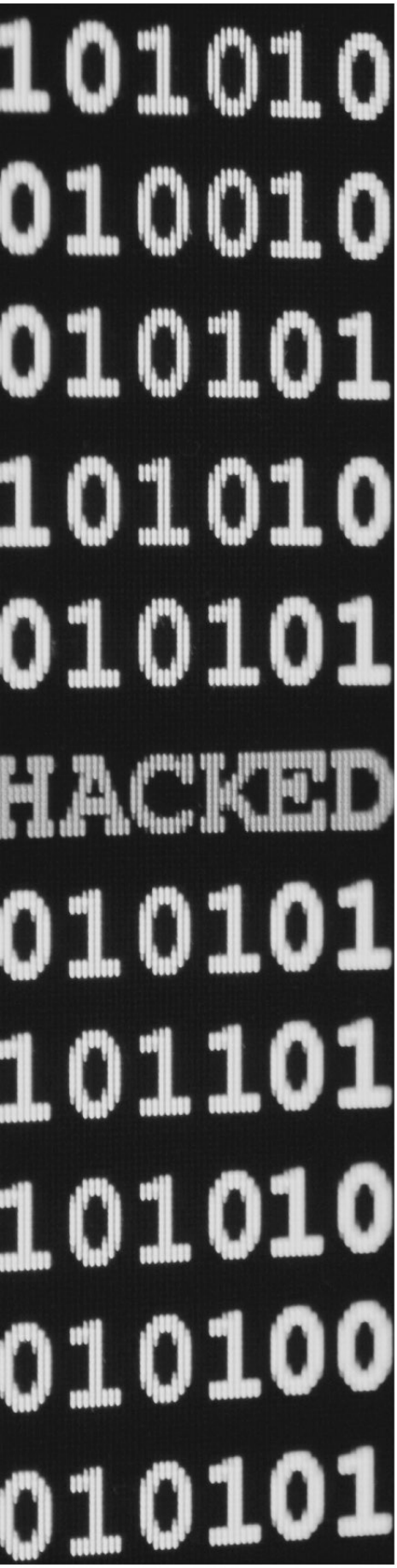
PAXIS
TECHNOLOGIES

THE CYBERSECURITY CRISIS

Provided as an educational service by:

Daniel Hale, President
Paxis Technologies
5430 Hilton Industrial Way
Knoxville, TN 37921
Phone: 865-588-9823
www.paxistech.com



SMALL & MEDIUM BUSINESS CYBERSECURTIY CRISIS

This report outlines essential protections every business must implement NOW to safeguard their bank accounts, client data, confidential information, and reputation from the rising tide of cybercrime and ransomware attacks.

Cybercriminals are becoming more advanced and relentless. **In 2023 alone, over 40% of cyberattacks targeted small and medium-sized businesses, with ransomware attacks costing businesses an average of $4.62 million per incident, according to the 2023 IBM Cost of a Data Breach report.**

Whether you run a large corporation or a small business, the risk is real, and your organization will be vulnerable unless you implement the strategies in this report. No company is too small to be a target, and waiting to take action is no longer an option.

WHEN A CYBERATTACK STRIKES, HOPE IS NOT A SUFICIENT STRATEGY

It feels incredibly unfair. Victims of traditional crimes, like burglary or theft, are met with sympathy and support. But when a business suffers a cyberattack that compromises client or patient data, the reaction is often very different. Instead of sympathy, you'll be seen as negligent. Questions will flood in—what did you do to prevent this? If your answers don't measure up, you could face fines, lawsuits, and irreparable damage to your reputation—even if you trusted a third-party IT company to protect your systems. Simply not knowing won't be an excuse, and the fallout will rest entirely on your shoulders.

But it doesn't stop there…

Federal laws require you to inform your clients that their data was exposed. Your competition will seize the opportunity, and your clients may lose trust and move on. Internally, morale can take a hit, with employees holding you responsible. To make matters worse, your bank isn't obligated to reimburse funds stolen by cybercriminals, and unless your insurance policy specifically covers cybercrime, you could be left without financial recourse.

Don't underestimate the risks. Assuming your IT company or person is taking all the right steps to protect your business is a gamble—one you can't afford to take. With your approval, we can quickly assess where your vulnerabilities lie.

WE'RE COMMITED TO PROTECTING BUSINESSES

My name is Daniel Hale, the proud President of Paxis Technologies. Since 1981, we've empowered businesses with tailored solutions that boost productivity and reduce risks. As the digital landscape and threats change, our strategy & model quickly adapt to protect our clients.

Our expertise spans cybersecurity, compliance, phone, and cloud services, all customized to meet the unique needs of each company. We begin with a thorough assessment of your technology infrastructure to identify vulnerabilities and inefficiencies. Our skilled engineers mitigate and resolve issues & are ready to address any challenges as they arise. Plus, as your business evolves, we provide ongoing assessments to ensure your systems remain secure and optimized.

In recent years, we've seen a sharp rise in businesses calling us after a ransomware attack or data breach. Often, by the time they reach out, their operations are paralyzed—data is encrypted or held for ransom, and years of work seem to vanish. They're left scrambling, frustrated, and concerned about how to notify clients whose data might have been exposed.

These attacks don't just affect large corporations—small and medium-sized businesses are also frequent targets. The truth is, cybercriminals are opportunistic, and businesses of all sizes have valuable data worth stealing. What's even more troubling is that most of the businesses we help had trusted an IT provider to safeguard their systems, only to find out too late that the protection was insufficient.
At our core, we believe in empowering business owners with the tools and knowledge to defend against cyber threats. We've made it our mission to help you avoid the stress, downtime, and financial loss that come with a cyberattack.

Don't wait until you become a target. Institute these practical steps you can take to safeguard your business—and schedule a free cybersecurity assessment to ensure you're protected.

YES, IT CAN HAPPEN TO YOU- AND THE RISKS ARE REAL

Cyber threats like ransomware and hackers are on the rise, and many businesses underestimate their vulnerability. If your IT provider hasn't discussed critical protections or a cyber disaster recovery plan with you, you might be at risk.

Don't think you're in danger because you're "small" and not a big company like Experian, J.P. Morgan, or Target? Think having "good" people and protections in place means it won't happen to you? That's exactly what cybercriminals are counting on. It makes you easy prey because you have no protections or inadequate ones.

Right now, there are over 980 million malware programs and counting (source: AV-Test Institute), with 70% of attacks targeting small businesses (source: National Cybersecurity Alliance). You rarely hear about these attacks because the news focuses on big breaches, and smaller companies often stay quiet out of fear, lawsuits, or embarrassment.

In fact, the National Cybersecurity Alliance reports that one in five small businesses were victims of cybercrime in the last year. And that only includes reported cases. Many small businesses are too embarrassed to report breaches, so the actual numbers are likely much higher.

Are you “too small” to be impacted by a ransomware attack that locks your files for days? Or by a hacker using your server to infect your clients, vendors, and employees? According to Osterman Research, the average ransomware demand is now $84,000 (source: MSSP Alert). Small businesses lose over $100,000 per ransomware incident, with 25+ hours of downtime.

When was the last time your IT company had this conversation with you? If not recently, it’s time to review this report and act.

WON’T MY INSURANCE COVER ME?

Relying on insurance alone is risky. Insurance companies are in the business of making money, not paying out claims.
A few years ago, cyber insurance providers kept 70% of premiums as profit, paying out only 30%. Today, those numbers have reversed, leading to stricter requirements for coverage and higher scrutiny during claims.

To even qualify for basic cyber-liability or crime insurance now, you may need to demonstrate that you have key security measures in place, like multi-factor authentication, password management, and endpoint protection. Some policies also require phishing and cybersecurity awareness training, a Written Information Security Plan (WISP), or a Business Continuity Plan. The list of required security protocols varies based on your situation and the coverage you're seeking.

The greatest risk comes when businesses overlook enforcing these security protocols. If a breach occurs, insurance companies will investigate whether your security measures were actually in place and followed. They can deny your claim if you failed to meet their requirements.

You can’t rely on your IT company to take responsibility either. They won’t guarantee your security or your compliance with insurance requirements. If you haven’t been documenting your security efforts and maintaining compliance, the financial burden will fall on you.

IT'S NOT JUST CYBERCRIMINALS YOU NEED TO WORRY ABOUT

While cybercriminals from overseas often steal the spotlight, internal threats are just as dangerous. Disgruntled employees and vendors can cause significant damage, exploiting their insider knowledge and access to sensitive data.

Employees may leave with your company's files, client data, or confidential information stored on personal devices. They may also retain access to cloud apps like Dropbox or OneDrive that your IT department may overlook. A study by Osterman Research found that 69% of businesses experience data loss due to employee turnover, with 87% of employees taking data when they leave. Some may sell the information to competitors, use it at their next job, or even start competing businesses.

Sneaky Ways Employees Steal—and It's More Common Than You Think
According to StatisticBrain, 75% of employees have stolen from their employers. This can range from inventory theft to check and credit card fraud, often happening in small increments that fly under the radar. But the most common way employees steal is by wasting hours of paid time on non-work-related activities—shopping online, browsing social media, or running personal errands. You might think you're paying for a full 40-hour week, but in reality, you could be getting far less while they push for more hires, claiming they're overworked.

If your IT company isn't monitoring employee activity, this behavior can also put you at risk legally. Employees might visit high-risk websites for gambling, adult content, or illegal downloads, increasing the chance of viruses and phishing scams entering your system.

Employees Can Delete Everything
Another all-too-common scenario occurs when a disgruntled employee quits or is fired—they might delete emails and critical files before leaving. Without proper backups, you could lose all that data, and even if you win a lawsuit, the legal fees, time, and effort to recover what's been lost can be far greater than any damages you might collect.

Whistleblowers Pose a Legal Risk
Employees can also become whistleblowers, reporting HIPAA violations or other non-compliance issues. Whistleblowers are often financially rewarded and protected by law. In fact, many complaints come not from actual cyber-attacks but from whistleblowers inside the organization—often disgruntled employees or clients.

With the rise of cybersecurity laws, whistleblowing is becoming more common. There are even websites like CorporateWhistleBlower.com, which encourages people to report fraud for rewards. Ambulance-chasing attorneys are capitalizing on this trend, offering to take on whistleblower cases, particularly in sectors like healthcare, where non-compliance with data protection laws can lead to serious consequences.

Vendor theft.
Third-party vendors like your payroll, HR, or accounting firms have direct access to sensitive information and the ability to commit fraud. It's not just their leadership team you need to worry about—anyone on their staff, including temporary or part-time employees, can exploit your data. For example, a seasonal data entry worker, often unsupervised and working remotely, could decide to steal money or sell your confidential information for extra income

THE REAL COSTS OF CYBERCRIME: HOW VULNERABLE IS YOUR BUSINESS?

1. Reputational Damages:
What's worse than a data breach? Trying to cover it up. Companies like Yahoo! learned this the hard way, facing class-action lawsuits for not informing users about their hacks right away. With dark web monitoring and forensics tools, breaches are easily traced back to the source, so hiding isn't an option.

When your data is compromised, will your clients have sympathy, or will they demand answers? Social media spreads news like wildfire, and if you have to admit that you didn't prioritize proper security, the fallout can be swift and unforgiving.

2. Government Fines, Legal Fees, Lawsuits:
Data breach laws are becoming increasingly strict. Multiple senators are pushing for "massive and mandatory" fines for breaches, and almost every state already has its own data breach notification requirements. Small businesses are not exempt—any company that collects customer information must comply.

Healthcare and financial sectors have even more stringent rules under HIPAA, SEC, and FINRA. For example, if a healthcare breach affects more than 500 clients, HIPAA requires notifying the media. Non-compliance comes with severe penalties. Has your IT provider helped you navigate these regulations?

3. Costs Piling Up:
One breach or ransomware attack can cause significant disruptions. There's business downtime, lost sales, and the overwhelming task of forensics to determine the extent of the damage. IT restoration efforts could be costly, and paying the ransom might be your only option for recovering data.

On top of that, legal fees and crisis management costs stack up as you work to reassure clients and handle media inquiries. Many states now require companies to offer credit monitoring to consumers impacted by a breach, and the average cost per record compromised is $225 (according to the Ponemon Institute). Multiply that by the number of clients and employees you have, and the potential costs skyrocket—especially for healthcare businesses, which see the highest breach costs.

4. Bank Fraud:
If hackers gain access to your bank account, don't expect your bank to cover the losses. Take the story of Verne Harnish, CEO of Gazelles, Inc., who had $400,000 stolen when hackers intercepted emails between him and his assistant. The hackers, posing as Harnish, convinced the assistant to wire money to various accounts. That money was never recovered, and the bank was not liable.

It's easy to think, "Not my assistant, not my employees," but the truth is, anyone can make a mistake. Just as you don't expect a car crash every day, you still wear a seatbelt. Ignorance or blaming your IT company won't protect you—you and your business will face the consequences.

5. Using You to Infect Your Clients:
Sometimes hackers don't steal your data or money—they use your systems to infect others. Your server or website could be hijacked to spread viruses, relay spam, run malware, or promote their agendas. Imagine the damage to your clients' trust if your systems are used to attack them.

This is why advanced security tools like endpoint security, spam filtering, and web gateway security are critical to protect your systems and your clients. Are you prepared for the consequences if you're not?

IS YOUR CYBERSECURITY UP TO DATE?

In today's digital landscape, cybersecurity threats are evolving rapidly. Consider these recent findings:

- The average cost of a data breach reached $4.45 million in 2023, up 15% over 3 years[1].
- 74% of breaches in 2023 involved human factors, including errors and social engineering[2].
- Global cybercrime costs are projected to reach $10.5 trillion annually by 2025[3].

Given these trends, it's crucial to ensure your IT provider is proactively addressing emerging threats. Ask yourself:

1. Has your IT company recently conducted a security audit?
2. Are they keeping you informed about new cybersecurity risks?
3. Have they proposed updated security measures?
4. Do they have specialized cybersecurity expertise?
5. Are they transparent about potential vulnerabilities?

Even well-intentioned IT professionals may struggle to keep pace with rapidly evolving threats. To ensure robust protection, consider seeking a second opinion from cybersecurity specialists.
Contact Paxis Technologies today for a free consultation to evaluate your IT infrastructure and ensure your cybersecurity measures meet current best practices.

[1] IBM Security. (2023). Cost of a Data Breach Report 2023. [2] Verizon. (2023). 2023 Data Breach Investigations Report. [3] Cybersecurity Ventures. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025.

EVALUATING YOUR IT PROVIDER'S CYBERSECURITY PRACTICES

To help you assess your current IT company's cybersecurity measures, we've prepared a comprehensive checklist.

Key points to remember when using the checklist:

- Thoroughness matters: A robust cybersecurity strategy should address all aspects of the checklist.
- Verification is crucial: For critical items, especially those involving insurance or compliance, request documentation.
- Stay informed: Regular updates and clear communication about your cybersecurity posture should be standard practice.

IT PROVIDER'S CYBERSECURITY CHECKLIST:

☐ **Regular Security Reviews and Risk Assessments**

- Quarterly comprehensive security reviews
- Annual risk assessments, especially for sensitive data handling
- Discussion of new security tools and technologies
- Reports on protective measures and emerging threats

☐ **Proactive Monitoring and Maintenance**

- Regular network monitoring and security updates
- Firewall log reviews and web-filtering technology
- Verification of maintenance activities

☐ **Advanced Security Measures**

- Multifactor authentication for sensitive data access
- Ransomware-proof backup system with regular testing
- Advanced endpoint security replacing traditional antivirus
- Email system configuration to prevent data leaks

☐ **Mobile and Remote Device Security**

- Written policy for mobile and remote devices
- Secure VPN for remote access (avoiding unsecure tools)

☐ **Employee Training and Policies**

- Regular cybersecurity awareness training
- Acceptable Use Policy (AUP) implementation
- Education on phishing and malware risks

IT PROVIDER'S CYBERSECURITY CHECKLIST (CONT.)

- [ ] **Data Protection and Monitoring**
  - Dark web/deep web ID monitoring
  - Data encryption on devices storing or processing critical data
  - Compliance with relevant data protection laws

- [ ] **Insurance and Liability Coverage**
  - Discussion of cyber insurance options
  - Review of current policy for compliance
  - Provider's professional liability insurance

- [ ] **Incident Response Planning**
  - Comprehensive incident response plan
  - Team briefings on cybersecurity incident procedures

- [ ] **Transparency in Service Delivery**
  - Disclosure of any outsourced services
  - Clarity on system and data access
  - Security controls for outsourced services

Remember, effective cybersecurity is an ongoing process that requires regular attention and updates. While these points are important, they represent a starting point rather than an exhaustive list. Every organization's needs may vary based on their specific risk profile and industry requirements.

We recommend discussing these points with your current IT provider to understand their approach to cybersecurity. If you're unsure about any aspects of your current protection, don't hesitate to seek a second opinion.

Contact Paxis Technologies today for a free, no-obligation consultation to evaluate your IT infrastructure and ensure your cybersecurity measures align with current best practices.

IMPORTANCE OF INDEPENDENT CYBERSECURITY RISK ASSESSMENTS

A thorough, independent cybersecurity risk assessment is crucial for ensuring your organization's digital safety. Here's why:

1. Comprehensive Evaluation
   - Reviews and stress-tests your entire network
   - Identifies potential vulnerabilities before they're exploited
   - Provides a detailed view of your current security posture

2. Early Detection and Prevention
    - Catches security issues while they're still manageable
    - Reduces potential costs associated with major breaches
    - Minimizes disruption to your business operations
3. Objective Third-Party Perspective
    - Brings fresh eyes to your cybersecurity setup
    - Offers unbiased insights, free from internal biases
    - Identifies blind spots that internal teams might miss
4. Actionable Insights
    - Delivers a confidential, comprehensive report
    - Provides a roadmap for improving your security measures
    - Helps prioritize cybersecurity investments
5. Compliance and Due Diligence
    - Demonstrates commitment to cybersecurity best practices
    - Helps meet regulatory requirements in various industries
    - Can be valuable for cyber insurance applications

Regular independent assessments complement your ongoing internal security efforts, providing an extra layer of assurance in an ever-evolving threat landscape.

PAXIS TECH'S FREE CYBERSECURITY RISK ASSESSMENT: GAIN CLARITY & CONFIDENCE

Paxis Technologies is offering a complimentary Cybersecurity Risk Assessment to select businesses. This service provides:

1. Expert Evaluation
    - Conducted by qualified third-party professionals
    - Comprehensive review of your current cybersecurity measures
    - Verification of your IT provider's security protocols

2. Minimal Time Investment
    - Initial meeting: 1 hour
    - Findings review: 1 hour

3. Non-Invasive Process
    - Confidential investigation of your network
    - Assessment of backups and security protocols
    - No disruption to your daily operations

4. Unbiased Insights
    - Detailed Report of Findings
    - Clear, actionable recommendations
    - Identification of potential vulnerabilities

5. Strict Confidentiality
    - All findings and discussions remain private
    - No obligation to pursue further services
    - Your current IT provider need not be involved

This assessment offers an opportunity to gain an independent perspective on your cybersecurity posture, helping you make informed decisions about your digital safety.

INSIGHTS YOU'LL GAIN FROM YOUR FREE CYBERSECURITY RISK ASSESSMENT

Our assessment will provide you with crucial information about your cybersecurity posture:

1. Dark Web Exposure
    - Scan for compromised login credentials
    - Confidential, on-site results review
2. Security Vulnerabilities
    - Evaluation of current IT systems and data protection
    - Identification of potential threats from external and internal sources
3. Backup Resilience
    - Assessment of backup systems against ransomware scenarios
    - Recommendations for robust, recoverable backup solutions
4. Employee Cybersecurity Awareness
    - Phishing email identification test for your team
    - Tailored training recommendations based on results
5. Compliance Alignment
    - Review of IT systems, backups, and security posture
    - Evaluation against HIPAA, GLBA, SOX, NIST, CIS standards, and industry best practices
6. Actionable Remediation Plan
    - Detailed report of findings
    - Proposed solutions for any identified issues

Our Commitment to You

- Strict confidentiality of all discoveries and discussions
- No-obligation, pressure-free assessment
- Expertise-driven, fact-based insights

OUR SKILLED TEAM IS READY TO CONDUCT YOUR FREE CYBERSECURITY RISK ASSESSMENT

This assessment offers you an opportunity to gain an independent perspective on your cybersecurity posture, helping you make informed decisions about your digital safety.

At Paxis Technologies, we aim to:

- Demonstrate our expertise and earn your trust
- Provide valuable insights without obligation
- Offer a path to improved cybersecurity, should you choose to proceed

We understand past experiences may have left you skeptical. That's why we offer this risk-free opportunity to experience our approach firsthand. Our goal is to provide you with the information you need to make informed decisions about your IT security.

To schedule your free Cybersecurity Risk Assessment, contact Paxis Technologies today at (865) 588-9823 or www.paxistech.com.