



Cybersecurity Preparedness Program

A simple way to understand how prepared your business really is before attackers find out for you.

Developed by Cyber Command with over 10 years of experience in IT and cybersecurity, helping businesses identify vulnerabilities and strengthen their defenses.

[Get Your Cybersecurity Preparedness Rep...](#)

[Run a Free Public Exposure S...](#)

See What Attackers Can Already See

Before a cyberattack ever happens, attackers do their homework. They look for exposed credentials, leaked data, and publicly available signals that indicate weakness. Understanding your digital footprint is the first step toward protection.

Our free Public Exposure Scan checks whether your business data is already visible through known breach sources and exposure databases. This scan provides immediate insight into your organization's external vulnerability profile without touching your internal systems.

Run a free scan using any of the following:

-
- A business email address
- A first and last name (optional)



- ☐ No systems are accessed. No changes are made. This scan only checks publicly available exposure data, giving you peace of mind while providing valuable insights.

[Run Free Exposure Scan](#)

What This Is... and What It Isn't

This IS:

- A cybersecurity preparedness check
- A simulated fire drill for your existing security
- A clear, executive-ready report
- Vendor-neutral findings you can actually use

This IS NOT:

- A sales pitch
- A replacement for your IT team
- A compliance scare tactic
- A contract or obligation

We offer clarity, not fear. Our goal is to empower you with the knowledge needed to make informed decisions about your cybersecurity posture, without pressure or manipulation.

Why We're Doing This



Cybercrime doesn't just impact large corporations. It hits local businesses, schools, cities, and families – often without warning and without mercy. The financial and reputational damage can be devastating, especially for organizations without dedicated security teams.

After more than a decade in cybersecurity, we've seen a hard truth: **most organizations don't discover their gaps until something breaks.** By that time, the damage is done, recovery costs are high, and trust is shattered.

We believe staying silent about that would be irresponsible. So we built a way to share clarity without pressure, without fear, and without forcing change.

Because cybersecurity is a responsibility, not just a product.

What the Preparedness Fire Drill Tests

The Cybersecurity Preparedness Program includes a controlled, real-world fire drill designed to validate whether your existing security would actually hold up during an incident. Think of it as stress-testing your defenses before a real emergency strikes.



Access & Identity Readiness

Testing authentication controls, password policies, and multi-factor authentication implementation



Email and Phishing Exposure

Evaluating susceptibility to social engineering and malicious email attacks



Endpoint Visibility

Assessing monitoring and protection across workstations and devices



Network Exposure

Identifying vulnerabilities in network perimeter and internal segmentation



Backup and Recovery Viability

Validating backup integrity and testing restoration capabilities



Detection and Response Readiness

Measuring ability to identify, contain, and respond to active threats

This is not theoretical. It's a pressure test. We simulate real-world attack scenarios to see how your defenses actually perform under pressure.

What You Receive

Your Cybersecurity Preparedness Report

You'll receive a clear, plain-language report designed for leadership – not technicians. No confusing jargon, no overwhelming technical details, just actionable insights you can understand and use immediately.

Your comprehensive report includes:

- An overall preparedness rating that benchmarks your security posture
- What's working today and providing effective protection
- What would fail first in an actual attack scenario
- Estimated time-to-impact during a real incident
- Prioritized, vendor-neutral recommendations for improvement

You can share this report with your leadership team or your current IT provider. It's designed to facilitate informed conversations about security investments and priorities.

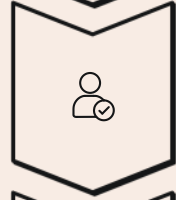


How It Works



Request Your Report

Submit your information through our secure form to begin the process



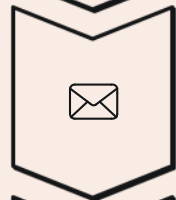
Confirm Participation

Verify your authorization via a secure opt-in link sent to your email



Fire Drill Conducted

Cyber Command performs the controlled preparedness assessment



Results Ready Notification

Receive an email titled: "Your Cybersecurity Preparedness Results Are Ready"



Schedule Review Call

Book a short 10-minute review to discuss key findings



Report Delivered

Your full detailed report is delivered after the review session

No pressure. No obligation. Just answers. The entire process is designed to be transparent, straightforward, and respectful of your time.

Safety & Responsibility

Controlled Testing


All testing is carefully controlled, fully authorized, and designed to validate your security posture – not disrupt your operations. Every test follows strict protocols to ensure business continuity.

No System Harm

No production systems are harmed during the assessment. No changes are made without explicit permission. Your business operations continue normally throughout the entire process.

Awareness, Not Guarantees

This process does not guarantee prevention of all attacks – it provides awareness of your current security posture and identifies areas for improvement. Knowledge is the foundation of better protection.

 **Your trust matters to us.** We take the responsibility of testing your security seriously and conduct every assessment with the highest standards of professionalism and care.

Real-World Impact: Why Preparedness Matters

The cybersecurity landscape has changed dramatically. Today's threats are more sophisticated, more frequent, and more costly than ever before. Understanding your preparedness isn't optional, it's essential for business survival.

\$4.45M

Average Data Breach Cost

The global average cost of a data breach in 2023, with small businesses often facing proportionally higher impacts

93%

Attacks Via Email

Of all cyberattacks begin with a phishing email, making email security a critical defense layer

60%

SMBs Close After Attack

Small-to-medium businesses that suffer a major cyberattack close within six months due to financial impact

277

Days to Identify Breach

Average time organizations take to identify a data breach, during which attackers have free access to systems

These statistics aren't meant to scare you, they're meant to inform you. **The organizations that fare best are those that prepare before an incident occurs.** That's exactly what our Cybersecurity Preparedness Program helps you achieve.

Ready to Understand Your Preparedness?



Taking the first step toward understanding your cybersecurity readiness doesn't have to be complicated or intimidating. Whether you choose our comprehensive Preparedness Report or start with the quick Public Exposure Scan, you're making a smart decision to protect your business.

Knowledge empowers action. Understanding where you stand today is the foundation for building stronger defenses tomorrow. Our team is ready to provide the clarity you need, without pressure or obligation.

Don't wait until an attack reveals your vulnerabilities.

Comprehensive Assessment

Get your full Cybersecurity Preparedness Report with detailed findings, executive summary, and actionable recommendations.

Perfect for: Organizations wanting a complete security evaluation

Quick Exposure Check

Run our free Public Exposure Scan to see what data about your business is already visible to potential attackers.

Perfect for: Getting immediate visibility into external exposure

[Request Your Cybersecurity Preparedness Report](#)

[Run the Free Public Exposure Scan](#)

Questions? Contact Cyber Command today to speak with a cybersecurity specialist who can help you choose the right option for your organization.