dentist. He's also the person in his practice with the weakest password, no MFA on his email, and admin access to every system in the building. When I asked why, he shrugged and said, "It's my practice. I need to be able to get into everything." I pulled up his Microsoft 365 admin portal and showed him that his account — the one with the simplest password and no second factor — had access to every patient record, every financial document, and every employee file in the practice. If an attacker compromised Jeff's account, they wouldn't just get into one system. They'd get into everything. Every HIPAA-protected patient record. Every bank statement. Every employee's Social Security number. Jeff didn't have a security problem. Jeff was the security problem. And the worst part is, Jeff is one of the good ones — he genuinely cared about doing the right thing. He just didn't realize he was the weakest link in his own chain.

Your business holds valuable digital property — client records, pricing models, financial data, proprietary processes. Without deliberate controls around who can reach what, these assets can leave when employees leave, surface accidentally through misconfiguration, or be extracted wholesale during an attack.

This chapter addresses who holds the keys to your digital kingdom. Every person connected to your operation — staff, contractors, outside accountants — needs specific, bounded access to do their work. The objective is ensuring each person reaches only what their role requires, and only for as long as that role exists.

But before we get into the specific habits, I need to address the person holding this book.

The Pattern I See Most Often

Across every industry I've worked in, the single most frequent security gap isn't technical. It's behavioral. And it starts at the top.

Business owners routinely exempt themselves from the very policies they set for everyone else.

The pattern is remarkably consistent. I'm told confidently that the whole company is using two-factor authentication. I open the admin dashboard and find a handful of exceptions. Almost invariably, one of them is the owner.

The justification varies. “It's my company — I need quick access.“ “I'm too busy for the extra step.“ “I know what I'm doing.“ Meanwhile, this person carries the broadest permissions in the organization, has access to the most sensitive information, and represents the single highest-value target an attacker could compromise.

The security culture of any company I've ever assessed is a direct mirror of the owner's personal habits. If you take it seriously, your team absorbs that. If you cut corners, they notice — and they follow your lead.

Four Habits That Deliver Maximum Impact

These four practices, executed consistently, neutralize the majority of identity-related risks. They're not complicated. They just need to be non-negotiable.

1. Require Multi-Factor Authentication Everywhere

You already use this concept with your bank — enter your password, then confirm with a code from your phone. The first element proves you know the password. The second proves you possess the device. An attacker who steals one without the other is stuck.

This matters because credential theft is constant and pervasive. The question isn't whether your employees' passwords have been exposed somewhere — it's how many have been, and when. Without a second verification step, a criminal holding a compromised password walks straight in. With that second step, the stolen password becomes worthless. The attacker reaches the login prompt, gets

challenged for a device code they don't have, and the intrusion dies on the spot.

Microsoft's own data indicates that second-factor authentication defeats 99.9 percent of automated credential attacks. The 2025 Verizon breach report found stolen login data implicated in roughly nine out of ten web application attacks. This single control directly addresses the primary attack vector.

Despite this, research shows that close to half of small and mid-size companies still operate with passwords as their sole barrier. The gap between what the evidence says works and what businesses actually do is staggering.

This is also the control that your insurance carrier is most likely to verify. Increasingly, proving MFA enrollment on email and remote access systems is a prerequisite for both policy issuance and claims approval.

> **FROM THE FIELD**
>
> Here's what I see constantly along the Wasatch Front: A business owner tells me confidently that everyone in the company uses MFA. I pull the report. Ninety percent enrolled. Sounds solid, right? Except in a twenty-person company, ninety percent means two people don't have it. And those two unprotected accounts are the ones an attacker will find. Security isn't a batting average. It's a chain. One weak link breaks the whole thing. One hundred percent means one hundred percent — including the owner.

---

2. Deploy a Business-Grade Password Manager

Here's the reality of passwords: the typical professional juggles dozens of them, sometimes approaching a hundred. Memorizing that many distinct, complex strings is a task the human brain simply wasn't designed for. People cope with shortcuts — recycling the same password across sites, appending a number to an old favorite, building passwords from family names or pet names, or sticking them on a note attached to the monitor.

These adaptations aren't laziness. They're predictable human behavior in the face of an impossible task. The solution isn't lecturing people to try harder. It's providing a tool that makes strong, unique credentials effortless.

A password manager generates a random, unguessable credential for every account and stores them all in an encrypted vault. Each employee memorizes one strong passphrase to unlock their vault; the manager handles everything else. Password reuse vanishes overnight because every site gets its own unique string. The weakest credentials disappear because the manager generates complexity that no human would create on their own.

These tools also solve the shared-account challenge. Company social media logins, vendor portals, shared service accounts — instead of circulating the password through email or a spreadsheet, you grant specific individuals access through the manager without them ever seeing the underlying credential. When someone departs, revoking their access to every shared account takes a single click.

3. Restrict Access to What Each Role Actually Requires

Every person in your organization should hold the minimum level of system access their job demands. Nothing beyond that.

Your marketing coordinator needs access to the marketing folder and social media accounts, not the payroll system. Your salespeople need the CRM, not the HR files. This sounds obvious, but in practice, most businesses hand out permissions liberally — “just in case“ someone might need something — and almost never review or revoke them.

After a few years of this, you end up with a situation where the majority of your staff can reach the majority of your data. That's a problem because the damage from any single compromised account scales directly with that account's reach. If someone on your sales team gets phished and their credentials are stolen, an attacker inherits whatever that salesperson could access. If that's just the sales pipeline — the blast radius is limited. If it's everything because nobody scoped their permissions — the entire company is exposed.

A 2025 industry report found that forty-one percent of attacks leveraged overly broad permissions to navigate through the victim's network and escalate the damage. Tightening access strips that capability away.

FROM THE FIELD

I worked with a construction company that had been growing quickly — they went from eight employees to thirty in about two years. Every new person who came on board got basically the same access as the person before them. By the time I looked at their system, every single employee — from the project manager to the newest laborer who only needed to submit timesheets — could reach the entire shared drive. Financial records, bid documents, employee files, client contracts. Nobody had reviewed access in over a year. It wasn't malice. It was just growth without process. We spent a Saturday morning creating four access groups based on actual job functions, and it took about three hours. Three hours to fix a vulnerability that had been growing for two years.

4. Formalize the Onboarding and Offboarding Process

You need two documented checklists — one that governs how a new person is provisioned, and one that governs how a departing person is de-provisioned. I've included templates for both in the appendices.

The onboarding process ensures that a new hire receives only the access their specific role requires, provisioned deliberately rather than cloned from whoever held the job previously.

The offboarding process is arguably the more critical of the two. The instant a departure is confirmed, this checklist activates. It should enumerate every account the person touches — email, network login, every SaaS application the company uses — and the target should be complete deactivation within minutes, not days.

Speed here matters enormously. Research indicates that roughly a third of workers acknowledge accessing a former employer's systems after leaving. Studies from 2025 show that the vast majority of organizations carry dormant accounts from long-departed personnel — legacy credentials sitting active and

unmonitored, invisible invitations for anyone who discovers them.

What Effective Training Actually Looks Like

Since annual training videos accomplish almost nothing, let me describe what does work.

Effective awareness programs share three traits: they're brief, they're recurring, and they connect to threats the audience actually faces.

Brief means each touchpoint lasts five minutes or less. A three-minute video on recognizing suspicious messages, delivered monthly, embeds far more than a marathon session administered once a year.

Recurring means training happens on a steady cadence. Monthly touchpoints — a short video, a simulated phishing exercise, a tip in the company newsletter — keep vigilance present in daily routines. The objective is reflex-building, not box-checking.

Relevant means the content maps to your actual risk landscape. Generic awareness material washes right over people. Training that says “here is exactly what a fraudulent invoice email targeting our industry looks like, and here is the specific procedure we follow when one arrives“ sticks. If you operate a real estate firm, train on wire fraud scenarios. Medical practice? Train on HIPAA-themed phishing. Construction company? Train on the fake vendor payment redirects that target accounts payable.

The strongest security cultures I've observed in Utah businesses have one trait in common: the owner participates visibly. When the boss shows up in the training completion reports, discusses the latest phishing simulation in team meetings, and models attentive behavior personally — that's when the culture genuinely shifts.

Mistakes That Undermine the Work

Sharing administrative credentials. Common in smaller shops — one “admin“ login for a critical system, passed around to everyone who needs it. The moment something goes wrong, there's no trail to follow. Multiple people had the keys; nobody knows who turned the lock. The rule is absolute: one human being, one unique account. Every time.

One-and-done training. An annual compliance video that employees click through while checking their phones changes no behavior. Short, frequent, specific — that's the formula that actually shifts habits.

Questions to Put to Your IT Provider

“Pull me a report showing every user enrolled in MFA. I want to confirm it's one hundred percent — and I want to see my own name on the list.“ Accept nothing less than full coverage. A single exception is the gap an attacker will exploit.

“Walk me through our offboarding procedure. From the moment I tell you someone is leaving, how fast are they fully disconnected?“ You need a concrete commitment measured in minutes — and a written checklist, not an informal understanding.

“Generate a list of every account with administrative privileges. Let's review it together and confirm each one is still justified.“ Only you, as the business owner, can judge whether each person on that list genuinely requires that level of access today.

> **THE OWNER IN THE MIRROR**
>
> Pull up your email admin dashboard right now. Look at the MFA enrollment report. Is every single account covered — including yours? If even one is missing, that's the opening an attacker is looking for.

CHAPTER 6

Devices & Endpoint Security

Meet Angela. She runs a staffing agency in Taylorsville with thirty employees, half of whom work from home at least part of the week. One Friday afternoon, a recruiter left her laptop in her car while she ran into Costco. When she came back twenty minutes later, the window was smashed and the laptop was gone. The laptop had no disk encryption, no remote wipe capability, and a password that was the recruiter's dog's name. On that laptop: the personal information of over two thousand job candidates — Social Security numbers, addresses, employment history, salary expectations. Angela had to notify every single one of them. She had to file a breach report. She had to hire a lawyer. The total cost was just under a hundred thousand dollars, and the reputational damage to her staffing agency — a business built entirely on trust — was even worse. A forty-dollar laptop lock and a free encryption setting built into Windows would have made this a non-event. Instead, it nearly ended the business.

Every laptop, desktop, phone, and tablet that connects to your business is a potential doorway for an attacker. A single unmanaged machine can pick up malicious software from one careless click and propagate it to your main systems within minutes, crippling everything.

This chapter focuses on making sure every piece of hardware that touches your data is accounted for, hardened, and current. We're shifting from controlling who has access to controlling what they access it with.

Four Habits That Prevent Most Problems

1. Maintain a Real-Time Device Inventory

This is foundational. You need a living, current record of every computing device used for your business — not a static spreadsheet from two years ago, but an operational view of what's connected right now.

If a device goes missing — as Angela's recruiter discovered in the Costco parking lot — you need to know immediately what's unaccounted for so you can lock or erase it remotely. When an incident occurs, the first question investigators ask is “which device was involved?“ Without an accurate inventory, you're guessing during the window when speed matters most.

A well-configured inventory tool also serves as an early detection system, alerting you when an unfamiliar device appears on your network or when a known device stops reporting in.

2. Enforce Baseline Security on Every Machine

Every device that reaches your data needs to meet a non-negotiable minimum standard.

Full-disk encryption must be active on every laptop and desktop. Both Windows (BitLocker) and macOS (FileVault) include this capability natively — it just needs to be turned on. Encryption renders the contents of the hard drive completely unreadable without the correct credentials. If hardware is lost or stolen, the thief gets a paperweight, not your customer database. Without encryption, a stolen laptop is a complete data breach — everything on the drive is open for the taking. Industry data indicates that physical loss or theft contributes to roughly one in five security incidents. Encryption is the direct countermeasure.

Administrative privileges should be removed from daily-use accounts. “Admin rights“ grant the power to install software and alter system configurations. When an employee with admin privileges clicks a malicious link, any code that executes inherits those same elevated powers — it can disable protective software, install persistent backdoors, and propagate across the network. A 2025 report documented that forty-one percent of attacks exploited overly broad privileges to move laterally and deepen the compromise. Removing admin access from routine accounts creates a substantial obstacle for most attack patterns. When someone legitimately needs new software, a quick approval-and-install workflow through your IT provider handles it without exposing the entire system.

3. Deploy Modern Endpoint Protection

The antivirus software that served you a decade ago operates on a fundamentally outdated model. It maintains a catalog of known threats and scans incoming files against that list. If a file matches a known signature, it gets blocked. If it doesn't, it passes through.

The problem is that modern attackers have moved far beyond file-based malware. The most dangerous techniques today are “fileless“ — they hijack your computer's own legitimate tools (scripting engines, administrative utilities) to accomplish malicious objectives without ever dropping a recognizable virus. Traditional signature-based scanning is completely blind to this approach.

Endpoint Detection and Response tools take a fundamentally different approach. Instead of matching files to a blacklist, they observe behavior. They recognize when a word processing application starts attempting to encrypt files, or when an administrative tool begins communicating with an unfamiliar server overseas at an unusual hour. When something suspicious is detected, a good EDR platform can automatically quarantine the affected machine — severing its network connection before the problem can spread.

The tooling alone is only half the equation. Those alerts need a human being watching and responding. This is something I feel deeply about. At Brivy, every endpoint we deploy comes with managed detection and response, monitored around the clock by a security operations center. What pays off each day isn't a single dramatic save — it's my peace of mind, knowing the business owners I've committed to protecting are actually protected. It's craftsmanship: doing the work right when nobody is looking, not skipping steps, not treating the admin console as merely a place to add users and assign licenses. There is tremendous depth in these systems, and bringing skill and care to that depth is a point of pride.

Why Legacy Antivirus Falls Short

Traditional antivirus operates like a bouncer checking names against a list. If your name is on the list, you're turned away. If it's not, you walk right in. That model collapses when adversaries generate hundreds of thousands of unique malware variants daily and increasingly abandon malware entirely in favor of abusing your own system tools.

EDR shifts from “is this a known threat?“ to “is this behavior normal?“ That shift is the difference between catching today's attacks and missing them entirely.

4. Stay Current on Software Patches

When a vendor discovers a security defect in their product, they publish a correction. The instant that correction is announced, a race begins. You're trying to apply it. Criminals are scanning for everyone who hasn't.

The criminals usually have the speed advantage. They can operationalize a new exploit within hours. The typical organization needs close to two months to remediate even half of its critical vulnerabilities. That gap is the window through which breaches occur.

Your patching cadence doesn't require complexity — it requires consistency. Operating system and browser updates should be applied weekly. For critical zero-day vulnerabilities under active exploitation, the turnaround needs to be a day or two. Your IT provider should automate this process and deliver a monthly compliance report showing what percentage of your fleet is fully current.

The 2025 Verizon report found that exploitation of unpatched software now accounts for one in five breaches, up significantly from prior years. Nearly twenty-nine thousand new vulnerabilities were catalogued in 2024. A disciplined patching routine closes the gap that attackers depend on.

Common Pitfalls

Granting admin rights for convenience. The reasoning sounds practical — “it's easier if they can install things themselves.“ But when a malicious link is clicked, any resulting code executes with whatever privileges the user holds. Admin access means the malware can embed itself deeply, disable defenses, and move laterally. Revoking admin rights is one of the highest-impact, lowest-effort changes you can make.

Ignoring personal devices. When employees use personal phones or laptops for work tasks, the question becomes: are those devices encrypted? Password-protected? Running current software? If a personal phone carrying company email disappears, your data goes with it. If personal devices touch business systems, they need to meet minimum standards.

Questions for Your IT Provider

“Show me a report confirming every device accessing our environment is encrypted.“ Complete coverage. No exceptions. This is what turns a stolen laptop from a breach into an inconvenience.

“If a device is lost or stolen, what's the timeline to remote lock or wipe it?“ You need a specific commitment backed by a documented procedure.

“What endpoint protection platform are we running, and who is monitoring the alerts around the clock?“ The first answer should reference EDR, not traditional antivirus. The second answer matters more — an alert that nobody sees at 2 AM is an alert that doesn't help.

> **THE OWNER IN THE MIRROR**
>
> Your laptop likely carries more permissions than any other device in the building. Is it the most hardened machine in your fleet, or the most exposed? When did it last receive an update?

CHAPTER 7

Email, Web, & Collaboration Security

Meet Tom and his wife Brittany. They run a mid-size landscaping and hardscaping company in Herriman — twenty-two employees, a fleet of trucks, and contracts with several HOAs and commercial property managers along the Wasatch Front. Brittany handles the books. One Thursday afternoon, she received an email from what appeared to be their biggest commercial client — a property management company they'd worked with for three years. The email said the client had switched banks and included new wire instructions for an outstanding seventy-two-thousand-dollar invoice. The email came from the right person's name, referenced the correct project, and even included their standard email signature. Brittany processed the payment. Two days later, the real client called asking about the overdue invoice. The email had been sent by an attacker who had been reading the client's email for weeks, waiting for the right invoice to intercept. The seventy-two thousand dollars was gone. Tom told me later that the hardest part wasn't the money — it was looking at Brittany and knowing she felt responsible for something that wasn't her fault. She'd done exactly what anyone would have done. The only thing that would have caught it was a phone call to verify the bank change. They didn't have that process. Now they do.

Email, messaging platforms, and collaboration tools form the circulatory system of modern business. They carry everything — invoices, contracts, customer records, confidential plans, day-to-day communications. That centrality is exactly what makes them prime targets.

The FBI reports that Business Email Compromise — the category of fraud that hit Tom and Brittany — generated close to 2.8 billion dollars in domestic losses during 2024, with typical incidents costing around fifty thousand dollars each.

Phishing delivered through email remains the dominant pathway into business networks.

Four Protective Habits

1. Layer Advanced Email Filtering

The built-in protections that ship with Microsoft 365 or Google Workspace handle routine spam and known malicious attachments reasonably well. They were not engineered to intercept a carefully researched, personalized attack crafted by someone who has studied your organization.

Dedicated email security platforms add capabilities the defaults don't provide. When an attachment arrives, the tool detonates it in an isolated sandbox environment to observe whether it exhibits malicious behavior. Links embedded in messages are evaluated in real time — if an employee clicks through to a credential-harvesting page or malware distribution site, the tool intervenes before any damage occurs. Research indicates that email serves as the delivery vehicle for upward of ninety percent of malware. This layer catches the threats that basic filtering lets through.

2. Establish an Ironclad Verification Process for Payments

This is a procedural control, not a technical one. And it's the single most effective countermeasure against wire fraud. Tom and Brittany's experience is exactly why it needs to exist.

The rule: any request to alter a vendor's banking information, or to process an unscheduled or urgent payment, must be confirmed through a live voice conversation at a phone number you already have on file. Not a number extracted from the suspicious message itself. Not a text. An actual phone call to a number you independently trust.

This works because it breaks the attacker's confinement. The entire fraud depends on you staying within their controlled channel — email. The moment you step outside that channel and verify through an independent one, the deception collapses.

In Utah, where professional relationships are personal and trust runs deep, this particular vulnerability is amplified. We're inclined to take people at their word. Attackers weaponize that inclination. Establishing a verification policy isn't a sign of distrust toward your vendors — it's a sign of disciplined operations. And it protects your employees from the devastating guilt of having processed a fraudulent payment they had no realistic way of spotting.

FROM THE FIELD

Phishing pages have become disturbingly convincing. An employee receives a message that appears to come from Microsoft — “Your password is expiring, click here to update it.“ They click through and land on a page that's visually identical to the real 365 login portal. Same design, same branding, same layout. They enter their credentials and hit submit. Nothing obvious happens, so they try again, maybe get redirected to the real site, and move on with their day. What actually happened: every keystroke went straight to the attacker, who now holds their username and password. If MFA isn't configured — or if the attack is sophisticated enough to intercept the second factor in real time — the attacker is inside the mailbox within seconds. A web filter catches this before the employee ever reaches that fake portal. It evaluates the destination URL, recognizes it as malicious, and blocks the connection. The employee sees a warning instead of a counterfeit login form. That single interception can prevent a six-figure loss.

---

3. Filter Web Traffic Across All Devices

Think of web filtering as an automated guardrail for internet navigation. It blocks connections to sites known to be malicious or suspicious.

Many attacks begin with a link in an email. The web filter serves as a backstop when a busy employee clicks before thinking. If the destination is a known malware distribution point, the filter severs the connection. If it's a fake credential-harvesting portal, the filter stops the page from loading.

With remote work, this protection must reside on the endpoint itself, not just on the office network. It needs to travel wherever the employee works. Given that research shows the average time between a phishing message arriving and the recipient clicking the link is under half a minute, there simply isn't enough time for human judgment to intervene. An automated system doing the catching is not optional — it's essential.

4. Default All Sharing Settings to Private

Collaboration platforms like Teams, SharePoint, and Google Drive are engineered for frictionless sharing. Sometimes that friction-free design works against you. The most dangerous feature is the “share with anyone“ link — a URL that grants access to a file or folder without requiring any authentication.

Accidental exposure through these links is far more common than most business owners realize. An employee tries to share a folder with a single external party but selects the wrong option. That folder — potentially loaded with contracts, financial projections, or customer records — is now reachable by anyone who has or obtains the link. A 2025 study found that ninety-nine percent of surveyed organizations had data exposed in their cloud environments, frequently due to precisely this kind of misconfiguration.

The remedy is straightforward: configure a company-wide policy so that any new file, folder, or site starts with the most restrictive permissions available. Sharing externally should require a deliberate, multi-step action — not be the default. The secure path should also be the path of least resistance.

The Human Cost of a BEC Attack

Business Email Compromise deserves particular attention because the fallout extends well beyond the financial statement.

When one of these scams succeeds — when an employee processes a fraudulent wire transfer — the money is devastating. But the emotional toll is often worse. The person who authorized the payment followed what appeared to be a completely normal business process. They did what they believed was right. And now they carry the weight of having caused a catastrophe.

I've watched employees break down. I've seen people offer to quit. I've seen the guilt follow them home and strain relationships. This isn't a cybersecurity

statistic. It's a human reality that plays out in offices along the Wasatch Front regularly.

As a business owner, it's essential to understand that this is not the employee's failure. These attacks are engineered to exploit standard business processes and human trust. Assigning blame creates a culture of fear that makes people reluctant to flag suspicious activity in the future — which makes the next attack even more likely to succeed.

The right response is to fix the process. Implement the phone verification policy. Make it a permanent part of how your company handles financial transactions. In doing so, you remove an impossible burden from your team's shoulders and replace it with a reliable, repeatable safeguard.

Common Errors

Assuming default email security is sufficient. Attackers study what the standard filters look for and design their campaigns to evade them. A supplementary layer catches what the defaults miss.

Relying on email for anything financial. The protocol was never designed with security in mind. Sender names and sometimes addresses can be convincingly forged. Any communication involving the movement of funds should be treated as potentially fraudulent until independently verified.

Expecting training to solve phishing by itself. Awareness training is valuable and necessary. It cannot be your sole defense. People are distractible, fatigued, and operating under time pressure. Technical controls exist to catch the inevitable moment when a person slips.

Questions for Your IT Provider

“What are we running for email security beyond the built-in filters?“ They should be able to explain, in plain terms, how the tool handles a malicious link a user clicks. If they can't, it's not doing its primary job.

“Can you enable an 'EXTERNAL' banner on all inbound messages from outside our organization?“ Simple, free, and effective. It keeps a persistent visual reminder to exercise additional scrutiny — especially valuable for

catching impersonation attempts.

“Confirm that our default sharing permissions in Teams or Google Drive are set to 'private.' Show me the admin policy.“ The answer should be yes, supported by a screenshot of the enforced configuration. A suggestion is not a policy.

THE OWNER IN THE MIRROR

When was the last time you personally called to verify a payment instruction before approving it? If the answer is “never“ or “I can't recall,“ you're depending on luck rather than a process.

CHAPTER 8

Data Protection — Your Digital Safety Net

Meet Karen. She runs an insurance agency in Sandy — eight employees, a solid book of business, and client relationships going back twenty years. Karen's agency used a cloud-based management system for everything — client records, policy documents, claims history. Her IT provider ran nightly backups of the on-premise server, which held some legacy data. But nobody was backing up the cloud system. Nobody even thought about it. "It's in the cloud," Karen told me. "Isn't that the same as being backed up?" It's not. When a disgruntled former employee — whose access had never been revoked — logged in remotely and deleted over three years of client notes, correspondence, and policy documentation, the cloud provider's recycle bin only held thirty days of history. Most of the deleted data was gone for good. Karen spent the next four months reconstructing client files from paper records, emails, and memory. She estimates she lost about forty percent of her historical client data permanently. Her business survived, but the trust damage with long-term clients was significant. The irony is that a Microsoft 365 backup — the kind we deploy as a standard part of every client engagement — would have had that data back within hours.

The loss of your business data — whether through an attack, an accident, or a hardware failure — can end your company. I've personally witnessed it. I've been the one scrambling to recover what's recoverable. And the consistent lesson is clear: the organizations that weather a data crisis are the ones that prepared before the crisis arrived.

This chapter addresses two dimensions of data protection: ensuring only authorized individuals can view sensitive information, and ensuring that information remains available to you when you need it. Both are equally critical.

Four Practices That Build a Genuine Safety Net

1. Implement the 3-2-1 Backup Architecture

This strategy has persisted for years because the logic is airtight.

Maintain at least **three** copies of your important data — your production copy plus two additional backups. Distribute those copies across **two** distinct storage technologies — such as a local device and a cloud platform, or your primary server and a separate backup appliance. Keep **one** of those copies physically or logically isolated from your main network.

The reasoning: no single event should be able to destroy everything simultaneously. A building fire wipes out local equipment? The cloud backup remains intact. Ransomware encrypts your server and everything connected to it? The isolated copy is untouched.

That isolated copy is the linchpin in today's threat environment. Modern ransomware operators have adapted to the reality that businesses maintain backups. So they target the backups first — encrypting or deleting them before detonating the ransomware on production systems. A 2024 report found that attackers attempted to destroy backup data in ninety-four percent of ransomware events. When those attempts succeeded, only about one in five organizations managed to recover within a week.

Two approaches to isolation dominate. An “air-gapped“ backup lives on media that's physically disconnected from the network — you plug it in, run the backup, and unplug it. An “immutable“ backup, a feature offered by many cloud backup providers, locks the data against modification or deletion for a defined retention period. Both prevent an attacker who's already inside your network from reaching your last line of defense.

2. Verify Your Recovery Process Through Regular Testing

A backup that's never been tested is a hope, not a plan. The confirmation message your backup software produces doesn't prove you can restore your business. It confirms that bits were copied. Whether those bits constitute a complete, functional, uncorrupted recovery is a separate question — and you won't know the answer until you try.

Recovery testing means periodically selecting critical systems or data sets and actually restoring them. You don't need to rebuild your entire environment every time. But you do need to regularly confirm that key elements — your primary file store, your critical database, your email archive — come back cleanly and completely.

The purpose is to surface problems under controlled conditions. You'd rather discover that a crucial folder was excluded from the backup job, or that a database export is silently corrupt, during a scheduled drill than during an actual crisis at three in the morning.

A recent industry report found that a quarter of organizations test their recovery plans once a year or less. If your last test was more than ninety days ago — or if you've never done one — you have an unanswered question at the center of your entire security posture.

FROM THE FIELD

Data isn't just living on the server anymore. It's everywhere — in Microsoft 365, in SharePoint, in Teams, in OneDrive, in a dozen SaaS platforms your team uses every day. Those complexities mean we have to level up and map the critical data to understand what the business actually needs, not just sell whatever backup product has traditionally been offered. At Brivy, every client gets Microsoft 365 backups as a standard part of what we do. It's not an upsell. It's part of the baseline. And we've had numerous restore moments where the recovery was deeply impactful — emails, files, SharePoint data brought back when people thought it was gone for good. That's what it means to protect the whole ecosystem, not just the server in the closet. Karen's story didn't have to end the way it did. With the right backup in place, that data would have been back within hours, not lost for good.

The Critical Difference Between Sync and Backup

I encounter this confusion frequently enough that it deserves its own section.

Many business owners believe their data is backed up because it lives in Dropbox, OneDrive, or Google Drive. It isn't. Those platforms are synchronization services, not backup systems. The distinction is fundamental.

A sync service mirrors your files in real time across devices. That's excellent for accessibility and collaboration. But it means that deletions, corruptions, and encryptions also synchronize. If ransomware encrypts your local files, those encrypted versions overwrite the clean copies in the cloud. If an employee — or a disgruntled former employee with lingering access — deletes records, those deletions replicate everywhere. Some services offer a limited version history or trash recovery window, but these features are typically constrained to thirty or ninety days and were never designed to withstand a deliberate attack.

A genuine backup is architecturally different. It creates independent, timestamped copies of your data that exist separately from your production environment. These copies are protected against modification. They allow you to restore to a specific moment in time — last night, last Tuesday, three months ago.

Karen's cloud management platform synced beautifully. When data was deliberately destroyed, the sync service faithfully destroyed it everywhere. A proper backup would have resolved the situation in hours instead of months.

The bottom line: sync is a productivity feature. Backup is a survival mechanism. You need both, and you need to understand which is which.

> **FROM THE FIELD**
>
> I've had clients tell me with complete confidence that their data is backed up because “everything is in OneDrive.“ When I ask them what would happen if ransomware encrypted their local files and those encrypted versions synced to OneDrive, the room goes quiet. That's the moment the light goes on. Every SaaS platform your business relies on — Microsoft 365, your CRM, your accounting software, your project management tools — needs its own backup strategy. The data in those systems is your data. The cloud provider won't restore it for you if something goes wrong on your end.

---

3. Map the Location of Your Most Valuable Information

Protecting your most important data requires first knowing where it actually resides. Just as you track where physical valuables are stored in your office, you need an accurate picture of where your digital crown jewels live.

Data migrates over time. A critical proposal gets saved to someone's desktop rather than the shared drive. A key financial model lands in a personal cloud folder. An outdated customer list sits on a spare machine in a closet. Scattered data is vulnerable data — files on personal desktops and unauthorized cloud accounts typically fall outside your backup coverage and your access controls.

Ask yourself today: where do your accounting records actually live? Your primary customer database? Your employee HR files? Your executed contracts and proprietary processes?

Once you've established where this information should reside, you can verify those locations are backed up, access-restricted, and monitored. Research indicates that at a majority of financial services firms, over a thousand sensitive files are accessible to every employee. Fewer than one in ten companies maintain an effective system for classifying and tracking sensitive information.

Categorizing Your Data Simply

“Data classification“ might sound like a corporate exercise, but for a small business it just means sorting information into three tiers.

Sensitive. The material that would cause serious harm if exposed — client Social Security numbers, medical records, financial account details, employee HR files, trade secrets, legal documents. This data lives in controlled locations with encryption, strict access policies, and regular backups. It never travels through unencrypted email, sits on personal devices, or gets shared via public links.

Internal. Important business information that isn't intended for outside audiences but wouldn't trigger a crisis if exposed — project plans, internal memos, standard procedures, meeting notes. Standard protection and backups, but lighter access controls.

Public. Material that's already available or designed to be shared — marketing collateral, published pricing, public-facing documents. No special handling needed.

Most businesses I assess treat all data identically, which typically means everything receives the minimal tier of protection. The problem: when your marketing brochures and your customer Social Security numbers share the same folder with the same permissions, your most valuable data is defended at the level of your least valuable.

4. Encrypt Every Device That Stores Company Data

Activating the built-in encryption on every company laptop is one of the highest-impact, lowest-effort security measures available. Windows includes BitLocker; macOS includes FileVault. Both are free. Both just need to be switched on.

Encryption renders the contents of a hard drive completely unreadable without proper authentication. A lost or stolen laptop with encryption enabled is a hardware replacement. Without encryption, it's a full-scale data breach — every file, every saved password, every customer record is exposed.

Despite the simplicity and effectiveness of this control, surveys indicate that fewer than one in five small businesses have implemented it. Enabling encryption across your fleet immediately places you ahead of the overwhelming majority of your peers.

Errors to Avoid

Leaving your only backup on the same network as your production data. If ransomware can reach both, you have zero copies. Your isolated backup must be genuinely isolated.

Neglecting to include all critical data in backup jobs. This happens when you don't know where important information actually lives. Your file server might be covered, but the critical spreadsheet on your CFO's desktop is not. The essential proposal in a personal OneDrive folder is not.

Conflating sync with backup. Worth repeating because the consequences are severe. Sync services replicate changes — including destructive ones. Backup services preserve independent point-in-time copies that can survive those changes.

Questions for Your IT Provider

"When did we last execute a full recovery test? What did we restore, how long did it take, and where's the documentation?" You're not asking about backup job logs. You're asking about actual restoration. The answer should cite specific systems, specific durations, and specific results.

"Demonstrate how our offsite copy is protected against ransomware." If it's air-gapped, describe the physical process. If it's immutable, show the configuration setting. This confirms you possess a copy that an attacker with full network access cannot destroy.

"Provide a list of every data location currently included in our backup jobs. Let's compare it against our list of critical assets." Match reality to requirements. Every crown jewel location should appear in the backup configuration.

> **THE OWNER IN THE MIRROR**
>
> Do you know where your most critical business data actually resides right now — not where it's supposed to be, but where it genuinely is? If you can't answer with confidence, your backup almost certainly has blind spots.

CHAPTER 9

Networks & Cloud Basics

Meet Tyson. He runs a growing e-commerce company in Lehi — thirty-five employees, a warehouse, and a small office. Tyson's team had a single Wi-Fi network for everything: employee laptops, the warehouse barcode scanners, the smart TV in the break room, the security cameras, visitors' phones, and even the IoT sensors on the shipping line. One afternoon, a vendor rep connected to the Wi-Fi to show a product demo on their laptop. That laptop had malware. Because everything was on one flat network with no segmentation, the malware spread from the vendor's laptop to the warehouse scanners, then to a workstation in accounting, and eventually to the main file server. The entire operation was down for two days — no shipping, no order processing, no invoicing. Total cost: about seventy thousand dollars in lost revenue and emergency IT work. A separate guest network — something that costs almost nothing to set up — would have kept the vendor's infected laptop completely isolated from Tyson's business systems.

Your network is the connective tissue of your entire operation — linking employee devices, servers, cloud platforms, printers, cameras, and everything else. When an attacker penetrates this network, they can traverse it laterally to reach your most valuable assets. Tyson's experience demonstrated this perfectly: a single infected visitor device cascading through every system in the building because nothing stopped it from moving freely.

This chapter is about creating internal boundaries — dividing your network and cloud environment into zones so that a compromise in one area cannot freely propagate to others.

Three Habits That Prevent Most Network Problems

1. Create Separate Network Zones

Visualize your network as a building. You wouldn't allow a delivery person to wander from the reception area into your financial records room. The same principle applies digitally.

Network segmentation means partitioning your infrastructure into isolated zones. At a minimum, three: a primary network for company-managed devices that you control and trust, a guest network that provides internet access only with no path to internal resources, and a dedicated zone for IoT devices — smart TVs, security cameras, badge readers, wireless printers, and employees' personal phones.

The Internet of Things Blind Spot

IoT devices deserve specific attention because they represent a growing vulnerability that most businesses ignore.

These devices — smart thermostats, IP cameras, wireless printers, digital signage, even some coffee machines — share a troubling commonality: they ship with weak default credentials, run outdated firmware that's difficult or impossible to update, and provide minimal security features. Some transmit data to servers in unexpected jurisdictions.

When an IoT device sits on the same network as your business computers, an attacker who compromises that device can potentially pivot to your file server or accounting workstation. This scenario sounds improbable but is well-documented. In one widely reported case, attackers breached a casino's network through a smart aquarium thermometer connected to the main infrastructure.

Along the Wasatch Front, I encounter this routinely. Security camera systems sharing a network segment with the accounting department. Conference room displays on the same Wi-Fi as the executive team's laptops. Wireless printers carrying default administrative credentials untouched since installation.

The solution is simple: confine these devices to their own network zone. They receive the internet connectivity they need to function, but they have no route to your business systems. It's the digital equivalent of giving the smart TV internet access without handing it the keys to your safe.

Without these internal boundaries — a configuration IT professionals call a “flat network“ — any compromised device becomes a launching point for lateral exploration. A 2025 report found that forty-one percent of attacks leveraged this type of unconstrained movement to escalate damage. Segmentation directly eliminates that pathway.

2. Lock Down Remote Access

With team members connecting from home offices in Draper, coffee shops in Sugar House, and co-working spaces across the valley, the pathways they use to reach your systems represent major attack surface.

One rule is non-negotiable: **Remote Desktop Protocol must never be directly exposed to the internet.** RDP is a built-in Windows capability for remote machine control. Placing it on the open internet is the digital equivalent of posting your office key combination on a billboard. Ransomware operators maintain automated tools that scan for exposed RDP continuously. Research indicates that vulnerable remote access services serve as the initial entry point for more than half of ransomware deployments.

All remote connections should be routed through a secured, managed gateway that mandates multi-factor authentication. Even if credentials are stolen, the attacker hits a wall without the second verification factor.

Understanding Cloud Shared Responsibility

When you adopt a cloud service — Microsoft 365, Google Workspace, AWS, any of them — an invisible line divides security obligations between you and the provider. Misunderstanding where that line falls is one of the most expensive mistakes businesses make.

The cloud provider secures the infrastructure. Data center facilities, physical servers, core networking, environmental controls — these are their responsibility, and the major providers execute this exceptionally well.

You secure everything you do within that infrastructure. Your configurations, your permissions, your sharing settings, who holds access, how data moves in and out. The provider hands you the tools. Using them correctly is on you.

Think of it as renting professional office space. The building owner is responsible for the structure, the elevator, the fire suppression system. Inside your suite, you manage your own locks, your filing cabinets, and who gets a key. If you leave a cabinet unlocked and someone walks off with the contents, that's not the building owner's problem.

A 2025 Palo Alto Networks report attributed forty percent of cloud incidents to unmonitored assets and shadow IT, frequently including misconfigured sharing. IBM's 2025 data showed that seventy-two percent of data breaches involved cloud-stored information. In the majority of these cases, the platform itself wasn't breached — the organizations using it made configuration errors.

Remote Work Along the Wasatch Front

Utah's geography creates a distinctive remote work dynamic. An employee in Ogden works for a company headquartered in Lehi. Another connects from Park City. During winter inversions, half your workforce might be logging in from home.

Each of those remote connections extends your security perimeter to include the employee's home network — shared with teenagers streaming video, smart home devices, and potentially a neighbor who guessed the Wi-Fi password. This is why managed, MFA-protected remote access isn't a luxury. It's a baseline requirement.

3. Configure Cloud Sharing to Default to Private

The single most common source of accidental cloud data exposure is the “share with anyone“ link. An employee, working quickly to share a folder with a client, clicks the wrong option. That folder — potentially containing contracts, financial projections, or customer records — becomes accessible to the entire internet without any authentication.

The corrective measure: establish a company-wide administrative policy that sets the most restrictive sharing permissions as the default on every new file, folder, and site. Sharing externally should demand deliberate action with extra steps. The secure option should be the effortless one.

Common Errors

Believing your cloud provider manages all of your security. They protect the building. You're responsible for everything inside your suite. The tools exist; deploying them correctly is your job.

Operating your main Wi-Fi on a single shared password. If every employee knows the same network password and someone departs, revoking their network access requires changing the password and reconfiguring every device in the office. In practice, this never happens — meaning a former employee can potentially access your internal network months later. Modern wireless infrastructure authenticates each person with their own unique credentials. Disabling their account instantly revokes their network access.

Questions for Your IT Provider

“Prove to me that our guest Wi-Fi is fully isolated from our business network.“ You should see firewall rules or configuration screenshots demonstrating complete traffic separation between guest and internal zones.

“Confirm that no services — particularly RDP — are directly exposed to the internet.“ All remote access must route through a managed, MFA-protected gateway.

“What is the enforced default sharing permission for new content in our cloud environment?“ The answer should be “private,“ backed by an administrative policy screenshot confirming company-wide enforcement.

> **THE OWNER IN THE MIRROR**
>
> Is your personal phone connected to the same network as your company's server? If you're not certain, it probably is. That boundary needs to exist today.

CHAPTER 10

Vendor & Third-Party Risk

Meet Stephanie. She runs a medical billing company in Bountiful — fifteen employees processing claims for about forty healthcare practices across northern Utah. One of Stephanie's software vendors — a claims clearinghouse that connected her system to insurance companies — suffered a breach. The attackers used the clearinghouse's legitimate connection to access data flowing through Stephanie's system, exposing protected health information for thousands of patients across multiple practices. Stephanie didn't have a breach in her own systems. Her own security was solid. But because she was connected to a vendor that wasn't as careful, she was now in the middle of a HIPAA nightmare. She had to notify every affected practice. Each practice had to notify their patients. The legal costs, the compliance work, and the damage to her reputation as a trusted billing partner were devastating. Stephanie now requires every vendor with access to her systems to complete a security questionnaire and sign a security addendum before the contract starts. "I should have been doing this from day one," she told me. "I trusted them because they were a big company. Big companies get breached too."

Your business relies on a web of external partners — IT providers, payroll services, CRM platforms, accounting firms, marketing tools. Each of these relationships constitutes a connection into your environment. Even if your own defenses are strong, a weakness at any partner can become your problem.

The Trust Factor in Utah Business

I want to spend a moment on something distinctive about operating in this state, because it directly influences how vendor risk manifests here.

Utah's business culture is built on personal connection. Deals happen over handshakes. Your CPA is your neighbor. Your IT provider is someone you've

known for years through the chamber. Your insurance agent has been a family friend for a decade.

This is one of the genuinely wonderful aspects of doing business in the Beehive State. Trust accelerates commerce, deepens relationships, and makes work more human.

But in the context of cybersecurity, that trust can create blind spots. When you've known your payroll provider for fifteen years and your kids play on the same soccer team, asking probing questions about their security practices can feel uncomfortable — as though you're questioning their competence or integrity.

You're not. You're protecting your business and theirs.

The criminals who launched the MOVEit exploitation campaign in 2023 didn't factor in anyone's reputation or character. They found a technical weakness and exploited it across thousands of organizations, including many household names. Large, well-known companies suffer breaches regularly. In 2025, incidents at organizations like PowerSchool and Oracle Health affected millions.

Verifying your vendors' security isn't adversarial. It's professional — the same way you'd confirm a building contractor's license and insurance before they start work on your property. A simple: “We're tightening up our security program and asking all key partners a few standard questions — here's a short questionnaire.“ Most vendors will respect the diligence. Those who bristle at the request should raise a flag.

I've included a Vendor Risk Assessment Questionnaire in Appendix E for exactly this purpose.

Supply chain compromises have doubled in frequency since early 2025. Roughly a third of all breaches now involve third-party vectors. Vendor access accounts for over forty percent of ransomware incidents.

Four Habits for Managing Vendor Risk

1. Categorize Your Vendors by Exposure Level

Catalog every external entity that connects to your systems or handles your data — software services, IT providers, accounting platforms, payroll processors,

marketing tools. Then stratify them.

For each vendor, evaluate two dimensions: how critical are they to daily operations (if they went down tomorrow, would it be a minor annoyance or a crisis?), and how sensitive is the data they access (public contact information, or employee Social Security numbers?).

Your high-risk tier — vendors that are operationally critical and handle sensitive information — will be a short list. Typically it includes your IT provider, your payroll company, and your primary line-of-business software. These are the partners that warrant focused diligence.

2. Vet Security Practices Before Signing Agreements

For any new high-risk vendor, maintain a standardized set of questions you pose prior to contract execution. You're validating that their security discipline matches your own.

Core questions: Do they enforce multi-factor authentication for personnel who access your data? Do they maintain a structured approach to software updates? How is your data protected at rest? If they experience an incident, what's their notification timeline?

Research shows that fifty-nine percent of organizations have experienced a breach originating from a third-party provider. Fifteen percent of all 2024 breaches directly involved a vendor relationship — up sixty-eight percent from the prior year.

3. Enforce Scoped, Time-Limited Access

When granting external parties access to your environment, precision matters.

Eliminate shared credentials entirely. Creating a single “Vendor_Admin“ account and distributing the password to an entire support team destroys accountability. If a problem occurs, you know the vendor was involved but have no way to determine which individual took the action. Every external person who needs access receives their own unique, named account.

Scope each account to the minimum necessary. A web development contractor receives access to the web server. Period. Not the file server, not the accounting platform, not the email system.

Assign an expiration date to every vendor account. If a project spans three months, the account auto-disables at the end of that window. Forgotten, lingering vendor accounts — active but unmonitored for months or years — represent one of the most pervasive security gaps I encounter. A 2025 study found that eighty-eight percent of organizations harbor these dormant “ghost“ credentials.

Shadow IT and Ungoverned Applications

When an employee finds a useful tool, signs up with the company credit card, and starts loading data into it — all without informing IT — that's shadow IT. The employee solved their problem. The company now has sensitive data sitting in an unvetted, unmanaged, unmonitored service that nobody knows about.

In fast-moving Utah companies, especially along the Silicon Slopes corridor where teams value autonomy and speed, shadow IT grows quickly. The solution isn't a ban on new tools — that kills innovation. It's a lightweight review process: a quick request, a five-minute security check by your IT provider, and an approval before company data enters the platform. Make the approved path fast and easy so people don't feel compelled to circumvent it.

4. Codify Security Expectations in Contracts

Verbal commitments about security are useful. Written, enforceable obligations are better.

For high-risk vendors, attach a concise security addendum to the contract. It doesn't need to span dozens of pages. It should require the vendor to maintain reasonable security practices — MFA, patching, encryption — and most critically, it should mandate breach notification within a defined window, typically twenty-four to forty-eight hours.

That notification clause is the most valuable provision in the entire addendum. Research demonstrates that breaches discovered and contained within two hundred days cost, on average, 1.39 million dollars less than those that linger longer. Incidents involving stolen credentials take an average of nearly three hundred days to identify and contain. If those credentials belong to your vendor, you may not learn of the problem for months — unless the contract requires rapid disclosure.

Common Oversights

Equating brand recognition with security maturity. Stephanie's clearinghouse vendor was a major, established company. They were still breached. Connecting your business to any vendor, regardless of their size or reputation, means inheriting their risk exposure.

Adopting new tools without governance. Every ungoverned SaaS signup creates a data silo outside your protection framework. You can't secure information you don't know exists.

Questions for Your IT Provider

“Produce a complete list of all non-employee accounts with access to our systems. For each one, who internally owns it, and when is it scheduled to expire?“ Every account should have a named internal sponsor and a hard deactivation date.

“Describe our process for evaluating a new software tool before any department starts using it.“ There should be a defined, lightweight workflow — not bureaucracy, but a checkpoint before data enters an unvetted platform.

“If our most critical vendor suffered a breach right now, walk me through exactly how we'd sever their access within the hour.“ This tests preparedness. The response should reference a documented procedure, not an improvised plan.

> **THE OWNER IN THE MIRROR**
>
> Think about the vendor you trust most — the one you'd vouch for without a moment's hesitation. When did you last confirm they actually enforce multi-factor authentication, maintain current systems, and are contractually obligated to notify you if something goes wrong? Trust deserves to be verified.

PART III — When It Matters Most

CHAPTER 11

Incident Response & Business Continuity

It's 6:47 AM on a Tuesday. Mark owns a manufacturing company in West Valley City — forty employees, a production floor, and a front office that runs on a combination of ERP software, QuickBooks, and a decade-old file server. His production manager calls: "Something's wrong with the computers on the floor. The screens are showing some kind of message about bitcoin." Mark drives in. Every computer in the building — office and production floor — shows the same message. A ransom note. Every file is encrypted. The ERP system is down. QuickBooks is locked. The shared drive with twenty years of engineering drawings, customer purchase orders, and production schedules — gone. Mark's first instinct is to start unplugging things and calling people. But he doesn't have a list of who to call. He doesn't know if his backups are good — he assumed his IT guy handled that. He doesn't know if he should call the police, his insurance company, or a lawyer first. His production team is standing on the floor with nothing to do. His biggest customer has a shipment due Thursday. For the first ninety minutes, Mark does what most business owners do in this situation: he panics. The next eleven days are the worst of his professional life. This chapter exists so that if this happens to you, the first ninety minutes go differently.

I need to be straightforward: a cyber incident has the capacity to devastate your business. Revenue evaporates, reputation takes damage, and legal exposure appears from directions you didn't anticipate.

But the variable that separates organizations that make it through from those that don't isn't their technology budget or the sophistication of their tools. It's whether they had a plan and had practiced it.

I know this from direct experience. I've been the person who gets that call. I've watched the fear set in. I've sat in a Walgreens parking lot in Midvale buying cryptocurrency because nothing else was going to work. And the consistent thread across every one of those situations was not the complexity of the attack — it was whether the people involved had any idea what to do next.

Two Distinct Plans for Two Distinct Problems

Incident Response deals with the technical emergency — halting the attack's progression, determining how access was gained, and remediating the damage. It's the firefighting component.

Business Continuity addresses your operations — how you continue accepting orders, delivering to customers, and meeting payroll while the technical work is underway. Mark's production team standing idle while servers were being rebuilt — that's a continuity failure.

Both are essential. I've included a fillable Incident Response Contact Sheet in Appendix A. Print it, complete it, and store copies in places you can reach even when your office and network are inaccessible.

Before Anything Happens: Preparation

Build Your Contact List

The opening page of your plan should contain names and personal cell phone numbers. Not office extensions — in a genuine crisis, your phone system may be among the casualties.

Three roles need coverage (one person can fill multiple roles):

The Decision-Maker — handles the high-level business calls: whether to take systems offline, when to communicate externally, when to involve legal counsel. This is usually you.

The Technical Lead — initiates the investigation and coordinates the technical response. Your internal IT person or your primary point of contact at your IT provider.

The Operations Lead — keeps the business functional during the crisis, manages staff communication, and activates manual workarounds.

External contacts belong on this sheet too: your cyber insurance carrier (this should be your very first outbound call — most policies include a 24/7 hotline staffed with forensic investigators, attorneys, and crisis managers), law enforcement (the FBI's Salt Lake City field office handles cybercrime for Utah), and your company attorney.

Identify What Must Keep Running

Work through this exercise with your team before you need it. If your primary server is offline, how do you keep fulfilling orders? If the accounting platform is locked, how do invoices go out? If the CRM is unreachable, how does the sales team track active deals?

For each critical function, develop a simple fallback approach. Paper-based order forms. An invoice template stored locally. A phone tree for key clients. These interim solutions keep revenue flowing while systems are being restored. The exercise also reveals your restoration priorities — which systems come back first.

Institute the “Stop and Report“ Protocol

Teach every person in your organization one rule: if something looks wrong on your computer, stop immediately and contact the Technical Lead. Don't investigate. Don't try to fix it. Don't finish the task you're working on. Just stop and make the call.

Urgency matters enormously. A Palo Alto Networks report found that in close to one in five incidents, attackers were extracting data within the first sixty minutes of gaining access. An employee who flags something unusual right away might be the only thing standing between a contained problem on one machine and a full-scale organizational breach.

Build a Process, Not a Hero

It's natural to think “we'll just call the IT person — they'll know what to do.“ But what if they're asleep? Traveling? On vacation?

Your plan must be a straightforward, step-by-step guide that any competent manager could pick up and execute under stress, at 2 AM, with no technical background. Don't architect your response around one individual's expertise. Architect it around a process that anyone can follow.

During the Incident: Action

The Reality of the First Sixty Minutes

Let me describe what an actual incident feels like, because the textbook descriptions don't capture it.

First comes disbelief. “This isn't really happening.“ Then confusion — fragmentary information from multiple directions. Someone says the server is down. Someone else reports strange messages. A third person mentions a pop-up they've never seen. For the opening minutes, you're trying to distinguish between a genuine attack and a random technical glitch.

Then the adrenaline arrives. Once the reality registers, the impulse is to act — anything, right now. That urgency is simultaneously your greatest asset and your greatest liability. Speed is critical. Undisciplined speed makes things worse.

I've watched owners start deleting files they suspected were compromised — destroying forensic evidence. I've seen someone power down a server, erasing the volatile memory that investigators needed. I've seen a well-intentioned person log into the attacker's payment portal “just to see what they're asking for,“ inadvertently starting a countdown timer on data destruction.

This is precisely why preparation matters more than anything else in this chapter. Under stress, you don't elevate to the level of the challenge. You descend to the level of your preparation. If a printed checklist is in your hand, you'll follow it. If nothing exists, you'll improvise — and improvisation under duress rarely produces good outcomes.

> **FROM THE FIELD**
>
> One thing I tell every client: your incident response plan should be simple enough that someone who's frightened, exhausted, and non-technical can follow it at 2 AM. If the plan requires someone to “log into the SIEM dashboard and correlate event data,“ that's not a plan for a small business. Your plan should be: “Call this person. Unplug that cable. Touch nothing else.“ That's the plan that gets followed when it matters.

Contain the Damage

Sever network connections on affected machines without powering them off. Disconnect the ethernet cable. Disable the wireless adapter. But keep the device running — critical forensic evidence lives in active memory and evaporates the moment power is cut.

Reset credentials for any accounts used on affected systems. Treat every password that was entered or stored on compromised hardware as burned. Network login, email, any other significant accounts — change them immediately.

Suspend automated processes that could amplify the damage. If file synchronization services are replicating encrypted ransomware files to your cloud storage, overwriting clean copies, pause them immediately.

Treat the environment as a crime scene. Resist the instinct to clean up. Don't shut down machines unless your technical team specifically instructs it. Maintain a running log of every action taken — who, what, when. This documentation will prove invaluable for the investigation, insurance proceedings, and any legal matters that follow.

Sustain Business Operations

While the technical team works the crisis, your business continuity plan activates. This is where your pre-identified manual workarounds matter. Transition to paper processes where needed. Redirect customer communications.

The goal isn't operational perfection — it's survival until systems are restored.

Own the Narrative

Silence during a crisis breeds rumors, assumptions, and panic. If you don't provide information, people will fill the vacuum with their own — usually worst-case — theories.

Become the single authoritative source. You don't need every answer in the first hour. Communicate three things to your staff and key clients: what you currently know, what you're actively doing about it, and when the next update will come.

Choose a communication channel that doesn't rely on your company's infrastructure — a personal text group, a personal email distribution list — because your corporate systems may be compromised or offline.

Communicating After a Breach

If customer data was involved, the conversation you'll dread most is the one you need to have soonest.

The organizations that weather reputational damage are the ones that communicate early, honestly, and clearly. Those that delay, minimize, or go silent lose trust permanently.

Be the first to inform affected parties. Communicate what's known and what isn't. Describe what you're doing to protect them. Provide clear, specific guidance on any actions they should take. Your attorney and insurance carrier will help navigate the legal requirements.

After the Crisis: Review

Once systems are restored and operations have normalized, do not skip this step.

Convene your response team for a brief, blame-free retrospective. Two questions drive the discussion:

What was the actual root cause? Look beyond the surface. Dig past “someone clicked a link“ to the underlying gap — was MFA missing on the compromised account? Was a server running months behind on patches? Was a former vendor's access still active?

What one or two changes would have prevented this? Don't try to reform everything simultaneously. Identify the highest-impact adjustments, assign them to specific people with deadlines, and follow through.

Practice Before You Need It

A plan that exists only on paper (or only in someone's head) is untested theory.

The most effective validation is a tabletop exercise — a structured discussion where your response team walks through a realistic scenario. It takes one hour and costs nothing.

A Tabletop Exercise You Can Run This Week

Setup (5 minutes): Assemble your incident response team. Distribute copies of your contact sheet from Appendix A.

The Scenario (read aloud): "It's 8:15 AM on a Wednesday. Your office manager notices a message on her screen demanding bitcoin payment. Two other computers show the same message. Files on the shared drive won't open — their extensions have been changed. Accounting software won't launch. Email works on phones but not on any office computer. It appears to be ransomware."

Walk through these questions, one at a time:

What's the very first action? Who makes the first phone call? Do we have the right numbers? Can we reach our insurance carrier right now? How do we isolate affected machines? Do we know which systems are compromised and which are clean? Our largest customer expects a delivery Friday. How do we fulfill that commitment without our systems? Employees are arriving and can't work. What do we tell them? Who communicates? Through what channel? After two hours, the forensic investigator asks about backups. When was our last tested restore? Is our backup connected to the same network? By day three, a client calls asking if their data was exposed. What do we say? Who handles that conversation?

Wrap-up (10 minutes): Each participant identifies what surprised them, what gap they discovered, and what needs to be fixed before this scenario feels manageable.

Document every gap. Assign each to a person with a deadline. Schedule the next exercise for six months out.

IBM's 2025 research found that organizations that regularly rehearse their response plans save an average of 1.49 million dollars per breach compared to those that don't. Organizations without a formal, tested plan paid fifty-eight percent more per incident. Yet only three in ten companies conduct this kind of exercise regularly. A single one-hour session places you ahead of the vast majority.

> **THE OWNER IN THE MIRROR**
>
> If something happened tonight, could your team reach you? Would they know what to do for the first thirty minutes on their own? If not, that's the gap to close before anything else.

CHAPTER 12

Compliance & Governance — The Ethics of Doing It Right

I need to tell you a story before we get into the mechanics of this chapter.

Early in my career, I was called in to do a standard IT assessment for a physicians group — a well-known practice in the community, the kind of place you'd assume had everything buttoned up. We ran the assessment, documented the findings, and delivered the report.

Forty pages. And I'm not exaggerating when I say you would have had to try to make it that bad. Clear HIPAA violations, documented and disclosed. Gaping holes in their security. Old, unpatched, insecure systems. The kind of findings that make the word “negligent“ come to mind.

We delivered the report, walked them through the recommendations, presented the proposal, and waited for their response.

“We're not going to do anything.“

I sat there for a second. “Nothing? You don't want to fix any of the things we just showed you?“

“Nope.“

Their reasoning was purely business. They'd never had a HIPAA audit. They'd never had a data breach. They were going to roll the dice. If something happened, they'd plead ignorance and argue down any penalties, then fix what was required.

I went home that night and changed doctors.

It wasn't about losing the business. It was about watching people who were entrusted with their patients' most private health information make a deliberate

choice to do nothing — and then wondering what other corners were being cut to save money.

That story is why I care about compliance. Not because of paperwork or audit checklists. Because compliance, at its core, is about doing right by the people who trust you.

Defining the Terms

These three concepts get conflated constantly. Let me separate them.

Security is the actual protective work — deploying endpoint protection, testing backup recoveries, training your team to recognize threats. It's the equivalent of installing locks and cameras.

Compliance is the documentation and demonstration that you're meeting specific requirements — whether imposed by law, by your industry, or by customers who need assurance. It's presenting your sprinkler maintenance logs to the fire inspector.

Governance is the accountability structure — who owns the security function, how decisions are made, and how outcomes are verified. It ensures the work happens consistently and that someone is answerable when it doesn't.

You need all three operating together. Strong security without documentation makes it difficult to satisfy customers or insurance carriers. Compliance paperwork unsupported by actual security practices is a facade. And without governance, nobody is accountable and nothing persists beyond the initial enthusiasm.

Utah's Compliance Landscape

Several characteristics of our state's economy make compliance particularly relevant here.

Healthcare is everywhere along the Wasatch Front. Intermountain Health, University of Utah Health, and thousands of independent practices, clinics, dental offices, and specialists — every one of them subject to HIPAA. And it extends beyond direct providers to every entity that handles health data: billing companies, IT providers serving healthcare clients, insurance agencies.

Financial services are heavily concentrated in this market. Accounting firms, wealth managers, insurance agencies, mortgage brokers — all handling information subject to federal and state regulatory requirements.

Government contracting is significant in Utah. Hill Air Force Base, the NSA's Utah Data Center, Camp Williams, Dugway Proving Ground — the federal presence means many local businesses, particularly in technology and manufacturing, face requirements like CMMC certification to compete for contracts.

Technology companies in the Silicon Slopes corridor face growing pressure from enterprise customers and investors. SOC 2 assessments, penetration testing, and detailed security questionnaires have become baseline expectations for B2B tech companies seeking to scale.

Regardless of your specific industry, the fundamentals are consistent. The frameworks and habits throughout this book will serve you whether your obligations involve HIPAA, CMMC, or simply the ability to respond confidently to a customer's vendor questionnaire.

A Practical System

Follow Your Framework

The NIST or CIS framework you selected in Chapter 4 serves as your compliance roadmap. It enumerates the essential protections and, by extension, the evidence you'll eventually need to produce. No need to build anything from scratch.

Designate an Owner

For a small business, governance means naming one person who's responsible for ensuring security activities happen on schedule. The role doesn't require full-time dedication. But it demands a named individual. When accountability is shared by “everyone,“ it's owned by no one.

Establish a Monthly Rhythm

A thirty-minute monthly meeting between the security owner and relevant leaders is sufficient. Three standing questions drive the agenda:

“What changed in the business this month?“ — new hires, new software, new client agreements. Any operational change can introduce new exposure.

“Were there any incidents or close calls?“ — a convincing phishing attempt that someone flagged, a security alert that fired. Near-misses are how you detect and address small problems before they compound.

“Which controls are we verifying this month?“ — rotate through your checklist. This month, review the MFA enrollment report. Next month, examine the patching compliance data.

Building Your Evidence Trail

Documentation doesn't have to be painful. It's a habit of capturing proof as work happens.

Policies — brief documents stating what you do. “All employees are required to use multi-factor authentication on their email accounts. All company laptops must have full-disk encryption enabled.“ One page. Plain language.

Procedures — step-by-step guides for how the work gets done. A one-page illustrated walkthrough showing a new employee how to configure their authenticator app. A checklist for the offboarding sequence.

Evidence — dated proof that policies are being followed. A screenshot of the MFA enrollment dashboard. A report from the most recent backup recovery test. Notes from the monthly security review.

When a control check is completed — a recovery drill, an access review, a training session — save the output in a dated folder. “2026-01 Evidence.“ Add a one-line note to your meeting minutes: “Quarterly recovery test completed. Results in evidence folder.“ Two extra minutes of effort. When an auditor asks twelve months later, you'll have a clean, timestamped trail ready to present.

Practical Evidence Examples

MFA compliance screenshot — exported from your Microsoft 365 or Google admin console, showing enrollment status for every user. Takes your IT provider thirty seconds to pull.

Patching status report — a summary of what percentage of your fleet is fully current. Should be generated monthly as a standard deliverable from your IT provider.

Recovery test documentation — a brief summary confirming what was restored, how long it took, and any issues discovered. Even a paragraph in an email qualifies.

Access review notes — quarterly documentation of who holds access to what, what changes were made, and confirmation that no orphaned accounts remain.

Meeting minutes — dated notes from your monthly check-in. The simple act of maintaining these records demonstrates active governance.

None of these items requires more than five minutes to save. Collectively, over the course of a year, they construct a compelling portfolio that demonstrates your program is real, active, and maintained — not just a document gathering dust.

> **FROM THE FIELD**
>
> I've seen two types of businesses face an audit. The first scrambles for weeks trying to reconstruct evidence retroactively — digging through old emails, trying to remember when they last tested a backup, hoping their IT provider kept records they never requested. It's stressful, expensive, and looks unprofessional. The second opens a folder, pulls dated evidence, and hands it over. The audit concludes in a fraction of the time, and the auditor walks away impressed. The difference isn't security posture — it's the habit of preserving evidence as it's generated. Five minutes a month. That's it.

Responding to Audits and Questionnaires

An audit is someone checking your work. Whether it's a cyber insurance renewal, a prospective client's vendor assessment, or a regulatory examination, they're asking you to demonstrate that you take basic, sensible precautions.

If you've maintained the evidence habit, the process becomes straightforward. The questionnaire asks about MFA — you provide the policy document and last month's enrollment screenshot. It asks about backups — you produce the recovery test report. Professional, organized, substantiated.

The same approach applies to vendor security questionnaires from larger customers. Your framework serves as the answer key — the questions invariably map to the same control categories. Create a standard response document based on your policies. The initial questionnaire requires effort; subsequent ones draw heavily from what you've already prepared.

Privacy Obligations

If your business collects personal information — and virtually every business does, even if only employee records — you carry an obligation to protect it. Core principles: transparency about why you collect data, consent where required, retention limited to what's necessary, and secure disposal when the business justification expires.

Regulatory requirements vary by geography and customer base. California residents trigger CCPA obligations. European customers invoke GDPR. Utah enacted its own Utah Consumer Privacy Act (UCPA), effective since late 2023, applicable to businesses meeting specific revenue and data-processing thresholds. A conversation with a knowledgeable attorney is a worthwhile investment — several firms along the Wasatch Front specialize in data privacy for small businesses.

> **THE OWNER IN THE MIRROR**
>
> Are you the doctor in this story — choosing inaction because nothing bad has happened yet? The absence of a disaster isn't evidence that your security is working. It may simply mean you haven't been tested.

CHAPTER 13

A Note to Utah's Business Owners

If you've reached this point, well done. Most business owners never invest the time to genuinely think through cybersecurity. You've made that investment, and you now have a clear picture of what's at stake and what to do about it.

Here are the ideas I most want you to carry forward.

Control the Access

Enforce multi-factor authentication across every account — yours included. Maintain a current inventory of every device used for work. Revoke administrative privileges from daily-use accounts. This is the highest-impact area, and you can begin today.

Know Where Your Data Lives

Designate approved locations for sensitive information. Disable public sharing by default. An accidental cloud misconfiguration is among the most common ways organizations expose vast quantities of data.

Have a Plan for the Bad Day

Validate your backups through actual restoration tests. Conduct tabletop exercises. Keep your incident response plan to a single printed page with contact information at the top. Organizations that rehearse their response save an average of 1.49 million dollars per incident.

Separate Your Networks

Isolate guest traffic from business systems. Place IoT devices in their own zone. These simple boundaries prevent a problem on one device from cascading through your entire operation.

Manage Your Vendor Risk

Stratify vendors by exposure level. Require unique, expiring accounts. Codify security expectations in writing — particularly the requirement for rapid breach notification.

Verify, Don't Assume

Cultivate the evidence habit. Save dated reports and screenshots monthly. This documentation transforms good intentions into demonstrable professionalism.

Security Is a Habit

This is the fundamental mindset I'm asking you to adopt. Security isn't a project. Projects have endpoints. Security is an ongoing discipline — like bookkeeping, inventory management, or locking the office at night. Regular meetings, incremental adjustments, consistent recordkeeping.

When you internalize this, the topic stops being overwhelming. It becomes a sequence of manageable tasks integrated into normal operations. Review the backups. Audit the access list. Confirm software is current. Your IT provider should handle the execution, but the accountability belongs to you.

The true value reveals itself when something eventually goes wrong. Your team responds with practiced steps instead of panic. They know who to call, what to do first, and how to keep the business moving.

Where to Start — Your First 30 Days

If you're feeling the weight of everything that needs attention, pause and breathe. You don't have to tackle it all at once.

Week 1: Print and complete the Incident Response Contact Sheet in Appendix A — fifteen minutes. Verify your MFA enrollment report — confirm every

account is covered, including yours. Complete the Self-Assessment in Appendix F to identify your biggest gaps.

Week 2: Have the backup conversation with your IT provider using the questions from Chapter 8. Review the list of administrative accounts and remove privileges that aren't justified. Confirm your cloud sharing defaults are set to private.

Week 3: Build your onboarding and offboarding checklists from Appendices C and D. Implement the financial verification policy from Chapter 7. Identify and categorize your high-risk vendors.

Week 4: Schedule your first monthly security check-in using Appendix B. Block one hour for a tabletop exercise next quarter. Choose your framework — NIST or CIS — and begin mapping your current controls.

In thirty days, you'll have MFA verified, backups validated, access reviewed, processes documented, a plan printed, and a rhythm established. You're not finished — you'll never be “finished.“ But you've built the foundation that everything else stands on.

A Personal Offer

If you've read this book and you're ready to take the next step — or if you just need a conversation about where to begin — I'd like to offer you a **free, thirty-minute advisory call.** No sales pitch. Just a straightforward discussion about your business and your security.

Email: support@brivyit.com **Call or text:** (385) 200-7323 **Visit:** brivyit.com

Thank you for reading. Thank you for caring enough about your business and your people to invest this time. And thank you for being part of the community we're working to protect every day.

— John Huston Founder, Brivy IT 8415 S. 700 W. Suite 7 Sandy, Utah 84070

CHAPTER 14

Jargon Decoder

Our industry has a tendency to bury simple concepts under layers of jargon. This reference cuts through it. Keep it accessible as you implement the practices from this book and when conversing with IT providers, insurance carriers, and vendors.

30 Terms Every Business Owner Should Know

Authentication. The process of verifying that someone is who they claim to be — typically through a password, a verification code, or a biometric like a fingerprint.

Botnet. A collection of compromised computers controlled remotely by criminals, typically used for mass spam distribution, coordinated attacks on websites, or cryptocurrency mining. The owners of the compromised machines are usually unaware.

Business Email Compromise (BEC). A fraud scheme in which an attacker impersonates a trusted individual — typically via email — to manipulate an employee into transferring funds or divulging sensitive information. Among the costliest attack types targeting small businesses.

Cloud Computing. Using internet-hosted infrastructure — servers, storage, applications — operated by a third party, rather than owning and maintaining your own equipment.

Compliance. The practice of demonstrating adherence to a specific set of security or privacy requirements, whether imposed by law, industry standards, or customer agreements.

Cyber Insurance. An insurance product designed to offset the financial impact of a cyber incident — covering investigation costs, legal fees, notification expenses, and business interruption.

DDoS (Distributed Denial-of-Service) Attack. Overwhelming a website or online service with massive volumes of illegitimate traffic, rendering it unable to serve genuine users.

Encryption. The process of converting data into an unreadable format that can only be decoded with the proper key. Essential for protecting information on portable devices and during transmission.

Endpoint Detection and Response (EDR). A modern security platform that monitors computing devices for suspicious behavioral patterns rather than relying solely on a database of known threats. The evolution beyond traditional antivirus.

Firewall. A boundary enforcement system between your internal network and the public internet, governing what traffic is permitted to enter and exit.

Incident Response. The coordinated plan and set of actions executed when a security breach or attack is detected.

IP Address. A numerical identifier assigned to every device on a network — the digital equivalent of a street address.

Malware. The umbrella term for any software designed with harmful intent — encompassing viruses, spyware, ransomware, keyloggers, and remote access tools.

Managed Service Provider (MSP). An external IT firm retained to manage technology infrastructure and security on a continuous, ongoing basis — functioning as an outsourced IT department.

Multi-Factor Authentication (MFA). A login process requiring verification through more than one method — typically a password combined with a code from a mobile device. The single most effective defense against account compromise.

Network Segmentation. The practice of partitioning a network into isolated zones to prevent a compromise in one area from spreading to others.

Patch Management. The discipline of systematically applying software updates to remediate known security vulnerabilities before they can be exploited.

Penetration Testing. Engaging ethical security professionals to attempt to breach your systems under controlled conditions, identifying weaknesses before actual adversaries discover them.

Phishing. A deceptive communication — most commonly email — crafted to trick the recipient into clicking a harmful link, opening a weaponized attachment, or surrendering login credentials.

Ransomware. Malicious software that encrypts your files and demands payment in exchange for the decryption key. Frequently combined with data theft for additional leverage.

Remote Desktop Protocol (RDP). A Windows feature enabling remote control of a computer over a network connection. Critically dangerous when exposed directly to the internet without proper safeguards.

Risk. The potential for harm resulting from the intersection of a threat and a vulnerability. Security fundamentally revolves around managing risk — reducing both probability and impact.

Server. A computer dedicated to providing services, data, or resources to other devices on a network.

Social Engineering. The practice of manipulating human psychology — rather than exploiting technology — to induce people to reveal information or take actions they shouldn't.

Threat Actor. Any individual or group possessing both the intent and the capability to conduct a cyberattack — ranging from individual fraudsters to organized criminal syndicates to nation-state operations.

Two-Factor Authentication (2FA). A specific implementation of MFA using exactly two verification methods — commonly a password plus a mobile authenticator code.

VPN (Virtual Private Network). A technology that creates an encrypted communication tunnel over the public internet, commonly used to secure remote workers' connections to company resources.

Vulnerability. A weakness in software, hardware, or process that an attacker could potentially exploit. Tens of thousands of new vulnerabilities are identified annually.

Zero-Day Exploit. An attack targeting a security flaw that has been discovered but for which no patch yet exists — representing the most dangerous category of vulnerability because no defense has been published.

Zero Trust. A contemporary security philosophy built on the principle that no user or device should be automatically trusted, regardless of location. Continuous verification is required for every access attempt.

Utah Cybersecurity Resources

FBI Salt Lake City Field Office 257 East 200 South, Suite 1200, Salt Lake City, UT 84111

Utah Attorney General — Cybercrime Division attorneygeneral.utah.gov

CISA — Region 8 (includes Utah)

Utah Small Business Development Center (SBDC)

SCORE Utah

InfraGard — Salt Lake City Chapter

Silicon Slopes

Utah Consumer Privacy Act (UCPA) Utah's state privacy law, effective December 2023. Applies to businesses meeting certain revenue and data-processing thresholds. Consult an attorney for applicability.

Appendix A: Incident Response Contact Sheet

Print this page. Fill it out. Keep copies in your desk, your car, and your home. When your network is down, this paper may be the most important document you own.

Company Name: _____

Date Last Updated: _____

INTERNAL RESPONSE TEAM

Role	Name	Cell Phone	Email
Decision-Maker			
Technical Lead			
Operations Lead			
Backup Decision-Maker			

EXTERNAL CONTACTS

Contact	Company/Organization	Phone	Policy/Account #
Cyber Insurance Carrier			
IT Provider / MSP			

Contact	Company/Organization	Phone	Policy/Account #
Company Attorney			
FBI (Salt Lake City)	FBI SLC Field Office	(801) 579-1400	
Local Law Enforcement			
Bank (Fraud Department)			

FIRST 30 MINUTES CHECKLIST

- □ Activate “Stop and Report“ — instruct all staff to cease using affected systems
- □ Call cyber insurance carrier FIRST — their hotline will guide the response
- □ Isolate affected machines (disconnect network, disable Wi-Fi, keep powered ON)
- □ Reset passwords for any accounts used on affected machines
- □ Suspend automated file sync services (OneDrive, Dropbox, Google Drive)
- □ Begin a written log: who did what, at what time
- □ Do NOT power off affected machines — forensic evidence resides in active memory
- □ Do NOT attempt to clean, delete, or modify files on affected systems
- □ Contact IT provider / Technical Lead
- □ Activate business continuity workarounds

CRITICAL SYSTEMS — RESTORATION PRIORITY

Priority	System	Fallback Procedure
1		
2		
3		

Priority	System	Fallback Procedure
4		
5		

COMMUNICATION PLAN

Audience	Channel (independent of company systems)	Responsible Person	Template Location
All Staff			
Key Clients			
Vendors/Partners			

Appendix B: Monthly Security Check-In Agenda

Use this template for your thirty-minute monthly meeting. It forms the backbone of your governance routine.

Meeting Date: _____ **Attendees:** _____

1. Business Changes This Month (5 minutes)

• New hires? ___ Names: _____

• Departures? ___ Names: _____

• New software or tools adopted? _____

• New vendors with system access? _____

• New client contracts with security requirements? _____

• Other significant changes? _____

2. Incidents and Near-Misses (10 minutes)

• Reported phishing attempts or suspicious activity? _____

• Security tool alerts (EDR, email filter, etc.)? _____

• Unusual password resets or account lockouts? _____

• Lost or stolen devices? _____

• Lessons from any of the above? _____

3. Control Verification (10 minutes)

Select 2-3 items from your control register. Rotate through all controls quarterly.

Control Being Verified	Status	Evidence Preserved?	File Location
		[ ] Yes	
		[ ] Yes	
		[ ] Yes	

Suggested quarterly rotation:

• Month 1: MFA enrollment report, device encryption status

• Month 2: Backup recovery test results, patching compliance

• Month 3: User access review, administrative privilege audit

• Month 4: Vendor account review, offboarding log verification

• Repeat

4. Action Items (5 minutes)

Next meeting: _____

Appendix C: Employee Onboarding Security Checklist

Complete for every new hire before their first day of work.

Employee Name: _____ Start Date: _____

Role: _____ Manager: _____

ACCOUNT PROVISIONING

- ☐ Create unique user account (shared accounts are never acceptable)
- ☐ Configure initial password (require change at first login)
- ☐ Enable Multi-Factor Authentication on all accounts
- ☐ Assign role-appropriate access ONLY — minimum necessary permissions
- ☐ Add to appropriate security groups and distribution lists
- ☐ Provision password manager account

DEVICE CONFIGURATION

- ☐ Issue company-managed device (laptop/desktop)
- ☐ Confirm full-disk encryption is active (BitLocker / FileVault)
- ☐ Confirm endpoint protection (EDR) is installed and reporting
- ☐ Confirm device is enrolled in management/inventory platform
- ☐ Revoke local administrative privileges for daily use
- ☐ Confirm automatic updates are enabled

ACCESS ASSIGNMENTS

System/Application	Access Level	Approved By
Email (Microsoft 365 / Google)		

System/Application	Access Level	Approved By
File shares / SharePoint		
Line-of-business applications		
VPN / Remote access		
Other:		

TRAINING

- ☐ Security awareness training assigned (complete within first week)
- ☐ Acceptable use policy reviewed (signed copy filed)
- ☐ Shown how to report suspicious emails/activity
- ☐ Briefed on “Stop and Report“ protocol
- ☐ Trained on password policy and password manager usage

PERSONAL DEVICES (if BYOD applies)

- ☐ Personal device registered and meets minimum security standards
- ☐ Passcode/biometric lock confirmed
- ☐ Encryption confirmed
- ☐ Remote wipe capability confirmed

Completed by: _____ Date: _____

Appendix D: Employee Offboarding Security Checklist

Initiate immediately upon confirmed departure. Target: complete within hours, not days.

Employee Name: _____ Last Day: _____

Role: _____ Manager: _____

Departure type: [ ] Resignation [ ] Termination [ ] Contract end [ ] Other

IMMEDIATE ACTIONS (within 1 hour of confirmation)

- □ Disable email account (preserve for records — do NOT delete)
- □ Disable network / directory account
- □ Reset credentials on any shared accounts this person accessed
- □ Revoke VPN / remote access
- □ Deactivate MFA tokens linked to this user
- □ Remove from all security groups and distribution lists

APPLICATION ACCESS (complete same day)

System/Application	Access Revoked	Confirmed By	Date
Email	[ ]		
File shares / SharePoint	[ ]		
CRM	[ ]		
Accounting software	[ ]		

System/Application	Access Revoked	Confirmed By	Date
HR / Payroll	[ ]		
Password manager	[ ]		
Social media accounts	[ ]		
Other:	[ ]		
Other:	[ ]		

DEVICE RECOVERY

- □ Company laptop returned and accounted for
- □ Company phone returned (if applicable)
- □ External drives, USB devices, and physical keys returned
- □ Company data removed from personal devices (if BYOD)
- □ Remote wipe initiated on any unreturned devices

DATA & RECORDS

- □ Email forwarding configured to manager (if appropriate)
- □ Shared files transferred to designated team member
- □ Software license seats reassigned or canceled
- □ Employee removed from vendor/partner access lists

VERIFICATION

- □ Confirmed: individual cannot authenticate to any company system
- □ Confirmed: no active sessions persist on any platform
- □ Confirmed: all physical access credentials (keys, cards, fobs) returned

Completed by: _____ Date: _____

IT Provider confirmed all access revoked: _____ Date: _____

Appendix E: Vendor Risk Assessment Questionnaire

Apply to any new vendor that will access your systems or handle sensitive data. Prioritize for high-risk vendors — those critical to operations or handling sensitive information.

Vendor Name: _____ Date: _____

Primary Contact: _____ Title: _____

Services Provided: _____

Data Access: What categories of company data will this vendor access or process?

- □ Customer personal information
- □ Employee personal information
- □ Financial / accounting data
- □ Health / medical records (HIPAA-regulated)
- □ Intellectual property / trade secrets
- □ System credentials / administrative access
- □ Other: _____

Risk Classification: [ ] High Risk [ ] Medium Risk [ ] Low Risk

SECURITY QUESTIONS

Question	Yes	No	Notes
Does the vendor require MFA for personnel accessing our data?			
Does the vendor maintain a documented patching process?			
Is our data encrypted both at rest and in transit?			
Does the vendor conduct periodic security assessments?			
Does the vendor carry cyber insurance?			
Does the vendor maintain an incident response plan?			
Will the vendor notify us within 48 hours of a breach?			
Does the vendor issue unique accounts (no shared credentials)?			
Does the vendor hold SOC 2, ISO 27001, or comparable certification?			

Question	Yes	No	Notes
Can the vendor provide references from comparably sized clients?			

CONTRACT REQUIREMENTS

- ☐ Security addendum incorporated into agreement
- ☐ Breach notification clause (24-48 hour requirement)
- ☐ Right to request security documentation annually
- ☐ Data handling and destruction obligations upon contract termination
- ☐ Access scope explicitly defined and limited to necessary systems

ACCESS CONFIGURATION

- ☐ Unique named account created (no shared credentials)
- ☐ Access restricted to necessary systems only
- ☐ Account expiration date: _____
- ☐ Internal account owner: _____
- ☐ MFA required on vendor account

Reviewed by: _____ **Date:** _____

Approved: [ ] Yes [ ] No — Reason: _____

_____

Appendix F: Cybersecurity Self-Assessment for Business Owners

Answer honestly. This isn't a test — it's a diagnostic. Each "No" identifies an area of active risk.

IDENTITY & ACCESS

Question	Yes	No
Does every employee use MFA on email — including you?		
Do you use a business-grade password manager?		
Are employee permissions restricted to role-appropriate minimums?		
Do you have a documented onboarding checklist for new hires?		
Do you have a documented offboarding checklist for departures?		
Can you fully disable a departing employee's access within one hour?		

Question	Yes	No
Is there a designated individual (not “everyone“) responsible for security?		

DEVICES & ENDPOINTS

Question	Yes	No
Do you maintain a current inventory of all devices accessing company data?		
Is full-disk encryption active on every laptop and desktop?		
Are employees restricted from administrative privileges for daily use?		
Are you running EDR (not legacy antivirus)?		
Is someone monitoring security alerts around the clock?		
Are critical security patches applied within one week?		
Do personal devices used for work meet defined minimum standards?		

EMAIL & COMMUNICATION

Question	Yes	No
Do you run email security beyond the built-in platform filters?		
Is there a mandatory phone verification step for financial transactions?		
Do external emails display a warning banner?		
Is web filtering active on all employee devices?		
Are file-sharing defaults set to “private“?		

DATA PROTECTION

Question	Yes	No
Do you maintain at least three copies of critical data?		
Is at least one copy isolated (air-gapped or immutable)?		
Have you tested a backup restoration in the past 90 days?		
Can you identify where your most critical data currently resides?		
Are cloud sync services backed up independently?		

NETWORK & CLOUD

Question	Yes	No
Is guest Wi-Fi isolated from your business network?		
Is Remote Desktop blocked from direct internet exposure?		
Does all remote access require MFA?		
Are cloud sharing defaults enforced as “private“?		

VENDORS & THIRD PARTIES

Question	Yes	No
Have you identified and categorized your high-risk vendors?		
Do high-risk vendor contracts include breach notification clauses?		
Do all vendor accounts use unique credentials with expiration dates?		
Is there a review process for new software before adoption?		

INCIDENT RESPONSE & GOVERNANCE

Question	Yes	No
Do you have a written incident response plan?		

Question	Yes	No
Is it printed and accessible if your network goes down?		
Have you practiced the plan through a tabletop exercise?		
Do you carry current cyber insurance?		
Do you conduct a monthly security check-in meeting?		
Do you preserve dated evidence (screenshots, reports) monthly?		

INTERPRETING YOUR RESULTS

Count your “Yes“ responses:

30-35: Strong foundation. You're operating ahead of most organizations your size. Focus on maintaining these practices and closing any remaining gaps.

20-29: Solid start with meaningful gaps. Core protections are partially in place, but significant vulnerabilities remain. Prioritize the “No“ answers in the Identity and Data Protection sections.

10-19: Elevated risk. Your organization has substantial exposure. Begin with three priorities: MFA for every account, validated backups, and a completed incident response contact sheet.

Under 10: Critical. Your business is operating without fundamental protections. This is the posture most organizations have before something goes wrong. The encouraging reality: every practice in this book is achievable, and you can start today.

About the Author

John Huston is the founder and CEO of Brivy IT, a managed IT services company based in Sandy, Utah. He has spent his entire career in the office technology space, working across nearly every industry and developing a deep commitment to helping business owners solve problems through technology.

John founded Brivy IT on a simple conviction: that technology should work like a fine watch — a unified ecosystem built with precision, care, and craftsmanship. He believes security is not an upsell but a fundamental part of every client relationship, and that the businesses he serves deserve honest conversations about their technology — not just what they want to hear, but what they need to know.

Brivy IT provides managed IT services, cybersecurity, managed print, and physical security to businesses along the Wasatch Front and throughout Utah. The company is built around doing it right when nobody is looking, and bringing the same standard of care to the smallest detail as to the largest project.

When he's not working with clients, John is a musician who writes and releases original music, a creative writer, and an active member of the Utah community.

Connect with John and Brivy IT:

LinkedIn: linkedin.com/company/brivyit YouTube: youtube.com/@brivytech John's personal site: hustoninutah.com

Ready to Protect Your Business?

Schedule a free 30-minute advisory call with John Huston. No sales pitch. Just a conversation about your security.

brivyit.com

(385) 200-7323

support@brivyit.com

Managed IT • Cybersecurity • Managed Print • Physical Security

8415 S. 700 W. Suite 7, Sandy, Utah 84070

linkedin.com/company/brivyit • youtube.com/@brivytech

hustoninutah.com

BRIVY IT

Technology that works like a fine watch.