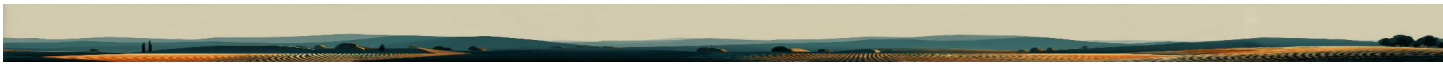
LATTIS

Cybersecurity for the Rest of Us

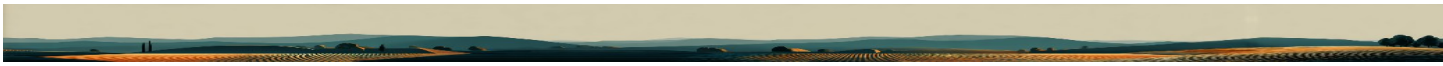
A plain-English guide to protecting your business from the threats that are actually out there

April 2026



LATTIS

Lattis · Atascadero, CA · lattisnetworks.com



LATTIS

Introduction

Most cybersecurity content is written for IT professionals. This guide is written for the business owner who doesn't have an IT team, or has a small one, and needs to understand what's actually at risk and what to do about it without wading through technical jargon.

The threats are real. The businesses getting hit aren't careless — they're busy. They made reasonable decisions with the information they had, and the criminals found the gap. Understanding where those gaps are is the first step to closing them.

In 26 years of managing technology systems for businesses on the Central Coast, I've responded to cyberattacks, sat across from bank vice presidents explaining how $20,000 disappeared, and helped businesses rebuild after ransomware locked up every server they owned. This guide draws on those experiences. The stories are real. The names aren't.

What a Business With No Cybersecurity Posture Looks Like

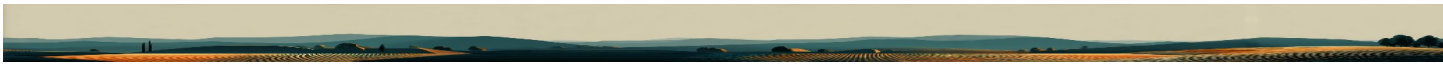
When I walk into a business that has no real security posture, I can usually tell within the first few minutes. Here's what I see.

Email pointed directly at the cloud provider

The company's email is hosted with a cloud provider, and their mail records point straight to that provider with no filtering layer in between. Every phishing email, every malware attachment, every spoofed invoice goes directly to the inbox with nothing stopping it.

No multi-factor authentication

Usernames and passwords are the only thing standing between a criminal and the entire email environment. One compromised password — from a phishing email, a data breach on another site, or a brute force attack — and the account is open.



LATTIS

Shared accounts without MFA

Multiple users sharing a single login because nobody wanted to deal with the MFA setup. Every person who's ever had that password still has it. There's no way to know who logged in or when.

Basic antivirus, unmanaged

There's an antivirus product installed on the computers but nobody's looking at it. It hasn't been updated. It's looking for known threats based on patterns — which means anything new gets through.

No patch management

Operating systems get updated eventually. The software running on those operating systems — the applications, the utilities, the browser plugins — often doesn't. Vulnerabilities in unpatched software are one of the most common attack vectors in existence.

Flat network, no segmentation

Every device on the network can reach every other device. A compromised laptop can talk to the server. A visitor on the Wi-Fi can see internal systems. There's no boundary between what should be accessible and what shouldn't.

Old Wi-Fi password, never changed

The wireless network password was set years ago. Every former employee, every contractor, every vendor who visited knows it. It's never been changed.

No outbound email encryption

Sensitive information — tax documents, payroll data, employee records, client financial information — goes out over email in plain text. Anyone intercepting that traffic can read it.

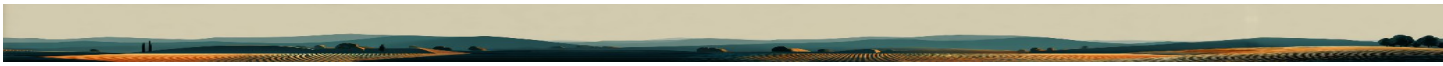
No endpoint detection and response

Standard antivirus looks for known threats. EDR looks for anomalous behavior — a process doing something it shouldn't, a file being encrypted in bulk, a user account accessing systems it's never touched before. Without EDR, that activity is invisible.

No backup of cloud services

The business assumes the cloud provider is backing up their email, their files, their shared documents. They're not. Cloud providers keep the platform running. They don't guarantee your data.

The Castle Wall Problem — Why Traditional Security Isn't Enough



LATTIS

Traditional network security works like a medieval castle. There's a wall, a moat, and a gate. If you get past the gate — through a phishing email, a stolen password, a compromised device — you're inside and you can move around freely. That's how ransomware spreads from one infected machine across an entire network in hours. The wall kept people out. Once someone was in, nothing slowed them down.

Zero trust is the answer to the castle wall problem. The idea is simple: getting inside the network doesn't mean you get to go everywhere. Every user, every device, every application has to prove who it is and what it's allowed to do — every single time, not just at login. A salesperson's laptop can reach the CRM but not the accounting server. A camera on the network can talk to the video management system but nothing else. A vendor logging in remotely can only access the specific system they're there to work on.

In practice for an SMB, zero trust shows up as things you already recognize: multi-factor authentication on every account, network segmentation so devices are isolated from each other, least-privilege access so users only see what they need, and monitoring that flags anything behaving outside its normal pattern. It's not one product. It's a philosophy that shapes every decision about how your network is built and managed.

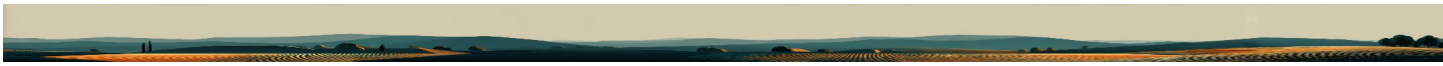
This Is What It Actually Looks Like — Three Real Incidents

I've been in the room when businesses found out they'd been hit. Here are three of those conversations — told as accurately as I can while protecting the people involved.

The Joke That Cost a Car Dealership $20,000

The controller at a car dealership received an email with a funny image attached. She opened it, saw the joke, laughed, and went back to work. What she didn't see was what happened underneath — a banking trojan installed itself silently on her computer. It included a keystroke logger and a component that watched for specific online banking portals.

When she opened her browser to log into the company's bank account, the virus hijacked the session. It created a new browser tab that looked identical to the bank's login page. She entered her username, her password, and her RSA multi-factor authentication code — and that information was instantly



transmitted to a criminal operating from a computer traced to a location in Georgia. The criminal used those credentials in real time, before the MFA code expired, to log into the actual bank account.

Four fictitious employees were added to payroll at believable salary amounts. The direct deposit accounts were mule accounts — accounts controlled by the criminal network that immediately transferred funds out once they arrived. By the time anyone noticed, approximately $20,000 was gone.

I sat in that meeting with the bank's vice president, who opened by saying there was nothing they could do. During the conversation I asked what monitoring the bank had in place to detect credential hijacking — and why a login from the customer's location would immediately initiate the kind of payroll transactions that followed. The vice president understood what I was getting at. By the end of the meeting, the bank refunded the money. Their own security posture hadn't held up to scrutiny.

The Patient Criminal and the $100,000 Wire

This one required no malware and no technical exploit. Just patience and one missing control.

A controller at a company with operations in multiple states had an email account with no multi-factor authentication. A criminal obtained her credentials — likely through a phishing email or a credential dump from another breach — and logged in quietly. They didn't do anything visible. They watched.

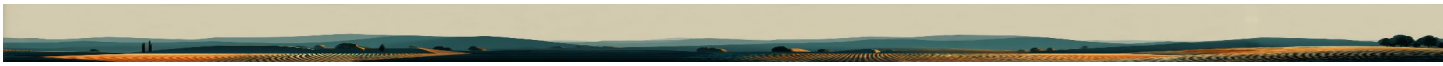
For weeks, the criminal monitored her inbox. They learned the cadence of the business. They saw that wire transfers were a normal part of operations. They identified the pattern of how payment requests arrived and how they were approved.

Then they set up an inbox rule — invisible to the controller — that intercepted incoming emails requesting payment via wire transfer, moved them to a hidden folder, edited the bank routing information, and placed the modified email back in the inbox. The controller received what looked like a legitimate payment request, processed it without verification, and wired $100,000 to the criminal's account.

The money was gone. No malware was ever installed. No system was ever breached in the traditional sense. One missing MFA control and a few weeks of patience was all it took.

The Ransomware Attack That Spread Across 20 Locations

I got a call from the president of a company. Their headquarters had been hit with ransomware. It had encrypted the servers and was moving through the computers at headquarters — and it was spreading outward across their site-to-site VPN network to remote locations. They had approximately 20 of them.



LATTIS

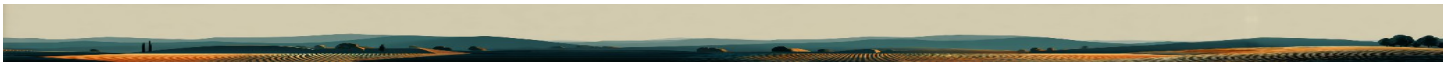
The first decision was to tear down the VPN connections to stop the spread. That isolated the headquarters damage but cut off the remote locations from central systems. Then the work of assessing and restoring began.

During the recovery, the in-house IT team brought a new accounting server online. It had never been backed up. That data was gone.

The cyber insurance company got involved. They negotiated with the criminals and ultimately paid a substantial ransom for the decryption key. Recovery took multiple days. The business survived because their main line-of-business application was cloud-hosted and stayed online throughout — but the accounting system was down, which created serious operational problems.

The aftermath was as significant as the attack itself. The insurance company paid close attention to this account going forward. The business was required to substantially improve their security posture and their systems resilience. The total investment to rebuild the environment correctly was well into six figures.

Two things made the difference between survival and something worse: cyber insurance that covered the ransom, and a cloud-hosted application that kept part of the business running. Two things made it worse than it needed to be: an unbacked server and a network that allowed the malware to spread freely before anyone could stop it.



LATTIS

Ransomware — What It Is and How It Works

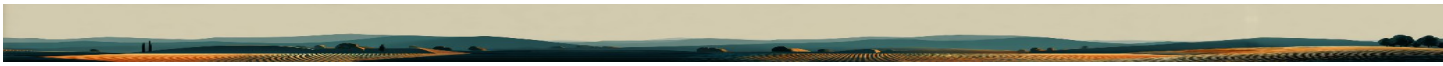
Ransomware is malicious software that encrypts your files and demands payment for the decryption key. It almost always arrives through a phishing email — an attachment someone opens, a link someone clicks. Once it's on one machine, it looks for everything it can reach on the network and encrypts that too. By the time anyone notices, the damage is done.

Modern ransomware operations don't just encrypt your data. They steal it first. They exfiltrate a copy of your most sensitive files before they activate the encryption. Then they threaten to publish that data publicly if you don't pay — what's known as double extortion. So even if you restore from backup and refuse to pay the ransom, they can still damage you by releasing confidential business information, client data, or employee records.

Ransomware Groups Have Customer Service

Sophisticated ransomware operations run like businesses. They have negotiation teams, payment portals, and a reputation to protect in their own criminal marketplace. They generally want to provide a working decryption key after payment — because if they develop a reputation for taking money and not delivering, victims stop paying and the business model collapses. That doesn't make them trustworthy. It makes them rational criminals with a financial incentive to follow through. It also means the ransom demand is often negotiable. None of this is a reason to skip backups. It's a reason to understand exactly what you're dealing with if you ever find yourself in that conversation.

The single most important protection against ransomware is backup architecture. Not just having backups — having backups that the ransomware couldn't reach. That means isolated backup systems on a separate network segment with no connection to the systems being backed up. If your backup is on the same network as your servers and workstations, and ransomware spreads across that network, your backup gets encrypted along with everything else. An isolated backup turns a catastrophic event into a painful but survivable one. You restore, you rebuild, you don't negotiate.



LATTIS

Email — The Most Common Attack Surface

Email is where most attacks start. A phishing email delivers a malicious attachment. A spoofed invoice redirects a payment. A compromised account watches your inbox for weeks before making a move. Securing email is not optional — it's the foundation of everything else.

Inbound email threat protection — a filtering layer that sits between the internet and your inbox — scans every message before it reaches your staff. It catches known malicious senders, analyzes attachments for malicious behavior, identifies spoofed domains that look like legitimate senders, and blocks phishing attempts that would otherwise land directly in the inbox. Pointing your mail records directly at your cloud email provider with no filtering layer is like leaving your front door open.

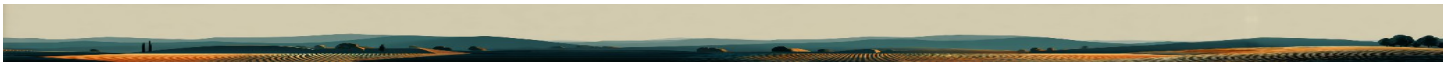
Outbound email encryption protects the sensitive information your business sends. Tax documents, payroll records, employee information, client financial data — all of it travels over email. Encryption ensures that information can only be read by the intended recipient. It also signals to clients and partners that you take their information seriously.

Multi-factor authentication on every email account is non-negotiable. A compromised password is a fact of life — data breaches happen constantly and credential lists circulate on criminal networks. MFA means a stolen password alone isn't enough to access the account. For businesses with shared accounts or staff without personal cell phones, hardware MFA tokens provide the same protection without requiring a personal device.

Endpoint Protection — Beyond Antivirus

Standard antivirus software looks for patterns of known threats. It compares files and processes against a database of identified malware. If the threat is new, or if it's been modified to avoid detection, antivirus misses it. That's not a flaw — it's a fundamental limitation of the model.

Endpoint Detection and Response — EDR — takes a different approach. Instead of looking for known bad things, it monitors for anomalous behavior. A process encrypting files in bulk. A user account accessing systems it's never touched. A program making outbound connections to an unknown server. When EDR sees behavior that doesn't fit the pattern, it locks down the affected system, initiates a



rollback of recent changes, alerts the IT team, and begins automated remediation. It doesn't wait for a human to notice.

Cloud email environments need their own layer of monitoring. A compromised email account behaves differently than a normal one — login attempts from unusual locations, access from known VPN services criminals use to mask their location, inbox rules that shouldn't exist. Monitoring the cloud environment for these signals catches account compromises that endpoint tools would never see, because the attack is happening in the cloud, not on the device.

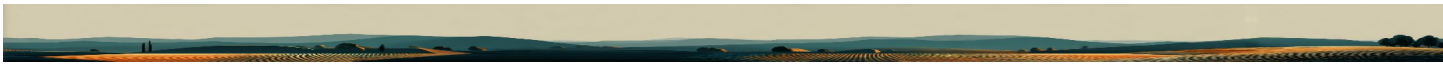
Network Security — Locking Down the Foundation

A flat network — where every device can reach every other device — is an attacker's best friend. One compromised laptop can talk to every server, every workstation, every camera, every printer on the network. Network segmentation fixes this by dividing the network into separate zones. Devices in one zone can't automatically reach devices in another. A compromised device is contained to its segment.

Wireless networks deserve particular attention. The guest wireless network should reach the internet and nothing else — no access to internal systems, no visibility into what's on the local network. The secure wireless network for staff should be on its own segment, authenticated against user credentials, and separated from other network traffic. And the wireless password for any network that has internal access should be changed regularly — because every former employee, every contractor, and every vendor who visited still knows the old one.

For organizations that want the strongest possible network access control, 802.1X authentication requires every device to prove its identity before it's allowed onto the network at all. Certificates or credentials are validated against a central authentication server before a switch port will pass traffic. Unauthorized devices — someone plugging a personal laptop into a network jack, a rogue access point someone brought in — simply don't get access. It's a powerful control for environments where the network perimeter matters.

An advanced firewall with intrusion detection and intrusion prevention inspects traffic flowing in and out of the network — not just whether it's allowed, but whether it looks malicious. Malware communicating with a command and control server. An internal device scanning the network in a pattern that suggests compromise. Payload inspection that catches malicious content before it reaches a device. This is the difference between a firewall that enforces rules and one that actively hunts for threats.



LATTIS

Backup — The Last Line of Defense

Every cybersecurity control can fail. Phishing emails get through. Credentials get compromised. Zero-day vulnerabilities get exploited before patches exist. Backup is the control that works even when everything else doesn't — but only if it's architected correctly.

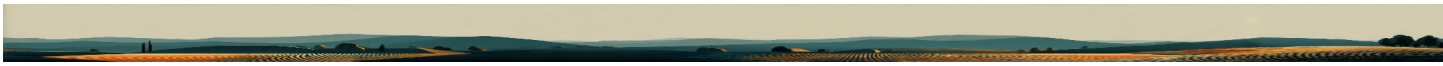
Enterprise backup at the hypervisor level captures the entire state of a server — not just files, but the operating system, the applications, the configuration, everything. That backup runs on an isolated network segment with dedicated storage that has no connection to the systems being backed up. Ransomware spreading across the main network can't reach it. A copy goes offsite to cloud storage. Three copies, two locations, one isolated from the rest of the network — that's the architecture that makes ransomware survivable.

Cloud services need their own backup strategy. Cloud providers keep their platforms running. They do not guarantee your data. If a mailbox is deleted, if ransomware corrupts shared files, if someone permanently removes documents from cloud storage, the cloud provider is not your recovery path. A separate backup of your cloud environment — email, shared documents, collaboration tools, file storage — gives you a recovery point that exists independently of what the cloud provider retains.

Password Management — The Overlooked Foundation

Credentials are one of the most poorly managed aspects of security in most businesses. Staff reuse passwords across personal and business accounts. Passwords are shared over email or written on sticky notes. When an employee leaves, shared passwords don't get changed. A data breach on an unrelated website exposes a password that someone also uses for their work email.

A password manager solves most of this. It generates strong unique passwords for every account, stores them securely, and makes them available to the right people without anyone actually knowing what the password is. For shared accounts — where multiple staff need access to the same login — a password manager provides that access without exposing the underlying credential. When someone leaves the company, access is removed from the manager and the password is rotated. Clean, documented, auditable.



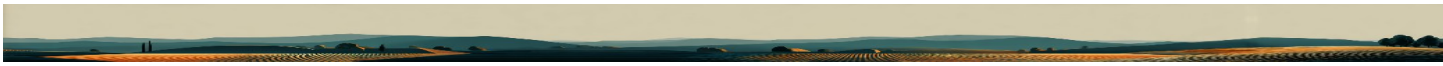
LATTIS

The House on the Street — How Opportunistic Attackers Think

You Don't Have to Be Impenetrable. You Have to Be Harder Than Your Neighbor.

Think of your business as a house in a neighborhood. Most hackers are opportunistic. They're not targeting you specifically — they're scanning for open doors. A house with the front door unlocked, the garage open, no fence, no lights, and no dog is an easy target. A house with a fence, motion-activated lights, locked doors with good deadbolts, and a German Shepherd is not worth the effort when the house down the street has none of those things.

You don't need a perfect security posture. You need a better one than the path of least resistance. Close the obvious gaps — MFA on every account, email threat protection, patched software, network segmentation, isolated backups, a password manager — and most opportunistic attackers will move on. The ones who are targeting you specifically are a different conversation. But they're also far rarer than the ones who are just looking for the unlocked door.

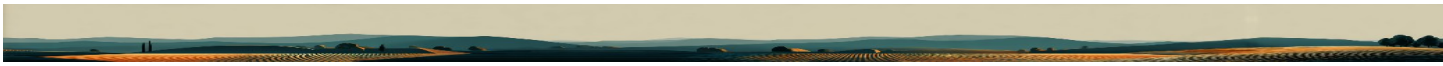


LATTIS

What to Do Right Now — A Prioritized Starting Point

Start here. In order of impact.

- ✓ **Turn on MFA for every email account —** this is the single highest-impact change most businesses can make today
- ✓ **Add email threat protection —** a filtering layer between the internet and your inbox
- ✓ **Add outbound email encryption —** sensitive information should never travel in plain text
- ✓ **Deploy endpoint detection and response —** go beyond antivirus to behavioral monitoring
- ✓ **Implement managed patching —** operating systems and applications, not just one or the other
- ✓ **Segment your network —** separate guest wireless, staff wireless, and internal systems
- ✓ **Change your Wi-Fi password —** and set a schedule to change it regularly going forward
- ✓ **Deploy a password manager —** for every user, for every shared account
- ✓ **Back up your cloud environment —** email, shared files, collaboration tools
- ✓ **Implement isolated on-site and offsite backup —** architecture matters as much as existence
- ✓ **Monitor your cloud accounts —** watch for anomalous logins and inbox rules that shouldn't exist
- ✓ **Get cyber insurance —** and make sure your controls meet what the policy requires
- ✓ **Document an incident response plan —** know who to call and what to do before it happens



LATTIS

Most businesses wait until after an incident to take security seriously. You don't have to.

We help businesses across San Luis Obispo and Santa Barbara Counties assess their security posture, close the obvious gaps, and build toward a more resilient environment. If you're not sure where you stand, start with a conversation. We'll tell you what we see — directly, and without a sales pitch.

lattisnetworks.com/contact | (805) 470-7666