



## **Rethink Risk**

The Shared Responsibility  
of Building Resilience

 **EXIGENT**

# Rethink Risk

## The Shared Responsibility of Building Resilience

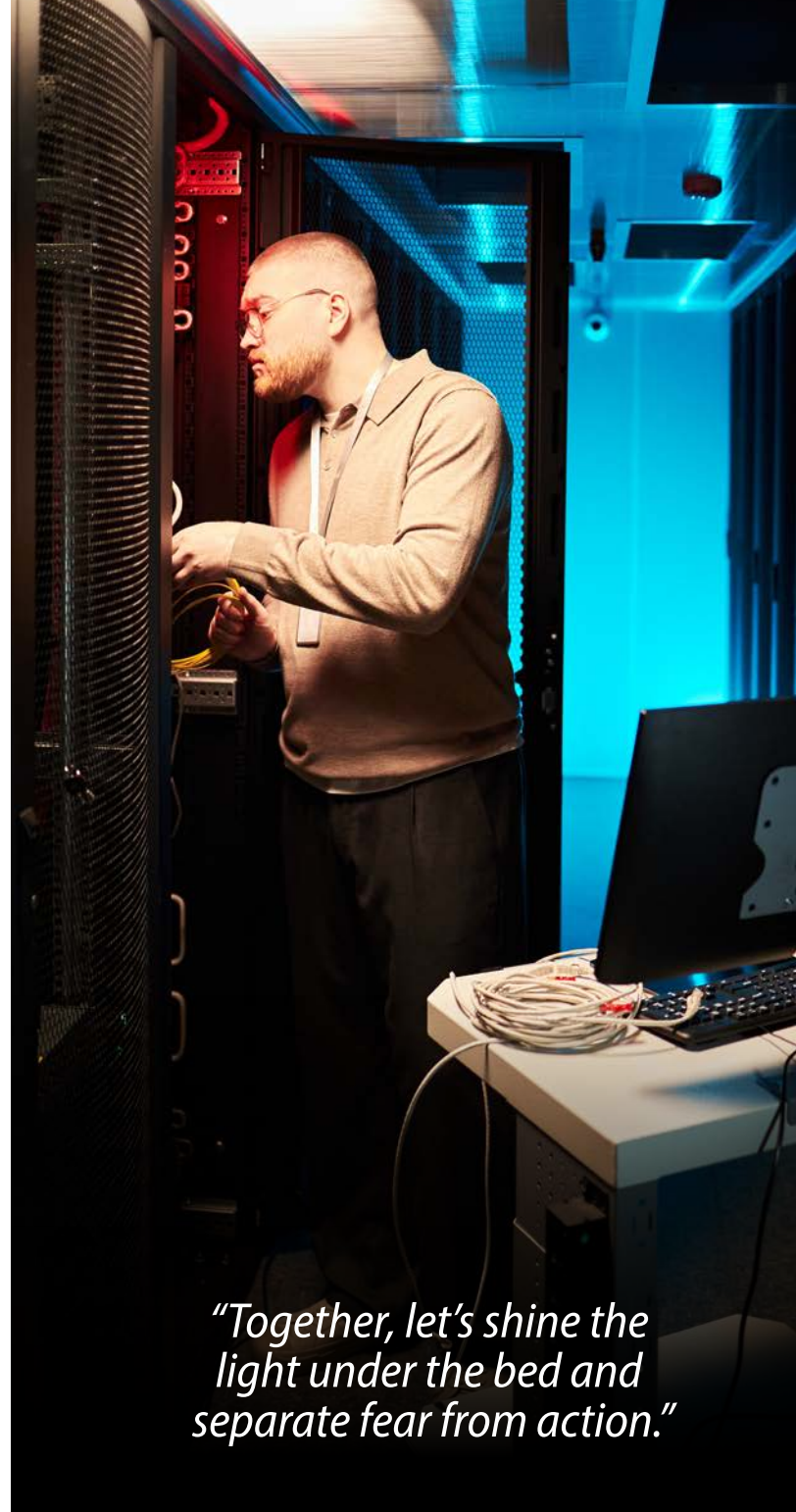
### Keep the Real Monsters at Bay.

When we were kids, the scariest threats were the ones we couldn't see. Monsters under the bed. Shadows in the closet. Every creak of the floorboard felt like the start of something terrifying. Of course, most of those fears turned out to be just that—fears.

Cybersecurity often feels the same way. The headlines scream, the statistics loom, and suddenly the “monster” of cyber risk seems impossibly big. While some of the headlines are hype, many of those “monsters” are real. Ransomware. Phishing attacks. Data theft. They thrive in the dark, and they target businesses of every size.

But much like childhood fears, the answer isn't panic — it's preparation. At Exigent, we believe cybersecurity is a team sport. With the right strategy, the right technology, and the right partners, you don't just manage risk — you control it. The Exigent Method focuses on collaboration and long-term protection, so your business can move forward with confidence.

**Together, let's shine the light under the bed and separate fear from action.**



*“Together, let's shine the light under the bed and separate fear from action.”*



### Be Wary of the Monster Online

It can be difficult to separate facts from the fear-mongering headlines, but that doesn't mean the facts aren't scary. According to **ConnectWise**:

- *43% of cyberattacks target small to mid-sized businesses (SMBs)*
- *75% of SMBs have experienced at least one **cyberattack in the last year***
- *60% of SMBs **go out of business** within six months of a cyberattack*
- ***Business email compromise attacks (BEC)** are steadily increasing, often enhanced by AI*

Those numbers are fueled by several factors:

- *A lack of formal security policies*
- *Missing, outdated, or ineffective security solutions*
- *SMBs underestimating the complexity, speed, and scale of threats*
- *Limited resources, both financial and expertise*
- *Artificial intelligence, which adds context and speed to attack creation*

All of this has increased urgency as managed services providers (MSPs) work to educate and support SMBs, ensuring their data, employees, customers, and businesses are protected. Gone are the days when traditional security was enough. Today, disparate cybersecurity solutions, unmanaged (or forgotten tools), and obsolete products will leave your business vulnerable.

An aggressive and complex threat landscape, fueled by artificial intelligence (AI) and sophisticated technology, takes a fully integrated approach, with real, live people involved. While AI provides advantages on both sides, the bottom line is that more than 90% of breaches involve human error. And you can't solve human error without educating and engaging your employees.

When you pair an experienced, engaged MSP with an educated workforce, the impact can be immeasurable—after all, how much is your business and reputation really worth?

It's time to renew focus on a consultative, integrated, and layered approach to security that is built on a philosophy of shared responsibility—the only viable path to true cyber resiliency.

Malware attacks have increased overall, with a notable **92% spike** in May 2024 alone

### Cybersecurity 2025 *A Layered and Integrated Defense in Depth*



#### 4 Security Wins You Can Implement This Month

- Turn on MFA across all accounts.
- Patch and update systems promptly.
- Decommission outdated technology.
- Schedule a phishing simulation and training session.

These simple actions close major gaps immediately — but only if leadership prioritizes them and employees follow through.

There is no silver bullet for cybersecurity. Modern attackers use layered, sophisticated tactics — ransomware that locks systems in minutes, AI-powered phishing, insider threats — and defending against them requires a layered, integrated defense-in-depth strategy.

Think of your IT environment like a hotel, not a house. There aren't one or two doors; there are countless entry points. Defense in depth ensures that even if one defense layer fails and leaves a door unguarded, other layers stand in the way and keep the monsters out.

Key layers include:

- **Perimeter defenses:** *firewalls, intrusion detection, secure remote access.*
- **Endpoint protection:** *antivirus, EDR, and device management*
- **Network security:** *segmentation, encryption, and secure application use.*
- **Data protection:** *backups, encryption, and access controls.*
- **The human layer:** *employee training, phishing simulations, and leadership buy-in.*

This approach isn't about stacking tools — it's about integrating people, process, and technology so each reinforces the others. That requires a shared responsibility mindset where your MSP designs and manages the layered strategy, but your team must implement policies, drive employee engagement, and model security-first behaviors.

### Helpful Hints

#### Glossary of Modern Cybersecurity Solutions

Even those businesses that operate in technology can be overwhelmed by the ever-changing jargon and never-ending list of acronyms. We've tried to gather the most common cybersecurity terms to help clear up some of the confusion.

- **CASB (Cloud Access Security Broker)** – A security checkpoint between cloud service users and providers, enforcing enterprise security policies.
- **Dark Web** – The hidden part of the internet often used by cybercriminals to buy, sell, and exchange stolen data.
- **Deep fakes** – Highly realistic manipulated videos and audio often created with AI
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)** – Email authentication protocol to prevent spoofing and phishing.
- **EDR (Endpoint Detection and Response)** – Detects and responds to threats at endpoint devices such as laptops or servers.
- **Firewall** – A network security device that monitors and controls incoming and outgoing traffic based on security rules. Often offered as-a-service by MSPs.
- **IAM (Identity and Access Management)** – A framework for ensuring only authorized users have access to critical systems and data.
- **Malware** – Software that is designed to cause damage to a computer. It can be destructive, or it can be used simply for information gathering
- **MDR (Managed Detection and Response)** – A proactive security service offering continuous threat monitoring and rapid response from a Security Operations Center (SOC).
- **Multifactor Authentication (MFA)** – Requires two or more forms of identity verification (e.g., password and mobile code) to access systems.
- **Phishing** – A cyberattack where attackers impersonate a trusted source (via email or text) to trick victims into revealing sensitive data.
- **Physical security** – Don't overlook the impact of leaving devices unlocked or passwords written down; breaches can also be physical attacks in public places.
- **Ransomware** – A type of malicious software that encrypts a victim's files and demands payment for the decryption key.
- **SAT (Security Awareness Training)** – Education that equips employees to identify and respond to cybersecurity threats, especially phishing.
- **Security Operations Center (SOC)** – A centralized team that continuously monitors, detects, and responds to cybersecurity incidents.
- **Shadow IT** – Download and use of apps for business purposes without the approval or knowledge of IT administrators.
- **SIEM (Security Information and Event Management)** – Collects, analyzes, and correlates security data from various sources for real-time threat detection.
- **Smishing** – Text version of phishing.



# Rethink Risk

## The Shared Responsibility of Building Resilience

- **Social engineered attacks** – Use knowledge of human psychology to convince others to give up sensitive and confidential information or perform tasks they otherwise would not do.
- **Spyware** – Software that tracks the user's activity and sends the information to another computer without their knowledge
- **Tailgating** – Physical access challenges where people hover behind employees to steal access codes and slip through protective doors.
- **Vishing** – Voice phishing; a scam where attackers call the victim while pretending to represent a legitimate organization.
- **XDR (Extended Detection and Response)** – Integrates data across endpoints, networks, cloud, and applications for holistic threat detection.
- **Zero Trust Network Access (ZTNA)** – A security model that assumes no implicit trust, requiring verification for every access attempt—internal or external.



# Rethink Risk

## The Shared Responsibility of Building Resilience

### What You Should Expect from Managed Services and Cybersecurity

Outsourcing IT doesn't mean outsourcing responsibility — particularly when it comes to cybersecurity. Managed services agreements typically include foundational tools such as patching, backups, and antivirus, but resilience requires much more.

At Exigent, we've found that the most effective relationships are rooted in a shared responsibility model, where MSPs provide the technical foundation and guidance, while business leaders and employees engage with policies, training, and prioritization. Let's remember: Your MSP isn't a cybersecurity silver bullet; it is your expert partner and advisor.

A strong MSP relationship begins with asking the right questions. At Exigent, we follow a proven process called **The Exigent Method** that is built on detailed onboarding processes and regular business reviews that help both sides align on expectations, share key information, and adapt to changing environments, threats, and business needs.

For example, our team starts partnerships with a series of discovery questions:

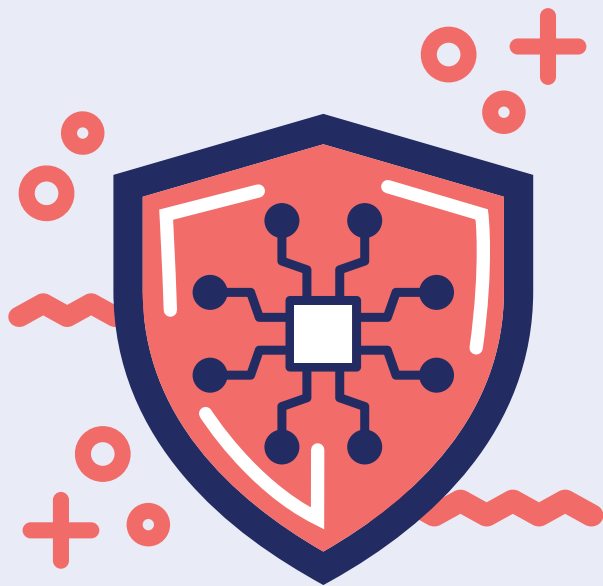
- *What are your compliance requirements?*
- *How much downtime is acceptable?*
- *Do you have written cybersecurity policies?*
- *How do you manage access and offboarding?*
- *Do you have security training?*
- *How do you handle access control (digital and physical)?*

These baseline discussions uncover hidden risks and help shape a roadmap for your unique environment.

**Responsibility Check:** Do you review your cybersecurity roadmap with your MSP regularly?



### The Crucial Role of Security Policies



#### Top Policies Every SMB Needs

1. Acceptable Use
2. Data Management/Classification
3. Password Management
4. Access Control (least privilege)
5. Incident Response
6. Business Continuity

Your MSP can guide and enforce — but ownership lives with your leadership team.

Cybersecurity tools are essential to safeguarding your organization, but they must be paired with leadership prioritization and employee engagement. That means an executive-level commitment to building a security-first culture. One critical step for any organization working toward improving its security posture is the creation and maintenance of written policies for acceptable use, data classification, and incident response; regular training and phishing simulations; and more.

Too often, companies draft policies but don't update them regularly, or they fail to communicate the importance of those documents. Why are security policies so important to your organization? First, most cyber attacks take advantage of simple vulnerabilities, such as a lack of MFA or unsecured devices, such as personal laptops used for BYOD. Second, holding your team accountable isn't possible unless the rules of the game are clearly documented. By regularly reviewing your policies and making sure you communicate the rules and reasons for the documentation across your organization, you can often improve your cybersecurity stance without spending a dime.

While some MSPs may draft policies as an add-on service to their clients, most offer guidance, templates, and best practices to guide internal creation. Writing or revising business policies can be overwhelming, but we've found that starting with documentation that touches the widest swatch of data or devices in your business is a good place to start. From there, phase 2 should address any unique, specific needs that you may have with policies that may play less of a role in protecting your organization from bad actors but are essential, nonetheless. Last, phase 3 should include a review of your incident response plan and cyber insurance policies to make sure you are prepared in case a cyber attack does happen. Policies should be reviewed at least annually; more often if your business is expanding rapidly.



### Why Shared Responsibility is Non-Negotiable

Technology alone won't protect your business — people and culture are equally critical. Most breaches begin with human error, which makes cybersecurity awareness and employee engagement essential.

A cybersecurity culture starts with leadership. When executives model good habits, participate in training, and treat cybersecurity as a business value, employees follow suit. Policies and processes must support this culture: Password standards, device usage rules, incident reporting, and safe channels for employees to raise concerns. Rewarding positive behavior reinforces the idea that security is everyone's responsibility.

MSPs play a key role here as partners. Beyond technology deployment, your MSP should:

- Offer frameworks for policies.
- Deliver or recommend security awareness training.
- Support long-term resilience through regular business reviews and coaching.
- Educate you on developing threats, from check washing schemes to social engineering and more.

Together, leadership, employees, and MSPs create a culture where security is woven into daily operations. That's the true ROI of cybersecurity culture: reduced breaches, faster incident response, and greater trust with clients.

But the partnership around cybersecurity doesn't stop with just your organization and IT provider. Much of your data, your clients' information, and more can be accessed by other business partners. In fact, any business with your financial, employee, or confidential data should be scrutinized as a potential portal into your organization.

Before signing on the dotted line with a business partner, be sure to fully vet their cybersecurity culture and effectiveness. More than one devastating breach has started with an access point shared by a business partner, or data in transit to and from a business partner. Too often, we expect that reputable companies share a commitment to cybersecurity, and that misconception can lead to vulnerability.

Once again, your MSP should be able to provide guidance when it comes to cyber awareness and accountability across your entire organization—leadership, employees, clients, business partners—the full spectrum. Think of a security-first culture as aligning with the adage “it takes a village” when it comes to successfully protecting your business. That said, remember to designate internal owners for cybersecurity initiatives. Who is in charge of making sure policies are updated? Vetting business partners? Keeping security training on track?

**Exigent Insight:** Culture eats tech for breakfast. Without a security-first culture, even the best tools fall short.



**Pro Tip:** Cybersecurity is everyone's job — from the boardroom to the breakroom to your business partners. Does your leadership set the tone that cybersecurity is essential and everyone's responsibility?

## The Role of Your MSP As Your Cybersecurity Partner

Sharing the responsibility of cybersecurity isn't the same with each MSP, with each level of managed IT services, or even with the deployment of advanced cybersecurity tools. How do you know where the lines are and who is handling what responsibilities? Communication is critical to ensure your team and your MSP partner are aligned on what your business needs are, what tools are in place, and exactly who is responsible for what. For example, many MSPs offer email filtering, but setting specific parameters and policies for what is allowed in terms of whitelisting domains is often handled by the customer.

The best approach to this shared responsibility is to have clear, detailed conversations with supporting documentation to ensure both teams are clear on roles. Additionally, regular business reviews should include a dedicated segment on cybersecurity, current and future state, providing an opportunity for ongoing adjustments and clarity.

An MSP should play a significant role in policy guidance, compliance support, and disaster planning – but the bottom line is simple. MSPs are business partners and advisors, but we cannot force any partner to make the right decision. Our role is education and expertise – making sure decision makers fully understand the consequences – good and bad – of cybersecurity investments.



### Cyber Insurance Readiness Questions

- Does our policy cover ransomware payouts and downtime costs?
- What security measures (MFA, patching, training) are required for eligibility?
- Are third-party/vendor breaches covered?
- What exclusions apply to social engineering or phishing?

Cyber insurance is no substitute for resilience, but it can be the difference between recovery and closure.

# The Role of Your MSP As Your Cybersecurity Partner

As your managed IT services provider, Exigent protects the core of our clients' operations—but each organization has critical responsibilities that only they can fulfill. Here's a breakdown:

## What **EXIGENT** Secures and Manages

Area	Description
<b>Network Perimeter</b>	Firewall policy enforcement, VPN access controls, intrusion prevention (IPS), and geo-blocking.
<b>Endpoint Protection</b>	Managed antivirus/EDR/XDR agents, real-time alerts, and automated threat containment where supported.
<b>Patch Management</b>	Routine OS and third-party software patching for covered workstations and servers.
<b>Backup Management</b>	Monitoring, integrity testing, and successful execution of local and/or cloud backups.
<b>Email Security (if subscribed)</b>	Advanced spam filtering, impersonation protection, and malware scanning
<b>Security Monitoring (if MDR)</b>	24/7 detection, triage, and incident response through our managed detection and response platform.
<b>Policy Implementation</b>	Enforcement of MFA, conditional access policies, and device compliance rules—if client-approved.
<b>Documentation &amp; Reporting</b>	System configuration records, audit support, and evidence generation for compliance frameworks.



In 2024 alone, ransomware cost businesses an average of **\$4.91 million per incident** when you factor in downtime, data recovery, and ransom payments.



# The Role of Your MSP As Your Cybersecurity Partner (cont.)

## What You Must Own and Manage

Area	Description
<b>Cyber Insurance Coverage</b>	You must procure and manage a cyber liability insurance policy tailored to your risk profile.
<b>Employee Security Training</b>	Phishing simulations and regular training are essential.
<b>Executive Engagement</b>	Security culture must be prioritized by leadership to allocate budget and enforce governance.
<b>Internal Policy Enforcement</b>	Acceptable use policies, HR discipline for risky behavior, vendor onboarding/offboarding protocols.
<b>Decision-Making for Risk Acceptance</b>	We'll surface the risks—but only you can decide whether to mitigate, accept, or insure against them.
<b>Third-Party Tools and Shadow IT</b>	Exigent cannot secure systems or software outside of our scope or awareness. Full visibility is required.
<b>Physical Premises Security</b>	Locked server rooms, secured physical access, and surveillance systems are outside our scope.
<b>Client-Owned Compliance Requirements</b>	If you're in a regulated industry (HIPAA, CMMC, NYDFS), ultimate responsibility lies with you to ensure alignment.



Attacks utilizing encrypted traffic are also on the rise, **increasing by 93% globally** in 2024

# Rethink Risk

## The Shared Responsibility of Building Resilience

### Building a Culture of Cyber Resilience

Too often, cybersecurity relies on fear, uncertainty, and doubt. While scare tactics may get attention, they rarely drive lasting behavior change. Instead, they lead to fatigue, disengagement, and resentment.

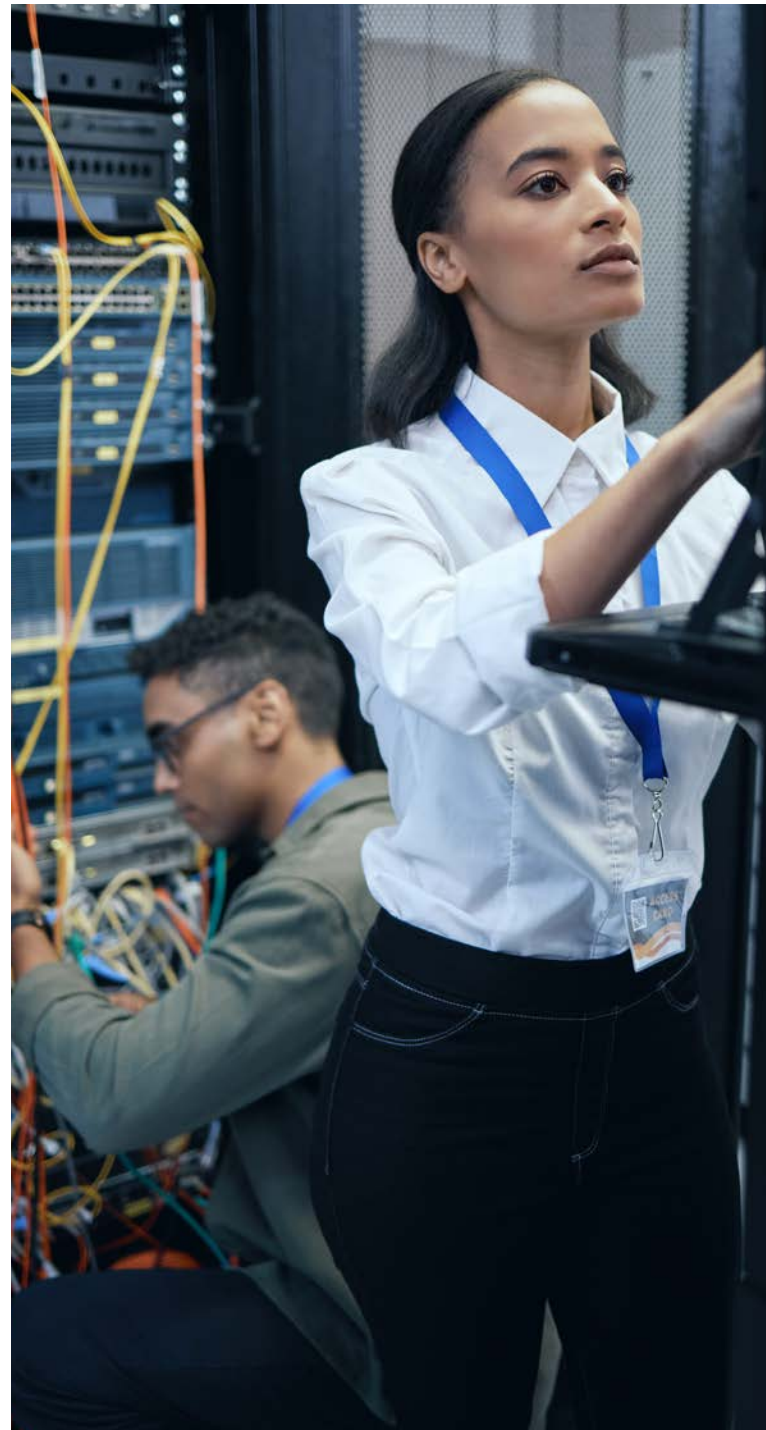
At Exigent, we believe effective training should be positive, personal, and ongoing:

- **Personalization:** *Training that reflects daily work tasks, not generic slide decks*
- **Positive reinforcement:** *Celebrating progress motivates employees far more than punishment.*
- **Humor and storytelling:** *Lighthearted enough to be engaging, serious enough to stick.*

When training is empowering rather than punitive, employees build confidence and actually look forward to participation. Over time, this approach leads to fewer phishing clicks, more proactive reporting, and measurable improvements in cybersecurity culture.



**Pro Tip:** Training must be continuous. Cyberthreats don't take a holiday, so programs like **Exigent's Vigilant Security** Awareness Training focus on reinforcement year-round, not one-off sessions.





## Rethink Risk

### The Shared Responsibility of Building Resilience

## Let's Protect What You've Built — Together

Remember those monsters under the bed? When we were kids, we would call for backup—our parents, siblings, the babysitter—and that team went hunting for those scary creatures lurking in the dark corners. Today, we do the same with cyber criminals. Together, your leadership, employees, business partners, and vendors can quickly turn that panic into power. By collaborating to share the responsibility of protecting your organization, you can better safeguard all you've invested in.

Remember:

- *Complete regular risk assessments and run quarterly vulnerability scans*
- *Engage with your MSP for periodic business reviews to ensure alignment and planning are on track*
- *Conduct annual incident response tests so you are confident in your ability to bounce back from any disruption*
- *Reinforce employee training with ongoing phishing simulations and other table-top exercises*


Shared responsibility is not a one-time project — it's a rhythm of continuous improvement.

## Appendix

**Cybersecurity Readiness Checklist**

**Incident Response Template**

**Cyber Insurance Questions for SMBs**



*"Together, your leadership, employees, business partners, and vendors can quickly turn that panic into power."*