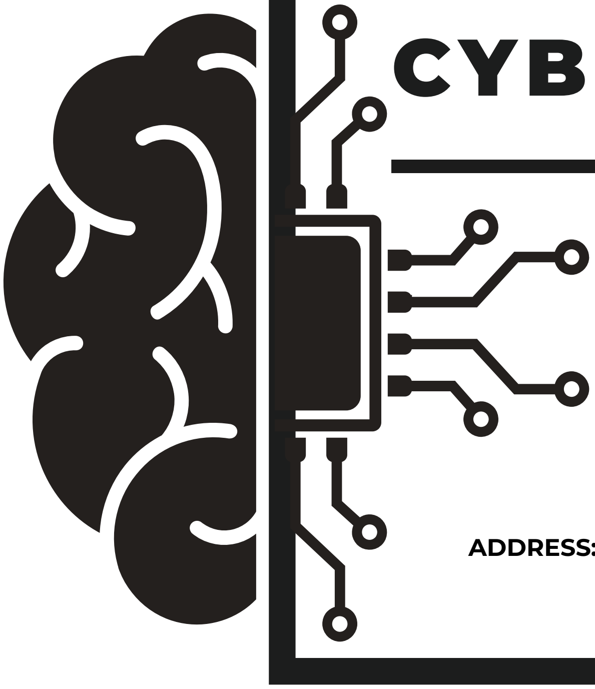
Superior
MANAGED IT

AI-FUELED CYBERCRIME



WHITE PAPER

Superior Managed IT
ADDRESS: 1306 County Rd F W, Arden Hills, MN
Phone: 612-999-6200
Web: www.SuperiorManagedIT.com

Table Of Contents

Unveiling the Surge:

AI-Fueled Cybercrime

Targeting Small Business Through Vulnerability Scanning & Trusted Communication Channels

Introduction

In today’s hyper-connected world, cybersecurity is critical for business success. In the current threat landscape, cybercrime is prevalent, and **everyone** is a target and should respond accordingly.

This makes it vital to secure enterprise infrastructure with robust cyber defenses. Businesses of all sizes are turning to the help of a managed security services provider (MSSP) to implement the latest strategies for cyber defense.

About Superior Managed IT

For over 30yrs, Superior Managed IT has been serving small to midsize businesses around the Twin Cities. We specialize in cybersecurity and compliance, cloud computing, data management, networking, sytems administration, infrastructure development, monitoring, and maintenance.

We're a local business who **emphasizes developing strong and lasting relationships**. As a result, you will get to know each member of our hard working Service Delivery Team as we help resolve all of your IT service requests and incidents in timely manner.

"IT can only be aligned when you have the right people, processes, and tools working together cohesively"

NICK HOULE
Managing Partner
& Co-Owner

Our team of both highly experienced technical and administrative professionals provide solutions and services across the entire IT life-cycle.

Superior Managed IT has a strategic network of partners with key players in a wide range of technologies. By drawing from a deep bench of industry-leading solution providers, we deliver targeted solutions driven solely by our customers' needs.

Whether you need Managed Services, Co-Managed Services, or Professional Services, our team will build the right plan for you to keep your business IT systems secure, functional, and optimized.

Executive Summary

The integration of artificial intelligence (AI) in cybercrime tactics has intensified the threat landscape, particularly for small businesses. This white paper delves into the alarming trend of cybercrime escalation facilitated by AI and highlights how small businesses, often lacking robust security measures, have become prime targets.

Moreover, it explores the emerging avenue of malware distribution through Microsoft Teams, a widely adopted collaboration platform, and offers actionable insights to mitigate these risks.

01. Small Businesses: Primary Target

Cybercrime has evolved into a sophisticated ecosystem driven by AI-powered tools and techniques, posing significant challenges for businesses of all sizes. Small businesses, in particular, are increasingly vulnerable due to limited resources and less stringent cybersecurity measures.

03. Microsoft Teams: An Unsuspecting Attack Vector

The widespread adoption of Microsoft Teams as a collaboration platform has inadvertently provided cybercriminals with a new vector for malware distribution. Through social engineering tactics and malicious file sharing, attackers exploit the trust of users to infiltrate organizations and spread malware.

02. Entry-Level Cybercriminals

AI technologies empower people from all walks of life to turn toward cybercrime to make ends meet. With AI, it's easier than ever to automate and optimize malicious activities, enabling them to scale operations and evade traditional security defenses.

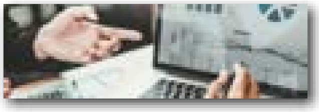
04. Mitigating Risks

To safeguard against the escalating threat of cybercrime, particularly via Microsoft Teams, small businesses must prioritize cybersecurity and adopt a multi-faceted approach to risk mitigation. By recognizing the heightened risks and implementing proactive measures, small business owners can be better positioned to

As of December 2023, the average cost of ransomware is $4.54 million, including both direct and indirect costs. Lesser cyber attacks cost small businesses $8,000 a year, on average.

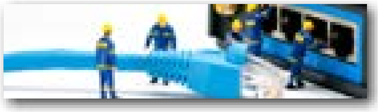
How Small Business became the #1 Target

Small businesses are particularly vulnerable to cybercrime due to several factors. Firstly, limited resources and budgets often result in inadequate investment in cybersecurity measures, leaving small businesses ill-equipped to defend against sophisticated cyber threats. Additionally, small businesses may lack dedicated IT staff or cybersecurity expertise, making them easy targets for cybercriminals seeking to exploit vulnerabilities in their networks and systems.



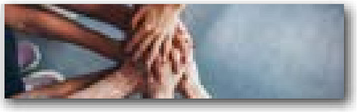
Limited Budget
and resources

Leaves small businesses Ill-equipped to defend themselves



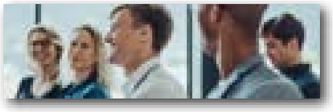
Lack Dedicated IT Staff
or cybersecurity expertise

Easy target for cybercriminals seeking to exploit vulnerabilities. SMBs that employee IT staff are limited to their knowledge.



Higher Level of Trust
among employees

Trust can be manipulated by cybercriminals through social engineering tactics by posing as trusted colleagues



Lack of Training
and awareness

users are most vulnerable to email phishing, fake invoice schemes, and wire fraud

Small businesses typically have a higher level of trust among employees and may have less stringent security protocols in place compared to larger enterprises.

This trust can be manipulated by cybercriminals through social engineering tactics, such as phishing emails or fraudulent phone calls, which exploit the interpersonal relationships within small business environments.

Additionally, the lack of employee training and awareness programs leaves small businesses susceptible to common tactics used by cybercriminals, such as email phishing scams or fake invoice schemes.

A Note on Reputation & Brand Damage

A cyberattack or data breach can have significant reputational and brand damage for small businesses, damagingcustomer trust and confidence in their products or services. Negative publicity resulting from security incidents can scare away potential customers and partners, leading to loss of revenue and market share.

Cybercrime is now entry-level

The integration of artificial intelligence (AI) into cybercrime tactics has democratized the creation and deployment of malware, **lowering the barrier to entry for less knowledgeable individuals to engage in illicit activities.**

AI-driven tools and techniques have automated and streamlined various aspects of malware development, enabling even novice attackers to create sophisticated and evasive threats with minimal technical expertise.

AI technologies empower cybercriminals to automate and optimize their malicious activities, enabling them to scale operations and evade traditional security defenses. AI enhances the efficacy and efficiency of cybercrime tactics, posing a grave threat to businesses worldwide. Cybercriminals leverage AI algorithms to analyze vast amounts of data, identify potential targets, and craft sophisticated attacks with greater precision and efficiency.

One alarming trend is the use of AI to easily manipulate scripts, allowing attackers to evade detection by traditional antivirus systems and other security controls.

Code Obfuscation and Evasion Techniques

AI-driven obfuscation techniques can conceal the true intent and functionality of malware, making it more challenging for security researchers and antivirus software to detect and

Automated Malware Generation:

AI-powered platforms and algorithms can automatically generate malware variants by analyzing existing samples and identifying patterns and characteristics associated with malicious code.

Marketplaces for Malware-as-a-Service

Underground marketplaces for MaaS offerings often include user-friendly interfaces and step-by-step guides, enabling even novice attackers to launch sophisticated cyberattacks with minimal effort.

KEY TAKEAWAY

AI-powered vulnerability scanning tools can identify and exploit weaknesses in software applications and systems, **enabling less knowledgeable attackers to deploy malware payloads through known exploits and vulnerabilities.**

By automating the discovery and exploitation of software flaws, AI facilitates the rapid deployment of malware without requiring deep technical expertise or programming skills.

2023 CYBER CRIME STATISTICS

40%

of Microsoft 365 tenants have had at least one unauthorized login attempt to gain access to the org's MS Teams platform

$12.5 B

880,418 complaints filed to the FBI's Internet Crime Complaint Center in 2023. Total losses from those complaints totaled $12.5 bil-

56%

The U.S. accounted for 56% of all ransomware attacks in 2023, and the UK was the second most targeted country, accounting for 5%

- Cybersixgill IQ
"State of the Underground Report 2024"

NEW MALICIOUS TRENDS TO LOOK OUT FOR:

MALVERTISING AND SEO POISONING

"Malvertising is a technique in which threat actors create malicious advertisements to facilitate criminal activity. Adversaries use SEO poisoning to falsely promote malicious websites to higher ranks in search engine results. Similar to malvertising, SEO poisoning relies on users believing the results closest to the top of a search result are the most credible.

Throughout 2023, adversaries such as LUNAR SPIDER regularly abused Google advertisements to ensure their malicious ads appeared at the top of search result pages. Threat actors such as SolarMarker operators regularly used SEO poisoning
throughout 2023."

-CROWDSTIKE 2024 GLOBAL THREAT REPORT

61% of hackers plan to use GenAI for hacking tools and to find more vulnerabilities.

GenAI started to become a cybersecurity concern in 2023 and it's likely to become a much bigger issue in 2024 and beyond.

GenAI is making phishing more dangerous by enabling attackers to more easily construct articulate lures to reel in potential victims.

The Cyber Kill Chain:

↘ *The 7 Steps of a Cyberattack*

The **Cyber Kill Chain** framework, developed by Lockheed Martin (2022), explains how attackers move through networks to identify vulnerabilities that they can then exploit. Attackers use the steps in the Cyber Kill Chain when conducting offensive operations in cyberspace against their targets. If you're responsible for defending a network, this model can help you understand the stages of a cyberattack and the measures you can take to prevent or intercept each step. The Cyber Kill Chain is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

Ref: EC-Council Cybersecurity Exchange

Step 1.
Reconnaissance

Before they start penetration testing, this first stage may include identifying potential targets, **finding their vulnerabilities**, **discovering which third parties are connected to them** (and what data they can access), and **exploring existing entry points as well as finding**

Step 2.
Weaponization

The attacker has discovered all necessary information and vulnerabilities about their target(s). Weaponization can include **creating new types of malware or modifying existing tools to use in a cyberattack**. For example, they may make minor modifications to an existing ransomware variant to create a new Cyber Kill Chain tool.

Step 3.
Delivery

Cyberweapons are used to infiltrate a target's network and reach users. These may involve **sending phishing emails containing malware attachments with subject lines that prompt users to click through**. Delivery can also take the form of hacking into an organization's network **and exploiting a hardware or software vulnerability to infiltrate it**.

Step 4.
Exploitation

In this process, cybercriminals often move laterally across a network to reach their targets. Exploitation can sometimes lead attackers to their targets **if those responsible for the network have not deployed deception measures.**

Step 5.
Installation

Attempts are made to install malware and other cyberweapons onto the target network to take control of its systems and exfiltrate valuable data. In this step, **cybercriminals may install cyberweapons and malware using Trojan horses, backdoors, or command-line interfaces.**

Step 6.
Command and Control (C2)

In the C2 stage, they start carrying out their objectives by **instructing the cyberweapon with the malware they've installed onto a target's network**. Attackers may use communication channels to direct computers infected with the Mirai botnet malware to overload a website with traffic or C2 servers to instruct computers to carry out commands.

Step 7.
Actions on Objectives

While cybercriminals' objectives vary depending on the type of cyberattack, some examples include weaponizing a **botnet to interrupt services with a Distributed Denial of Service (DDoS) attack**, **distributing malware to steal sensitive data from a target organization, and using ransomware as a cyber extortion tool.**

Risk Mitigation

To safeguard against the escalating threat of cybercrime, small businesses must prioritize cybersecurity and adopt a multi-faceted approach to risk mitigation. From CROWDSTRIKE's Global Threat Report 2024, the following are best-practice recommendations/key strategies for protecting your business in today's unforgiving digital environment.

MUST HAVE!

Identity Protection

Due to high success rates, identity-based and social engineering attacks surged in 2023. Stolen credentials grant adversaries swift access and control — an instant gateway to a breach. To counter these threats, it is essential to implement phishing-resistant multifactor authentication and extend it to legacy systems and protocols, educate teams on social engineering and implement technology that can detect and correlate threats across identity, endpoint and cloud environments.

Prioritize CNAPPs

Cloud-Native Application Protection Platforms (CNAPPs) integrate and centralize otherwise disparate security functions into a single user interface. The problem for many organizations is that responses to cloud native security have been reactive, rather than proactive – dealing with issues as one-off problems, rather than addressing cloud security more holistically. Cloud adoption is exploding as companies realize the potential for innovation and business agility that the cloud offers. Due to this growth, the cloud is rapidly becoming a major battleground for cyberattacks. Businesses need full cloud visibility, including into applications and APIs, to eliminate misconfigurations, vulnerabilities and other security threats.

Gain Visibility Across All Areas of Risk

Adversaries often use valid credentials to access cloud-facing victim environments and then use legitimate tools to execute their attack, making it difficult for defenders to differentiate between normal user activity and a breach. To identify this type of attack, you need to understand the relationship between identity, cloud, endpoint and data protection telemetry, which may be in separate systems. By consolidating into a unified security platform with AI capabilities, organizations have complete visibility in one place and can easily control their

Drive Efficiency:

Adversaries are getting faster - are you?

It takes adversaries an average of 62 minutes — and the fastest only 2 minutes — to move laterally from an initially compromised host to another host within the environment. It's challenging to keep up with that. Legacy SIEM solutions are now failing the SOC. They are too slow, complex and costly, and they were designed for an age when data volumes — and adversary speed and sophistication — were a fraction of what they are today. If you don't have an internal or outsourced SOC team, consider 24/7 managed detection and response (MDR).

Build a Cybersecurity Culture

Though technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses

The convergence of AI-driven cybercrime and the widespread adoption of collaboration platforms that can be easily exploited once an account has been compromised presents a formidable challenge for small businesses.

By recognizing the heightened risks and implementing proactive cybersecurity measures, small business owners can protect their organizations from malicious actors and safeguard against the growing threat of malware distribution and other cyber threats. Together, we can fortify the defenses of small businesses and preserve the integrity of the digital ecosystem.

Choosing the Right Partner

Before reaching out to a provider, it's important to understand your own organization's core values first and foremost and know what a healthy partnership means for you. This criteria varies widely from one business to the next, including the providers you evaluate. Think of this process like you were hiring for a senior-level position. You likely wouldn't hire an employee that wasn't thoroughly qualified, verified, and had no understanding of your industry. Once a business decides on their managed service provider, they should emanate both expertise and experience.

Top 4 Reasons Why Businesses Decide to Outsource Their IT or Change Providers

1. GROWTH

They feel like their existing staff or provider cannot accommodate their growing business, and it would be costly to hire additional full-time staff.

2. COMPLEXITY

With the number of disciplines that encompass IT, the time and expense of continuous training for internal staff doesn't make sense.

3. POOR SERVICE

Their existing service provider is not a good fit due to response or resolution time, or customer service is deficient.

4. STAFF RETENTION

Turnover and retirement IT employees accept another position, or have reached retirement age.

Top Trends for MSPs in 2024

Whether your IT is internal, fully managed by a 3rd Party or partially managed under a Co-Managed arrangement, you'll want to **ensure that team is staying ahead of the rapidly-evolving curve**. A team or provider that is focusing on the following IT competencies will not just boost their internal operational efficiency to better serve you/their clients, but will also give you an advantage over your competition by applying these important strategies to your business.

Your IT Team MUST be Committed to:

1

CYBERSECURITY

With 102,000 ransomware attacks per day last year, cybersecurity MUST be a top priority for IT providers to protect themselves and their clients.

2

AUTOMATION

With a storm brewing in the macroeconomic climate, businesses of all sizes will be asked to do more with less. Adopting automation can be the difference between thriving and surviving in 2024.

3

INTEGRATION

Slow, fragmented IT tools are no longer viable. IT providers need integrated solutions for efficiency & agility. Integrations are key for automation.

4

AI EXPERIMENTATION

While the effects of the AI revolution haven't been fully felt yet, smart IT providers are preparing now by rolling up their sleeves and diving into AI and building runbooks.

Source: Kaseya's Global MSP Benchmark Survey: Trends and Forecasts

Case Studies

A preview of Superior Managed IT’s proactive & reactive cybersecurity strategies

Microsoft 365 GCC High:
A Transition from Hybrid Exchange for Enhanced Security & Compliance

Discover how we guided a government contractor through transitioning to Microsoft 365 GCC High, enhancing their security compliance and ensuring robust data protection in alignment with strict government regulations.

View Online

Wire Fraud:
Strategic Response to an Advanced Business Email Account Takeover

This case study illustrates the essential role of rapid and coordinated responses in managing sophisticated cyber threats.

By immediately halting compromised communications and shifting to verified channels, the client mitigated immediate risks and implemented strategic long-term security enhancements.

View Online

THANK YOU

Superior Managed IT

ADDRESS: 1306 County Rd F W

Phone: 612-217-7030 **Web:** www.SuperiorManagedIT.com