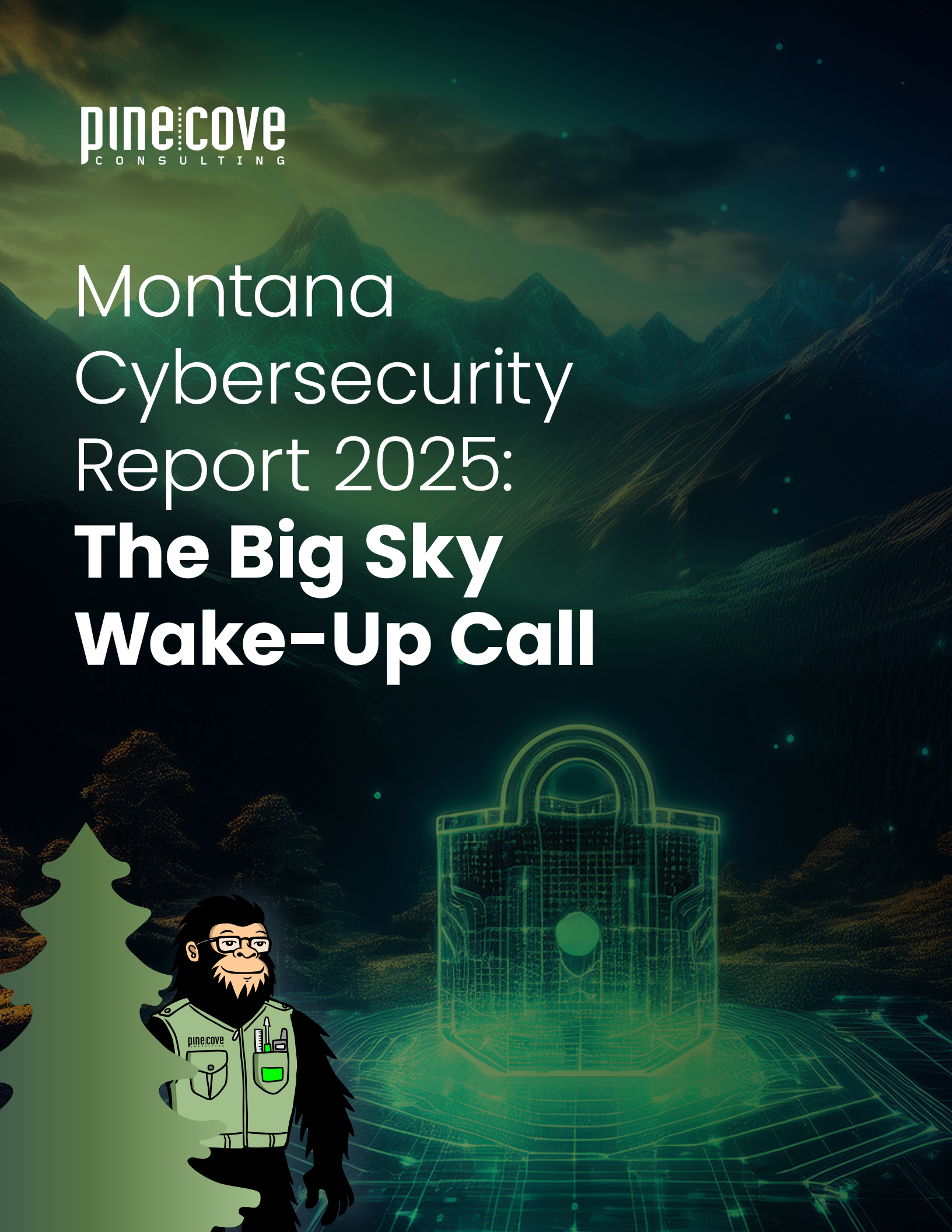
pine cove CONSULTING

Montana Cybersecurity Report 2025: **The Big Sky Wake-Up Call**



A letter from a local

I live here. I work here. I raise my family here. And like a lot of you, I want to see Montana thrive - not just in our towns and communities, but in the digital world too.

But let's be honest: cyber threats are hitting closer to home. Schools, hospitals, banks, and small businesses across our state are getting targeted because attackers think we're easy prey. This report is our way of pushing back.

We've packed it with real data, local insights, and practical steps to help you get ahead of the threats. It's not about fear - it's about being prepared.

Montanans are tough. We know how to take care of our own. Let's bring that same mindset to cybersecurity.

See you out there,

Brandon Vancleeve
President, Pine Cove Consulting

Executive Summary

Cybersecurity is no longer just a technical IT issue; it's a governance imperative for organizations in Montana. Attacks that once seemed distant are now knocking on the doors of our schools, hospitals, city halls, and small businesses. This report consolidates critical intelligence on Montana's cybersecurity landscape, with insights from public records, industry research, and Pine Cove Consulting's decades of experience supporting rural America.

If you're a business owner, Director of IT, CISO, or CTO in Montana, the question isn't if a cyber threat will strike, i t's when.

Key findings

- ✔ **Ransomware and Data Breaches Are Surging:** Higher education, healthcare, government agencies and other critical sectors in Montana are increasingly targeted. Recent high-profile breaches at LoanDepot, Planned Parenthood of Montana, and Montana State University underscore that even flyover country is on the front lines of global cybercrime. Attackers infiltrated Montana institutions, stealing sensitive personal, financial, and health data and forcing operations offline.

- ✔ **Local Vulnerabilities, Global Threats:** Smaller IT teams and leaner budgets have made Montana a soft target in the international threat landscape. Rural does not mean immune - quite the opposite. Adversaries are becoming faster and more sophisticated. For example, the average breakout time (time from initial breach to lateral movement) fell to just 48 minutes globally, with the fastest cases only 51 seconds. In 2024, ransomware attack volumes exploded by 259% in Latin America and rose 8% in North America, indicating that threats are escalating everywhere, including here in Montana.

- ✔ **Gaps in Cyber Readiness:** The human and process gaps in Montana's cyber defenses are alarming. In interviews with IT leaders, 62% reported having no dedicated cybersecurity personnel, 45% have no formal incident response plan, and over 70% do not conduct regular vulnerability scans. These gaps create wide-open doors for bad actors. A lack of resources leads to slower breach detection and response, which is catastrophic when every second counts. (For comparison, surveys indicate over half of companies globally still lack a documented incident response plan.) It's like responding to a wildfire with a single firefighter and a garden hose.

- ✔ **Economic and Reputational Stakes Are High:** The cost of cyber incidents is not just the ransom or IT recovery - it's the loss of trust, public disruption, and legal fallout. The global average cost of a data breach reached $4.45 million in 2024, the highest ever, and in the U.S. it's even higher at $10.43 million. Certain sectors incur extreme costs - healthcare breaches, for instance, are the most expensive. Yet many Montana organizations remain uninsured or under-prepared for these financial impacts. Nationally, breaches take an average of 277 days (about 9 months) to identify and contain, and interviews suggest Montana's detection times can exceed 240 days - meaning attackers may roam in networks for months. This long dwell time drives up the ultimate cost and damage of breaches.

- ✔ **IT Leaders as Risk Strategists:** Today's IT leaders in Montana must wear two hats - operational guardian and strategic risk manager. They are now front-line defenders of Montana's digital economy. This expanded role means proactively briefing executives on cyber risks, hunting for threats before they strike, practicing incident drills, and integrating cybersecurity into business continuity planning. In fact, ransomware is now the #1 concern of executives in 62% of organizations, reflecting how cybersecurity has become a boardroom priority. Montana's IT professionals are rising to this challenge, but they need support, training, and executive buy-in to succeed.

Our Roadmap to Resilience

To address these challenges, Pine Cove Consulting outlines a **Roadmap to Resilience** structured around four strategic pillars: **Awareness and Assessment, Infrastructure Hardening, Response Readiness, and Continuous Improvement**. Within each pillar, we present actionable steps (a field manual) that schools, hospitals, utilities, government agencies, and businesses can take to elevate their cybersecurity posture and reduce risk exposure. These recommendations are grounded in industry best practices and informed by the latest threat intelligence from leading cybersecurity technology manufacturers, ensuring Montana's strategy is both locally relevant and globally aware.

If your role touches public trust, digital systems, or operational continuity in Montana, this report is for you. It's both a wake-up call and a handbook for action. The following pages combine hard data with real-world narratives to illustrate not just what is happening, but why it matters for Montana's future. We begin by examining how the threat landscape has evolved for Montana, then delve into the readiness gap that persists, and finally outline strategic steps to fortify our defenses. Let's start by looking at where we stand today, and how we got here.

Introduction: A Matter of Urgency and Credibility

Picture this: It's Monday morning and Montana State University's network is paralyzed. Administrators can't access student records; faculty can't log in to their systems; emails across campus bounce back with cryptic error messages. By noon, the truth is clear—a ransomware attack has taken hold. Critical data is locked, attackers are demanding millions, and an institution that thousands rely on is at a standstill. This isn't a hypothetical scenario pulled from an IT horror story. It's Montana's new reality.

Cybersecurity is no longer just a back-office IT concern - it's a core threat to operations and public trust. Attacks that once felt like big city problems have reached Montana's schools, hospitals, city halls, and small businesses. If you're reading this, the question isn't whether your organization will face a cyber threat. It's whether you'll be ready when it happens. The credibility of our institutions and businesses is on the line. A single breach can erode customer confidence, disrupt vital services, and even put lives at risk (consider the stakes if a hospital's systems are taken down or a power utility is compromised).

This report consolidates the most critical intelligence available on Montana's current cybersecurity landscape. We've compiled data from public breach records, interviewed frontline IT leaders in Montana, and drawn on Pine Cove Consulting's 20+ years of experience protecting critical infrastructure in rural America. Where local data was unavailable, we've noted the gaps and pointed to areas for future investigation. The goal is to paint an honest picture of threats and preparedness in Big Sky Country, and to lay out a pragmatic action plan for resilience.

The Montana Threat Landscape: Then and Now

Cyber incidents in Montana are no longer rare or theoretical - they are frequent, impactful, and increasingly coordinated. Just a few years ago, a cyberattack on a local school district or business in Montana might have seemed far-fetched. Today, we have tangible examples happening in our own backyard. From ransomware infiltrating higher education to healthcare data being exfiltrated and leaked online, the state's most critical institutions have become regular targets for cybercriminals.

Recent Montana Breaches

In early 2024, a breach at **LoanDepot** (a national mortgage lender) exposed the personal data of over 49,000 Montanans as part of a massive ransomware attack. Weeks later, in August 2024, **Planned Parenthood of Montana** confirmed a cyberattack by the RansomHub ransomware group, which stole 93 gigabytes of sensitive data. This trove reportedly included sensitive health records and internal documents.

Around the same time, Montana's higher education was hit: **Montana State University** suffered a major ransomware incident in April 2023, with hackers claiming to have stolen over 100 GB of data including student and faculty records. **Great Falls College MSU** was also breached by likely the same Royal ransomware group in 2023, forcing parts of its systems offline. And these are just the publicized incidents—many organizations quietly face smaller ransomware attacks, business email compromise scams, or data theft attempts that never make headlines.

Education Sector Particularly at Risk: Educational institutions in Montana face heightened vulnerability due to increased hybrid and digital learning environments. According to Bitdefender's analysis, educational institutions are prime targets for ransomware due to rigid schedules and limited IT response capacities, causing recovery periods of 2 to 9 months, and potentially incurring losses up to $1 million. Tyler Baker, Director of Global Security Operations at Bitdefender, emphasizes: "Adversaries are increasingly bypassing traditional defenses by exploiting legitimate tools and applications already present in business environments. Our recent analysis of over 700,000 incidents found that 84% of attacks now involve Living-Off-the-Land (LOTL) techniques, making attack surface reduction a critical objective for organizations of all sizes."

The Broader Shift

These are not isolated incidents; they reflect a broader shift. Montana's digital infrastructure is now part of a national and international threat surface. Our state may be rural, but our networks are connected to the world - and that means global adversaries are only a phishing email or unpatched server away. Rural does not mean immune. In fact, the opposite is proving true: smaller teams and leaner cybersecurity budgets often mean slower detection and greater damage once attackers get in. Cybercriminals know this. They view Montana's organizations as softer targets compared to heavily fortified big corporations. A school district's IT network or a county government's database may lack the advanced defenses of a Fortune 500 company, yet they hold valuable personal data and sometimes control critical services.

Global Sophistication Meets Local Vulnerability

The tactics and tools used by attackers are more sophisticated than ever, but they are being unleashed on local targets. According to the CrowdStrike Global Threat Report 2025, adversaries have dramatically accelerated their attacks - the average time from an initial breach to spreading across a network (breakout time) dropped to just 48 minutes, with the fastest observed case only 51 seconds. In practical terms, this means a hacker might start stealing data or deploying ransomware in the time it takes you to grab a coffee.

Meanwhile, SonicWall's 2025 Cyber Threat Report notes that ransomware attacks surged 259% in Latin America and 8% in North America last year. We cannot assume Montana's geographic isolation offers any protection; threat actors anywhere can and do reach us through the internet. The Verizon 2025 Data Breach Investigations Report identifies additional concerning trends relevant to Montana organizations, notably a rise in third-party involvement in breaches, increasing from 15% to 30%

year-over-year. Ransomware remains a top concern, accounting for 44% of breaches analyzed globally. Verizon specifically notes increased vulnerabilities exploitation targeting edge devices and VPNs, with credential compromises exacerbated by poor remote work practices.

Evolving Attack Methods

Trends also show attackers are employing more brutal techniques. **Double extortion** - where data is not only encrypted but also stolen and threatened to be leaked - was prolific in 2024, and even triple extortion schemes are emerging. In **triple extortion**, attackers add additional pressure, for instance by attacking customers or launching DDoS attacks until payment is made. These statistics are more than numbers - each percentage increase represents shattered businesses, disrupted classes, or compromised patient records. The cost of cyber threats is not just financial; it's the erosion of trust, the paralysis of critical operations, and the invasion of personal privacy.

The Dwell Time Problem

Montana's recent experiences mirror national patterns. What's especially worrying is the dwell time of attackers in our systems. Nationally, the average time to identify and contain a breach is about 277 days (roughly 9 months). In Montana, interviews with IT leaders suggest local detection times can be even longer - often well over 240 days (8 months) in some cases. That means intruders could be quietly lurking and siphoning data for most of a year. Every extra day undetected increases the harm done. (For context, IBM's 2024 research found breaches that lingered over 200 days cost organizations $5.46M on average, significantly more than quicker-discovered breaches.)

The bottom line: Montana is not immune; it is exposed. Our state's organizations are caught in the same storm as the rest of the world. The threats are at our doorstep, and in some cases already inside. The next section explores how prepared (or not) we are to meet this challenge head-on.

Montana's Cyber Readiness Gap: A Crisis in the Making

The cracks in Montana's cyber defenses are not just technical - they're organizational and foundational. Across school districts, local governments, healthcare providers, and private enterprises, cybersecurity responsibility often falls to one or two overworked IT staff who wear many hats. These professionals are tasked with an almost impossible balance: keeping daily operations running, supporting hundreds of users, and defending against a constant barrage of sophisticated threats. It's a recipe for burnout and breaches.

Alarming Statistics

Our conversations with IT leaders across Montana revealed sobering statistics about this readiness gap:

- ✔ **62%** said they have no dedicated cybersecurity personnel on staff
- ✔ **45%** have no formal incident response plan (meaning when an attack hits, they're improvising on the fly)
- ✔ **Over 70%** do not perform regular vulnerability scanning or penetration testing of their systems

These aren't just numbers - each percentage point is an open door for attackers. Without skilled security staff, threats go undetected longer and responses are slower. Without an incident response plan, even knowing who to call or what steps to take in the first critical hours of a breach becomes chaotic. Without regular scanning, organizations are effectively blind to the weaknesses in their armor.

The Resource Challenge

These readiness gaps in Montana echo broader trends among small and mid-sized organizations. (A recent industry analysis noted that 55% of companies worldwide lack an up-to-date incident or crisis response plan.) The difference is, larger entities may have other mitigating defenses, while many Montana organizations operate with

extremely limited IT teams. It's not uncommon for a single administrator to manage everything from user support to network infrastructure to security. One local county IT director described it as "fighting a wildfire with a garden hose—you do what you can, but it's nowhere near enough for the scale and speed of the threat."

The Impact of Resource Gaps

The impact of this resource gap is evident in outcomes. Longer detection times (as noted, often exceeding 8 months locally) give attackers a huge head start. By the time many Montana organizations realize they've been breached, the damage is already done - data has been stolen and possibly sold online, ransomware has spread to every server, backups have been wiped or encrypted by the attackers (a common tactic - in 95% of ransomware attacks on healthcare, attackers tried to compromise backups, and succeeded 66% of the time). Recovery then becomes drastically more difficult and costly. It's no wonder that some businesses hit by ransomware never fully reopen, or that public agencies face citizen outrage and legal repercussions after preventable breaches.

The Human Factor

Another aspect of the readiness gap is training and awareness. Many breaches start with a simple phishing email that tricks an employee. Yet, cybersecurity awareness training is irregular at best in many organizations. Only a minority of Montana's smaller organizations conduct frequent phishing simulations or mandatory security training. When users aren't trained, they remain the weakest link - and attackers know it. (Globally, the most common breach vector in 2024 was stolen or compromised credentials, and phishing was the second-most common. These straightforward attack methods thrive on human error and lack of training.)

In short, Montana faces a perfect storm of cyber risk: determined global threat actors on the offensive, and local defenses strained to the breaking point. Imagine responding to a five-alarm fire with a single firefighter - that's our current state of cyber readiness.

It's not enough to acknowledge the threat; we must act decisively to close these gaps. The good news is, improving readiness is achievable with the right strategy and support. The next section discusses how IT leaders are evolving their role to meet this challenge, and later we'll outline practical steps under our Roadmap to Resilience to start shoring up Montana's defenses.

The New Role of IT: From Firefighter to Risk Strategist

IT leadership in Montana organizations is undergoing a fundamental transformation. Traditionally, IT managers and directors were the behind-the-scenes firefighters - expected to keep systems running and put out tech fires when they flared up. Now, they also must serve as forward-looking risk strategists. In today's environment, keeping the servers online is only part of the job; protecting the business's digital assets and continuity has become equally critical.

What This New Role Looks Like

Executive Engagement: First, IT leaders are taking a seat at the executive table more often, briefing CEOs, boards, or city councils on cyber threats and preparedness. They are translating technical risks into business terms—for example, explaining how a ransomware attack could halt revenue, jeopardize patient safety, or disrupt public services. This aligns with national trends: in a recent CFO survey, ransomware topped the list of C-suite concerns in 62% of organizations. Cyber risk is now business risk, and Montana's IT leaders are the ones who understand it best.

Proactive Risk Assessment: Second, there is a proactive shift towards cyber risk assessment and planning. Rather than waiting for an incident to occur, leading IT teams in Montana are initiating regular security assessments, vulnerability scans, and even hiring third parties to conduct penetration tests or red team exercises. They are identifying weaknesses before bad actors do, and shoring up defenses in advance. This includes not

just technical fixes but also process improvements, like ensuring software patches are applied rapidly (especially since 75% of exploits are leveraged by attackers within just 4 days of a vulnerability's public disclosure.) Being proactive greatly reduces the chance of a successful attack.

Threat Intelligence and Hunting: Another strategic priority is threat intelligence and hunting. Larger organizations and consortiums (like state agencies or healthcare networks) are starting to subscribe to threat intelligence feeds and share information about potential threats targeting the region. Some IT departments are practicing threat hunting—actively looking through system logs and network traffic for signs of intrusion rather than waiting for an alert. This active defense mindset can catch stealthy attackers who might evade basic security tools.

Cybersecurity Drills and Training: Critically, IT leaders are championing regular cybersecurity drills and training. Just as organizations run fire drills, forward-leaning Montana businesses and schools are beginning to run cyber incident drills. This could be a tabletop exercise where leadership walks through a ransomware outbreak scenario, or technical drills to test backup restoration and incident response procedures. The purpose is to ensure that when (not if) a breach occurs, everyone knows their role and can act swiftly. As one Montana CIO put it, "We don't want our first test to be the real thing." Practice reveals gaps in response plans and builds muscle memory for the team. It can also highlight the need for external partnerships—for example, knowing when to call in incident response specialists or law enforcement.

Support Requirements

To fulfill these new expectations, IT leaders need support: budgets for security tools and training, authority from executives to enforce security policies, and perhaps most importantly, a shift in organizational culture to treat cybersecurity as a shared responsibility (not just "the IT guy's problem"). In Montana, where resources are tight, creative approaches are being used—such as managed security service providers (MSSPs) that can monitor networks 24/7 on behalf of a small IT team, or regional collaborations where multiple counties or school districts share a cybersecurity expert. These can be effective force-multipliers.

The Evolution

The evolution from firefighter to strategist is challenging, but it's also empowering. IT leaders are now recognized as key defenders of organizational survival, not just the people who fix email outages. As one outcome, we're seeing cybersecurity and business continuity become a standing item in leadership meetings. The language of risk (likelihood, impact, mitigation) is entering the conversation. This is a positive development; it means cyber preparedness is being treated with the seriousness it deserves.

The following section provides a structured action plan—a Roadmap to Resilience—that IT leaders and executives in Montana can jointly pursue. It's time to move from awareness to concrete steps.

Roadmap to Resilience: A Strategic Action Plan

Securing Montana's digital future isn't about panic or throwing money at random tools - it's about strategic, sustained action. Pine Cove Consulting's **Roadmap to Resilience** is structured around four pillars that together form a continuous cybersecurity lifecycle: **Awareness and Assessment, Infrastructure Hardening, Response Readiness, and Continuous Improvement**. These pillars align with best practices recommended by cybersecurity experts and are tailored to the common challenges we see in Montana. This is not a one-time checklist, but a culture of vigilance and adaptation.

Below, we break down each pillar with actionable steps:

1 Awareness and Assessment

Human error remains one of the leading causes of security breaches. Building a strong security culture through awareness and regular risk assessment is the first line of defense. While technology is critical, the end user is often the deciding factor in stopping breaches or letting them in. Organizations should invest in educating their people and understanding their own vulnerabilities.

Key steps under this pillar:

- ✔ **Security Awareness Training for All Staff:** Conduct mandatory cybersecurity training for employees at least annually (ideally more often in short modules). Phishing simulation campaigns are highly effective - users learn to recognize suspicious emails before a real one lands in their inbox. Given that phishing was the entry point in ~15% of breaches and led to an average $4.76M cost per incident globally, training here delivers significant risk reduction. People should know how to spot common attack signs (strange senders, urgent requests for money/data, etc.) and feel empowered to report potential threats.
- ✔ **Executive and Board Briefings:** Ensure leadership is aware of cyber risks and their potential business impact. Frame it in terms of operational downtime, financial loss, safety, or reputation damage. This top-down awareness drives commitment. For example, if executives understand that ransomware could halt revenue or endanger patients, they are more likely to support funding security initiatives. Regularly brief the board or city council on the organization's security posture and improvements (quarterly or semiannually).
- ✔ **Cyber Risk Assessments and Audits:** Perform periodic assessments to identify where your vulnerabilities lie. This could involve an external security audit or a framework-based self-assessment (using tools like NIST CSF or CIS Controls). Identify critical assets (what data or systems would hurt most if compromised) and key threats to those assets. In many Montana organizations, basic assessments have revealed low-hanging fruit to fix—such as outdated software, weak passwords, or excessive user privileges. Catalog these issues and prioritize remediation. Assessment is the foundation on which all other improvements build.
- ✔ **Inventory and Classification of Data:** You can't protect what you don't know you have. Take inventory of sensitive data—whether it's student records, patient info, financial data, or customer personal information. Classify data by sensitivity and apply stricter controls to high-value data. For instance, sensitive personal data might be encrypted at rest and in transit, and access given only to staff who truly need it. Knowing your crown jewels focuses awareness efforts (e.g., employees handling sensitive data need extra training and scrutiny).

By fostering an informed workforce and leadership, and by continually assessing your risk, you create a security-conscious culture. Remember, awareness is an ongoing effort, not a one-off training video. Many Montana breaches could have been prevented or mitigated if just one person had spotted something strange and spoken up. Pillar 1 sets that expectation that cybersecurity is everyone's job.

2 Infrastructure Hardening

Once you know your risks from assessments, the next step is to harden your infrastructure - in other words, strengthen the shields and locks that protect your systems and data. Infrastructure hardening means implementing layers of security controls so that even if one is bypassed, others will stop or slow an attacker. Given how quickly attackers exploit new vulnerabilities (often within 48 hours of a fix being announced), a proactive, layered defense is vital.

Key steps to Harden Infrastructure:

- ✔ **Keep Systems Patched and Updated:** Establish a robust patch management routine. Apply security updates to servers, PCs, network devices, and software as soon as feasible - ideally within days, not weeks. This is crucial: 75% of the time, hackers start exploiting known security weaknesses within 4 days of a vulnerability's public disclosure. Consider enabling automatic updates where possible, and for critical systems, schedule expedited patch windows. Don't forget firmware and forgotten devices (printers, IoT sensors, etc. can have vulnerabilities too). Prompt patching closes the door on many opportunistic attacks.
- ✔ **Implement Multi-Factor Authentication (MFA) Everywhere:** Passwords alone are no longer sufficient. Weak or stolen passwords remain a top entry point for attackers. Enforce MFA for all users on email, remote access (VPNs), and any critical application. Modern phishing kits even try to steal one-time codes, so if possible use phishing-resistant MFA (like app-based push prompts or hardware security keys). Yes, MFA adds a minor inconvenience, but it dramatically reduces the chance that a single stolen password leads to a breach. Many major attacks in recent years would have been thwarted by MFA. For Montana organizations, this is one of the highest ROI defenses.
- ✔ **Critical Security Practices:** Leading cybersecurity experts at Marsh McLennan Agency emphasize that Montana organizations must prioritize MFA for all remote and privileged administrative access, adopt Endpoint Detection and Response (EDR) solutions, maintain regular patch management and vulnerability assessments, develop comprehensive and routinely-tested incident response plans, and conduct ongoing cybersecurity awareness training with regular phishing simulations. For financial operations, they recommend stringent secure practices for wire transfers, including dual authorization, segregation of duties, and thorough account verification processes.
- ✔ **Endpoint and Network Security Tools:** Deploy reputable endpoint protection on all servers and workstations—ideally modern Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) services that use behavior-based detection. Traditional antivirus is often not enough against advanced malware or fileless attacks. On the network side, ensure you have next-generation firewalls with intrusion detection/prevention features, and consider network monitoring

systems that can alert on abnormal activity. Segment your network so that a breach in one system doesn't immediately grant access to everything (for example, keep student lab networks separate from administrative networks, or isolate critical industrial control systems in utilities). Network segmentation contained the damage in some recent incidents.

- ✔ **Backup Systems and Offsite Backups:** Regular, reliable backups are a cornerstone of ransomware resilience. Ensure you are backing up critical data and systems frequently (daily or better for key data). Critically, keep copies of backups offline or offsite so attackers cannot easily find and encrypt or delete them. Test your backups periodically to make sure you can actually restore from them—too many organizations only discover their backups were failing after an attack. Strong backups can turn a potential multi-million dollar ransom event into a much smaller disruption (though data leak threats still remain). One note: also back up configuration data like network device configs, Active Directory, etc., not just user files.
- ✔ **Apply the Principle of Least Privilege:** Review user accounts and permissions. Users (and IT admins) should have the minimum access necessary for their roles. For example, if an accounting staff member doesn't need access to HR records, don't grant it. Domain admin or root access should be tightly limited to only those who absolutely need it, and they should use separate admin accounts for privileged tasks. This way, even if an attacker compromises a user account, the damage is limited by what that account can do. Consider network access controls as well—not every machine needs to talk to every other. Limit lateral movement pathways.
- ✔ **Adopt a Zero Trust Posture:** Zero Trust is a modern security philosophy that basically says "never trust, always verify." In practice, this means continuously authenticating and authorizing user and device identity for each session or transaction. Implementing Zero Trust can be complex, but start with small steps: require VPN for administrative access, use network segmentation and MFA as noted, and monitor for any device or user accessing resources they normally shouldn't. Assume that your network may already be penetrated and design controls to catch abnormal behavior (for example, an employee device trying to access a server it never has before could be a red flag). As SonicWall emphasizes, strict access controls and not assuming any implicit trust can greatly reduce an intruder's ability to roam free.

Hardened infrastructure doesn't mean your organization becomes impenetrable - but it does mean attackers will have a much harder time succeeding. Think of it like reinforcing a house: sturdy locks, an alarm system, maybe a watchdog. A burglar might still attempt entry, but you've raised the effort and risk to them. Many will move on to easier targets. For Montana's would-be soft targets, infrastructure hardening is how we stop being low-hanging fruit in the eyes of cybercriminals.

3 Response Readiness

No defense is 100% foolproof. Despite our best prevention efforts, incidents may still happen—and when they do, the speed and effectiveness of your response determines whether it's a momentary scare or a full-blown crisis. Response Readiness means having a tested plan, tools, and skills in place so that when an incident strikes, your team can spring into action and contain the damage rapidly. It's often said that in cybersecurity, it's not if you'll be breached, but when. This pillar embraces that reality and prepares for it.

Key steps to Enhance Response Readiness:

- ✔ **Develop and Document an Incident Response Plan (IRP):** If you don't have one, make this a priority. An IRP is a playbook that outlines roles, responsibilities, and step-by-step procedures for handling different types of incidents (ransomware, data breach, denial of service, etc.). It should answer: Who declares an incident? Who is on the response team (IT, management, communications, legal)? How do we contain malware spread? At what point do we involve outside experts or law enforcement? Having this written down and approved by leadership before an incident is critical. Keep the plan simple, practical, and accessible (printed copies in case networks are down). Without a plan, every incident starts in chaos. Organizations with a solid IR plan save on average $1.49 million in breach costs due to faster and more efficient response.
- ✔ **Practice the Plan with Drills:** A plan on paper isn't enough—teams need to practice. Conduct periodic incident response drills or tabletop exercises. This can be as simple as walking through a ransomware scenario: "It's Monday, all files are encrypted and a ransom note appears—what do we do first, who calls whom?" Through drills, you'll uncover gaps or uncertainties in the plan. Maybe you realize you don't have an easily reachable contact at your cyber insurance or that your technical staff isn't sure who has authority to shut down systems. Drills build confidence and identify improvements. Even a half-day tabletop exercise once a year can dramatically improve real incident outcomes. Frontline IT staff in Montana have reported that exercises helped them discover, for example, that backup restoration procedures were unclear—a fix made before an actual attack, thanks to the drill.
- ✔ **Ensure Backup and Recovery Preparedness:** We already stressed having good backups in Pillar 2; response readiness means being prepared to use them quickly. Keep documentation of restoration procedures and make sure multiple team members know how to perform them. If ransomware hits, swift restoration from backup can be your ace card—but only if you've planned and tested it. Also consider: Do you have spare hardware or cloud capacity to restore into if primary systems are compromised? How long will it take to get critical systems back up (what's your target Recovery Time Objective)? Knowing these answers in advance helps manage expectations during a crisis.
- ✔ **Establish External Support Relationships:** Identify now which external partners you might need in an incident. This could include an incident response firm (many companies keep a retainer or at least a contract in place with specialists who can be called 24/7), legal counsel knowledgeable in breaches, public relations support, and law enforcement contacts (the local FBI field office cyber task force, for instance). The moments after discovering a breach are not when you want to be frantically searching for qualified help. Montana organizations should also know that federal agencies like CISA and the FBI encourage reporting significant cyber incidents; they can sometimes provide technical assistance and will certainly use the intel to warn others.

Ensure your IR plan has an up-to-date contact list for all these stakeholders. In the event of something like a widespread ransomware attack, having pre-existing relationships can save precious time.

- ✔ Cyber Insurance and Communication Plans: As part of readiness, evaluate if cyber insurance is right for your organization (many find it valuable to cover certain costs, though it's not a substitute for good security). Know the terms—for example, insurers often require notification within 48-72 hours of an incident. Include that in your plan. Also, formulate a communications plan for incidents: who will inform employees, what do we tell customers or the public and when? Transparency is important, but so is accuracy; having templated communications and an approval process in advance helps avoid panic and misinformation.

The goal of response readiness is to contain and mitigate the damage quickly when the unthinkable happens. A fast, coordinated response can mean the difference between a minor disruption and a multi-million dollar catastrophe. Recall that IBM data found organizations with well-trained incident response teams significantly cut down the lifecycle of a breach, by over 70 days on average. That can translate to huge cost avoidance and less harm. For Montana entities, this pillar is your business continuity insurance—you hope you won't need to execute these plans, but you'll deeply regret it if you haven't prepared and an incident occurs.

4 Continuous Improvement

Cybersecurity is a dynamic, never-ending journey. The threat landscape evolves constantly—attackers find new vulnerabilities, new attack techniques (we've seen how AI tools have turbocharged attacks like never before, e.g. a 452% spike in certain AI-aided exploits), and organizations themselves change (new systems, new employees, etc.). Continuous Improvement is about establishing processes to regularly learn, adapt, and strengthen your cybersecurity posture over time. In essence, it's making security part of the organizational DNA, not a one-time project.

Key aspects of Continuous Improvement:

- ✔ **Post-Incident Reviews (Lessons Learned):** After any security incident or major drill, conduct a formal debrief. Analyze what happened, what was done well, and where the gaps were. If a breach occurred, how did it slip through? If the response was slow, why? Document these findings and turn them into concrete actions. For example, a post-incident review might reveal that staff didn't recognize an initial phishing email—the improvement could be to implement more frequent phishing tests and training refreshers. Or you might find your network monitoring failed to alert on certain behavior—leading to an upgrade or tuning of the system. Treat every incident (or near-miss) as free training from the universe on how to get better.
- ✔ **Stay Updated on Threat Intelligence:** Keep informed about emerging threats and trends, especially those relevant to Montana's key sectors. Subscribe to threat intelligence newsletters or feeds (many are free from companies like Pine Cove or agencies like CISA or MS-ISAC for government/education). Join information-sharing groups if available—for example, the Multi-State Information Sharing & Analysis Center (MS-ISAC) shares timely alerts tailored for states and local entities. When credible warnings arise (e.g., a new ransomware campaign targeting K-12 schools or a critical zero-day vulnerability), convene your team to assess and act (apply patches, heighten monitoring, etc.). The sooner you know about a threat, the more time you have to prepare or block it.

- ✔ **Invest in Advanced Security Tools Thoughtfully:** Evaluate and adopt new technologies that can significantly improve defense or response. This could include security automation and AI-driven tools that help overwhelmed staff detect anomalies. The impact can be huge—organizations that extensively used AI and automation in security cut their breach detection and response times by 108 days and saved about $1.77 million compared to those that didn't. For example, implementing an automated endpoint detection system could catch and quarantine ransomware in seconds, whereas a human might not react until the damage is done. However, tools are not a panacea—choose solutions that fit your environment and be sure you have the expertise to use them effectively (or a service to manage them).
- ✔ **Continuous Training and Skills Development:** Encourage and fund ongoing training for IT and security staff. Cyber threats evolve, and so must the defenders' skills. This might mean technical courses for your sysadmin on incident response techniques, or sending staff to cybersecurity conferences or workshops (even virtual ones). For general staff, keep the security awareness training fresh—change up phishing simulations, share news of relevant breaches in staff newsletters (see, this happened at a hospital in a neighboring state) to keep awareness real. A culture of continuous learning keeps complacency at bay. Celebrate improvements too—for instance, if phishing click rates drop by 50% after a new training initiative, acknowledge that win.
- ✔ **Regular Policy and Control Reviews:** At least annually (if not more), review your security policies, procedures, and configurations. Businesses change—maybe you adopted new cloud services this year or went through a merger. Do your access controls, network diagrams, and policies reflect current reality? Update them as needed. Also, conduct periodic vulnerability scans and even penetration tests on an ongoing basis (many organizations do quarterly scanning and annual external pen tests). Treat compliance requirements (if any, like HIPAA for healthcare or CJIS for law enforcement data) not as checkboxes but as baseline standards to continuously meet or exceed.

Continuous improvement prevents stagnation. Attackers certainly aren't standing still—if your defense today is the same as it was two years ago, you are at risk of falling behind. A poignant example is the rise of new tactics like the use of generative AI for crafting highly convincing phishing and fake personas—which means training that was sufficient last year might need an update to cover these new ploys. Or consider the surge in attacks on previously less-targeted sectors like agriculture; if you operate in that space, what was a low concern area before may now need more attention. The point is to keep iterating.

In summary, Pillar 4 is about building a resilient cybersecurity program that gets smarter and stronger each year. It's the acknowledgment that cybersecurity is a marathon, not a sprint. For Montana organizations, adopting this mindset will ensure that the investments you make don't wither on the vine but continue to bear fruit as threats evolve. It also sends a message to would-be attackers: we are not static targets—we're raising our game continuously.

Conclusion: The Responsibility Ahead

The data is clear. The risks are real. Montana can no longer afford to take a laissez-faire approach to cybersecurity. This report has shown that our state's organizations—from schools to hospitals, banks to utilities, family businesses to government agencies—are in the crosshairs of global cyber threats. We have also seen that preparedness pays off: those who invest in resilience suffer far less harm when attacks occur. Now is the time to close the readiness gap and take responsibility for defending our digital frontier.

The Roadmap to Resilience outlined here is not theory; it's a practical guide drawn from both local insights and global best practices. By focusing on **Awareness and Assessment, Infrastructure Hardening, Response Readiness, and Continuous Improvement**, any organization can meaningfully improve its security posture. This doesn't require the budget of a Fortune 500 company—many recommendations are about strategy, process, and smart use of available resources. Cybersecurity is as much about mindset and discipline as it is about hardware and software.

Montana has always been a place where communities look out for each other, where preparedness for harsh winters or wildfires is part of the culture. Cyber threats are just another storm we need to weather—except in this case, we have the advantage of foreknowledge and tools to fortify ourselves before the storm hits. Business owners and public leaders must treat cybersecurity as a core part of governance and risk management. The era of thinking "it won't happen to us" is over; as we've noted, it has already happened to some of us, and it could easily happen to you next.

There is a call to action here for every reader:

Take one step forward on the roadmap, today. Whether it's scheduling a meeting to draft an incident response plan, approving that MFA rollout, allocating budget for staff training, or simply educating yourself further—do it now. Each step reduces the odds of your organization becoming the next cautionary tale. Moreover, improving cybersecurity is not just a defensive act; it's an investment in the trust and confidence of your customers, constituents, and partners. Organizations known for good security are better positioned to thrive in the digital economy.

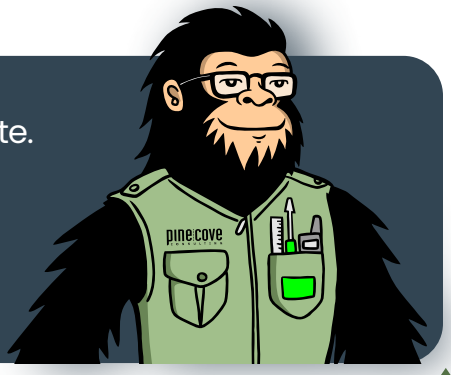
Montana's future in education, healthcare, finance, energy, agriculture, and beyond will increasingly be digital. With that opportunity comes the responsibility to safeguard the systems that underpin our way of life. We must rise to meet this challenge head-on, not with fear but with purpose and resolve. The good news is we are not starting from scratch; we have the knowledge, we have the roadmap, and we have each other as partners in this effort.

It's time for Montana to lead in cyber resilience. By taking the lessons in this report to heart and acting on them, we can turn Montana's reputation from a soft target to a shining example of how a community can come together to secure its digital destiny. The threats may be evolving, but so are we. All that remains is the commitment to act.

Regulatory Considerations: Montana organizations must also be aware of evolving compliance requirements. Montana's recent amendments to the Consumer Data Privacy Act significantly enhance compliance requirements, expand applicability, and remove previous grace periods, thereby increasing potential legal exposure for organizations failing to meet stringent data protection standards. This makes cybersecurity not just a business imperative, but a legal one as well.

If you need help, Pine Cove is here to support our home state.

For more information go to
www.pinecc.com
or call **(insert number we want to use)**



Appendix: Sources and References

1. IBM Security – Cost of a Data Breach Report 2024

Source: IBM & Ponemon Institute

Key data: $4.88M average global breach cost; $10.43M in the U.S.; 277-day average lifecycle

URL: https://www.ibm.com/reports/data-breach

2. CrowdStrike – Global Threat Report 2025

Key data: 48-minute average breakout time; 51-second fastest; surge in voice phishing and AI-driven social engineering

URL: https://www.crowdstrike.com/resources/reports/global-threat-report/

3. Sophos – State of Ransomware 2024

Survey of 5,000 IT/cybersecurity leaders in 14 countries

Key findings: 59% of organizations hit by ransomware; healthcare sector among the hardest hit

URL: https://www.sophos.com/en-us/content/state-of-ransomware

4. SonicWall – Cyber Threat Report 2025

Key findings: 259% rise in ransomware in LATAM; 8% in North America; 210,000+ new malware variants

URL: https://www.sonicwall.com/resources/white-papers/

5. SecurityWeek – Planned Parenthood of Montana Breach (2024)

Reported breach of 93GB of sensitive health data

URL: https://www.securityweek.com (search: Planned Parenthood Montana breach)

6. BankInfoSecurity – LoanDepot Breach Affects 49,000+ Montanans (2024)

URL: https://www.bankinfosecurity.com (search: LoanDepot Montana)

7. The Cyber Express – Montana State University Ransomware Attack (2023)

Hackers claimed 100GB data theft including student/faculty records

URL: https://cyberexpress.com (search: Montana State University ransomware)

8. BreachSense – Great Falls College MSU Royal Ransomware Incident (2023)

URL: https://www.breachsense.io (search: Great Falls College MSU ransomware)

9. Cobalt.io – Cybersecurity Statistics and Trends 2024

CISO survey data showing ransomware as top concern for 62% of leaders

URL: https://www.cobalt.io/blog/cybersecurity-statistics

10. Pine Cove Consulting – Interviews and Public Sector Assessments

Interviews conducted across Montana with IT leaders in public and private sectors

11. CISA, MS-ISAC – Threat Intelligence Alerts and Public Guidance

General threat advisories and toolkits used for continuous improvement practices

URL: https://www.cisa.gov, https://www.cisecurity.org/ms-isac

12. UnderDefense – Ransomware Trends 2024 (Coveware Data)

Trends in double and triple extortion ransomware tactics

URL: https://underdefense.com/blog/2024-ransomware-trends/

13. AGDAILY – Cyber Threats in Agriculture Sector (2024)

Coverage of ransomware incidents affecting food and ag supply chains

URL: https://www.agdaily.com

14. Bitdefender "Securing Education" Report (2024)

Analysis of educational sector vulnerabilities and Living-Off-the-Land attack techniques

Key insight: 84% of attacks involve LOTL techniques; education sector recovery periods of 2-9 months

Source: Tyler Baker, Director of Global Security Operations

15. Verizon Data Breach Investigations Report (DBIR) 2025

Key findings: Third-party breach involvement increased 15% to 30% year-over-year; ransomware accounts for 44% of breaches; increased exploitation of edge devices and VPNs

URL: https://www.verizon.com/business/resources/reports/dbir/

16. Marsh McLennan Agency Cybersecurity Best Practices Guide (2024)

Comprehensive recommendations for MFA implementation, EDR solutions, patch management, incident response planning, and secure financial practices

Focus on dual authorization and segregation of duties for wire transfers

17. Montana Consumer Data Privacy Act Amendments (2024)

Recent regulatory changes enhancing compliance requirements, expanding applicability, and removing grace periods

Increased legal exposure for organizations failing to meet data protection standards