USX CYBER

2022 CYBERSECURITY READINESS REPORT

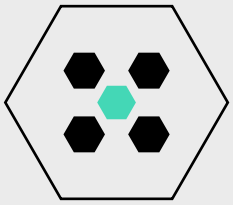
Analyzing the threats and preparedness among small business owners

INTRODUCTION

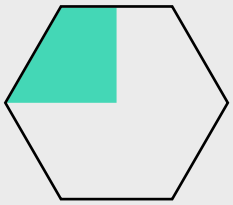
It's no secret the cybersecurity landscape is continuously evolving with sophisticated new threats, hackers, and vulnerabilities emerging daily. As company leaders shoulder the responsibility of running a small business, protecting company data – and the data of its customers – can be a daunting task. Furthermore, cybersecurity knowledge is rarely part of a small to medium-sized (SMB) company CEO's skill set. In contrast, most large businesses and organizations make cybersecurity an integral part of operations, with enterprise-level platforms and cyber professionals on staff. But as cyber attacks now impact organizations of all sizes, successful leaders must navigate the process of enlisting the right security solutions to protect their businesses and fit their needs.

USX Cyber's Readiness Report consolidates the insights from leaders at 615 SMBs regarding their current level of preparedness and experience dealing with the critical matter of cybersecurity.

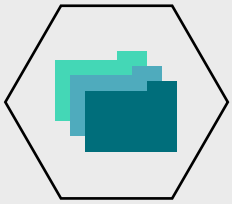
KEY TAKEAWAYS



1 IN 5 BUSINESSES SHOW LITTLE TO NO CONCERN ABOUT CYBERSECURITY EVEN THOUGH 30% OF BUSINESSES HAVE EXPERIENCED AN ATTACK IN THE PAST 12 MONTHS



A QUARTER OF BUSINESSES THAT EXPERIENCED AN ATTACK REPORTED A SEVERE HALT TO BUSINESS OPERATIONS



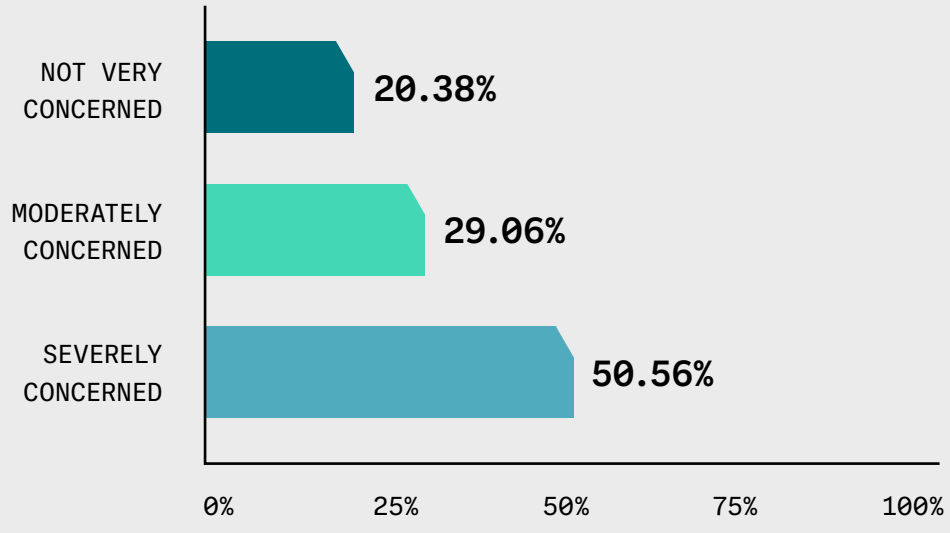
INDUSTRIES WHERE CONSUMER DATA IS MOST IMPORTANT WERE ALSO LEAST LIKELY TO HAVE A PLAN IN PLACE

A LACK OF CONCERN IS CONCERNING.

Of the individuals who participated in USX Cyber's Readiness Report, 94% expressed some level of concern about cybersecurity, with nearly 80% noting they were moderately to severely concerned. However, one-fifth of respondents had very little to no concern about the cybersecurity of their businesses. This lack of concern is an open door to a direct threat or attack, leaving their staff, customers, and clients vulnerable to loss of data, compromised financial information, or worse. In fact, 60% of small businesses close down after suffering a cyberattack.

According to a recent pentesting project, in 93% of cases an external attacker with intent can breach an organization's network perimeter and gain access to local network resources in a couple of days. This alone makes a compelling case as to why investments in these preventative measures should be made by anyone dealing with sensitive or personal data. As the stat above outlines, breaches like these can be fatal to a business.

Q: TO WHAT EXTENT ARE YOU CONCERNED OR WORRIED ABOUT WHETHER YOUR COMPANY HAS APPROPRIATE CYBERSECURITY DEFENSES?



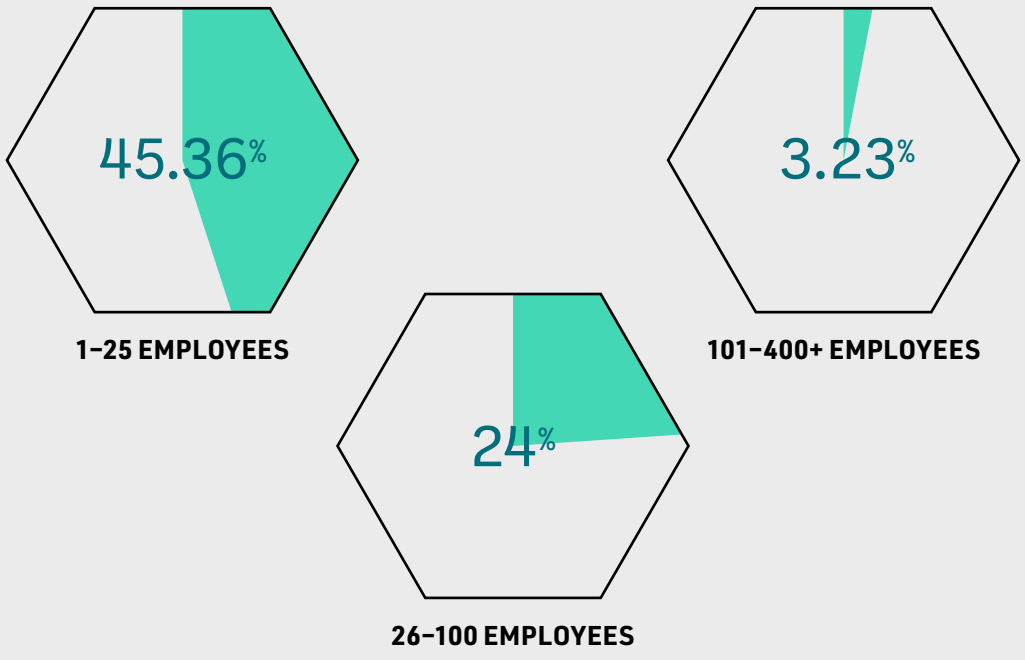
SOURCE: 2022 Survey of 265 business leaders

SMALL BUSINESS, BIG TARGET.

Despite the fact that businesses suffered 50% more cyber attack attempts per week in 2021 than in 2020, 28% of respondents answered "no" or "not sure" when asked if they had a cybersecurity plan in place. Reasons why SMBs often forgo cybersecurity protection ranged anywhere from thinking they are too small to be a target to using legacy IT systems that might not support the necessary new software.

Small businesses make up 43% of cyber attacks each year, yet these businesses are also the least likely to have a cybersecurity plan in place. Unfortunately, unpreparedness can be a grave mistake. A recent study showed that 60% of all small businesses suffering a data breach permanently close their doors within six months of the attack.

MICROBUSINESSES ARE LEAST LIKELY TO HAVE A CYBERSECURITY PLAN IN PLACE



SOURCE: 2022 Survey of 265 business leaders

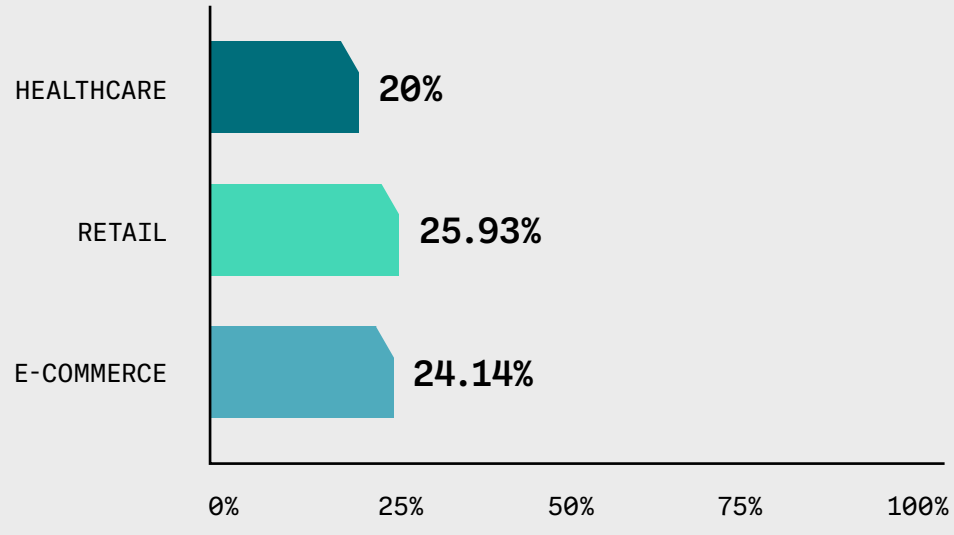
HAVING CUSTOMER DATA DEMANDS HAVING A PLAN.

No business is off-limits when it comes to cyber threats, and neither is any industry. While 72% of respondents claimed to have a cybersecurity plan in place, of the 28% who don't, Healthcare, Retail, and E-Commerce represented the most vulnerable sectors. Because so many businesses already operate digitally, even more so since the pandemic began, the general assumption is consumer data is safe. However, the facts tell a starkly different story. Less than two years ago, the Marriott hotel chain disclosed a security breach that impacted the data of more than 5.2 million users of Marriott's loyalty application, and then Marriott suffered another breach in 2022. The presumption of safety is unfounded, even with enterprise-level security that has not been properly updated.

> **Protecting your customers' data is a mandatory element of running a business – just like having internet, or email. Not having a cybersecurity plan in place can directly impact the trust and loyalty you build with your customers.**

– Clyde Goldbach, Founder of USX Cyber

TOP INDUSTRIES WITHOUT A PLAN IN PLACE



SOURCE: 2022 Survey of 265 business leaders

EARLY DETECTION IS KEY.

Of those surveyed in the Readiness Report, 29.81% admitted to experiencing a cyber attack in the past 12 months. However, the challenge for many SMBs is that without a robust cybersecurity monitoring system, these attacks go virtually undetected unless they cause a noticeable disruption.

The most common form of cyber attack reported was caused by unencrypted passwords (34%), followed by ransomware (30%) that required payment. Seventy percent of respondents who suffered an attack experienced either a temporary or severe disruption to their business. Financially speaking, some predict that ransomware will cost its victims somewhere around $265 billion (USD) annually by 2031.

Q: WHAT FORM DID THE CYBER ATTACKS TAKE?

34.15%	ACCESSING UNENCRYPTED PASSWORDS
30.49%	RANSOMWARE
28.05%	TROJAN VIRUS
26.83%	PHISHING CAMPAIGN
25.61%	DISTRIBUTED DENIAL-OF-SERVICE (DDoS) ATTACK
24.39%	MALWARE VIRUS
21.95%	MALWARE WORMS
21.95%	MALWARE SPYWARE
21.95%	MAN-IN-THE-MIDDLE ATTACK
21.95%	SQL INJECTIONS
21.95%	INTERNET OF THINGS (IoT) ATTACK
20.73%	REMOTE CONTROL VIA INSECURE DOWNLOADS, EMAILS
17.07%	ZERO-DAY EXPLOIT
17.07%	CROSS-SITE SCRIPTING
3.66%	I DON'T KNOW

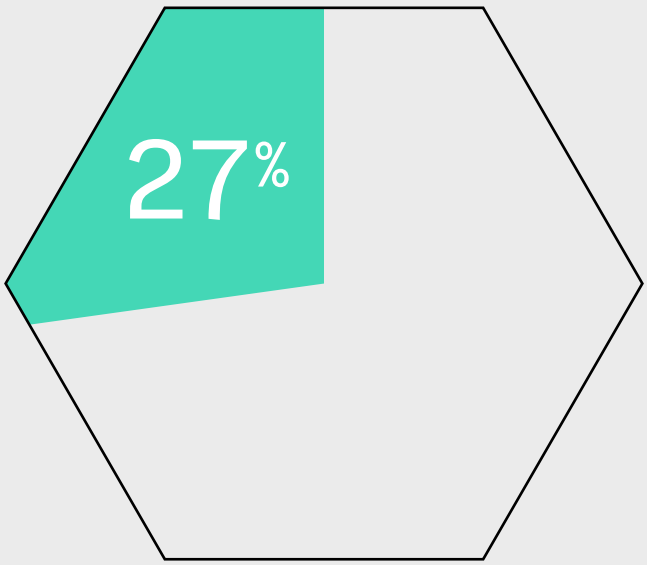
SOURCE: 2022 Survey of 82 business leaders who suffered an attack in the past year

ONE SECTOR STANDS OUT, AND NOT FOR A GOOD REASON.

As previously mentioned no single business sector is invincible when it comes to cyber attacks. However, the majority of respondents who reported suffering a cyber attack in the past 12 months were in the Business Services industry (27%). Business Services are defined as activities that help organizations but do not necessarily result in a physical commodity. They are traditionally outsourced to include training, marketing, consulting, legal, and even security services.

Of those respondents representing Business Services, 62% were seriously concerned about a cyber attack. Despite that worry, 39.13% reported not having cyber liability insurance in place, and 18.84% are without a cybersecurity plan. When businesses work directly with another business, a cyber attack poses an exponential threat, being passed from one organization to the next – putting two or more businesses at risk with just one successful attack.

TWENTY-SEVEN PERCENT OF CYBER ATTACKS WERE WITHIN THE BUSINESS SERVICES INDUSTRY



SOURCE: 2022 Survey of 82 business leaders who suffered an attack in the past year

Cyber threats do not discriminate based on company size. Small businesses are just as much of a target, if not more, for bad actors. With threats continuing to evolve and grow, businesses need to be at the ready.

– Frank Hughes, Chief Information Security Officer at USX Cyber

ACTION MATTERS MORE THAN CONCERN.

Although nearly 80% of respondents indicated a moderate to serious level of concern about their cybersecurity, nearly one-third (32.7%) of those respondents don't have cyber liability insurance, and almost a quarter (23.22%) don't have a cybersecurity plan in place.

One study from HBR indicates that behavioral economics are to blame, as most leaders see cybersecurity as a one-time investment and not an ongoing practice. Mitigation is a core element to cybersecurity, but it also requires management. Not only does a managed cybersecurity approach help prevent real-time and future occurrences, but it is shown to improve employee productivity and customer trust. In fact, according to a post-pandemic study on American consumers regarding cybersecurity and customer loyalty, 31% of consumers said a commitment to protecting data is the most important factor in their decision to be loyal to a brand.

YOU NEED A DYNAMIC DEFENSE.

There's no way around the stats. And there's no way around having the right cybersecurity for your business.

While ransomware, hackers, and cyber attacks might seem like a threat too big to manage on your own, having the right partner makes all the difference. If you are one of the many businesses without an effective cybersecurity plan in place, USX Cyber is here to help. Contact our experts today to find out about our Managed XDR platform, Guardient™ and get advanced cyber protection – before you need it.

METHODOLOGY

USX Cyber partnered with Merit Marketing to conduct a survey and analyze the responses of SMB CEOs and C-Suite executives in June 2022.

REPORT AUDIENCE OVERVIEW:

Date Created: Wednesday, June 01, 2022
Completed Responses: 615
Gender: Male + Female
Location: US Residents

Ages: 30-70
Business role: CEOs, C-Suite Business Leaders
Business size: 1-400 FTE

CONTACT

Rod Volz, Chief Growth Officer
Rod.Volz@USXcyber.com
USXcyber.com