BLACK TALON SECURITY

“Helping You Build a Secure Business”

# Cybersecurity Solutions For Small and Medium Businesses

blacktalonsecurity.com | 800-683-3797 | Breach Response | Forensics | Preventative Cybersecurity

# Cyberattack Prevention

## How Can We Help and What Do We Do?

We are NOT an IT company or Managed Service Provider (MSP), but rather a group of highly trained and experienced cybersecurity experts who work in partnership with your IT company to identify risk in your organization that would enable a hacker to breach your network and gain access to (or encrypt) your data.

## Cybersecurity Training

Cybersecurity Awareness Training is a very powerful solution that helps mitigate the "employee risk factor." By properly training your employees on threats that present through the use of email and the internet, you can reduce your exposure by reducing the chances of an employee clicking on a malicious link, attachment or falling for a social engineering scam.

## Vulnerability Testing

Utilizing the most advanced technology, Black Talon Security places software on your network that actively tries to find and exploit vulnerabilities in your network, server and firewall. The software detects vulnerabilities such as: weak passwords, out of date operating systems/software and open ports on your network and firewall. There are approximately 20,000 known computer and device vulnerabilities and our software can find all of them, mitigating your risk.

## Penetration Testing / Ethical Hacking

Our ethical hackers will attack your firewall, server and network to find exploits that other technologies simply can't find. Once this is complete, a detailed report is provided to your IT company/MSP for remediation purposes.

## Cybersecurity Audit

We will conduct a comprehensive audit of your operations to help you better understand where you have risks such as backups, remote access, email, etc.

## Predictive Threat Intelligence Software

Imagine being able to identify, in real-time, the "unlocked doors and windows" on your network that hackers can use to break in and actually be able to close them prior to an attack. Our Predictive Threat Intelligence software does exactly that. Hackers exploit computers and networks by finding vulnerabilities and executing code that often provides them full access to your system or encrypts your data with ransomware. In addition, we receive live intelligence feeds from various agencies and organizations and this threat data is cross-referenced with our real-time vulnerability data to alert us of high-risk vulnerabilities on your network. Using this information, we can make a proactive call to your business and alert you. This solution is a total game-changer in the security world and allows you to be proactive instead of reactive to an attack.

# Cyberattack Recovery and Response

## Incident Response

The minutes, hours and days following a breach often determine the severity and the outcome of the breach. It is imperative that you work with a cybersecurity firm that truly understands all aspects of breach response. Many state and federal laws dictate how a breach must be handled. All evidence and data must be carefully preserved. Systems may need to be shut down and brought back online systematically in order to prevent further attacks or loss of data. Determining how the threat actors breached the system and analysis of forensics data are required to help the business fully understand their overall risk and proper course of action.

Upon notification of a breach, Black Talon Security can put "boots on the ground" to provide command and control of the situation. We will coordinate efforts between legal, IT and insurance companies...ultimately taking you through very controlled and thorough processes to help maximize the best outcome for the business.

## Ransomware Negotiation / Response

Ransomware and extortion are significant threats that businesses of all sizes may have to deal with. Black Talon Security has highly trained individuals who are experts in ransomware negotiations. Ransomware attacks typically encrypt some or all of your data, making it inaccessible until the attackers turn over a decryption key or tool. Prior to paying the ransom, we will work closely with you to ensure that all other recovery options have been exhausted. We use our various personas to negotiate with the threat actors, confirm that the files can be decrypted (proof of life) and make a payment using cryptocurrency. We will work with you to confirm that the decryption tool is functional and the files can be decrypted. Copies of all applicable files and malware will be maintained in the event that law enforcement becomes involved.

## Digital Forensics

Black Talon Security will carefully and methodically collect all the relevant data associated with the attack or crime. Collection of data will occur prior to making any changes to the network environment...helping to ensure a positive outcome. We will make sure that a proper chain of custody process is followed when data is collected or devices are acquired. Our forensics experts have years of experience working in this field and utilize some of the most advanced tools available to gather as much information as possible. Our experts have testified in numerous criminal and civil court cases over the years and their credentials/certifications position us as the “experts” during testimony. Comprehensive reports are also provided to the client.

Our propriety data collection tools, which can often be run after-hours, enable us to quickly and accurately collect data associated with the breach or crime.

## Why Black Talon Security?

Black Talon Security has been protecting small and medium businesses since 2017 and 100% of our operations are US based. Our customer-focused approach has enabled us to provide industry leading support and customized cybersecurity solutions designed for your specific industry and business' needs. We currently support over 10,000 devices across the US and have done penetration testing for 800+ businesses. We support businesses of all types including: financial institutions, accounting firms, healthcare providers, information technology businesses, managed services providers, insurance companies and agencies, manufacturing, etc. Our primary goal is to help harden your network and train your employees to prevent threat actors from gaining access to your network and data.

## The Biggest Mistakes You Can Make as an Owner or Executive of Your Business

Every business that contacts us for help with recovering from a cyberattack has two things in common. First, they relied on basic security solutions such as firewalls and anti-virus software. Second, they did not engage with a cybersecurity company to identify risk, harden their network and train their employees. They simply relied on their IT vendor to provide security. Your IT vendor should not be checking and auditing their own security work. It is very poor practice to "self-audit" security. The best IT companies and MSPs always recommend that their clients have an independent company check and verify their security. If your IT vendor pushes back, you should sit back and critically ask yourself, "Why would they say we don't need a cybersecurity company?".  They truly do not have your best interests in mind.

Remember this is **your data** and ultimately, **you are responsible** for protecting it. Call us today to learn how implementing a cybersecurity solution in your business can help mitigate the chances of you having to shut down your business operations or having your data stolen.