2023 Annual SMO Cybersecurity Readiness Report

Table Of Contents

2023 SMO Annual Cybersecurity Readiness Report

Background

SensCy (which stands for Sensible Cyber) is a cybersecurity company located in Ann Arbor, Michigan focused on small and medium sized organizations (SMOs). As part of our platform, SensCy conducts cyber security assessments based on the National Institute of Technology Standards (NIST) framework and examines a SMO's cybersecurity readiness through the six pillars of a sound cybersecurity strategy (as identified by NIST): **govern, identify, detect, protect, respond, and recover.**

New National Institute of Standards and Technology (NIST)

01 Govern
Establish & monitor cybersecurity risk management strategy

02 Identify
Risk Assessment, Risk Management Strategy, Asset Identification, Governance

03 Detect
Detection Processes, Security Continuous Monitoring, Notification of Anomalies

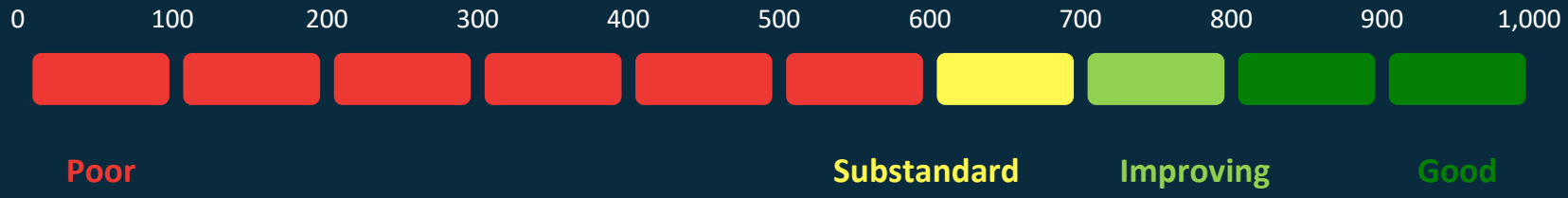
04 Protect
Awareness Training, Policies & Procedures, Protective Technology, Access Control

05 Respond
Incident Response Planning, Mitigations, Analysis, Communications & Improvements

06 Recover
Recovery Planning, Back-ups, Communications, & Improvements

The SensCy Score

SensCy developed the SensCy Score™, which is a proprietary algorithm that delivers a numeric representation of a SMOs cyberhealth from the SensCy cybersecurity assessment. **The SensCy Score is calibrated on a 1,000-point scale and should be thought of as a credit score for a SMOs cyberhealth**. As is the case with a personal credit score, 800+ is good, 700+ is improving, 600+ is substandard, and < 600 is considered poor.



The Data

The data profiled in this report is the result of hundreds of SensCy cybersecurity assessments conducted with SMOs across the United States. The data covers multiple business sectors/industries *(see appendix A for a complete list of sectors)*. The cybersecurity assessments conducted by SensCy generated individual SensCy Scores for each organization. Each assessment was conducted with representatives of the SMO and a cybersecurity professional from SensCy.

This report is designed to examine the cybersecurity readiness of SMOs in the six pillars of the NIST framework by examining the implementation or lack of implementation of various controls that are necessary for a sound cybersecurity framework and culture. This report is not intended to be all-inclusive but rather to provide a snapshot of the basic cybersecurity controls and to gain perspective on the cybersecurity readiness of SMOs.

For purposes of this report, and the associated analysis, a SMO is an organization with 1,000 or fewer employees.

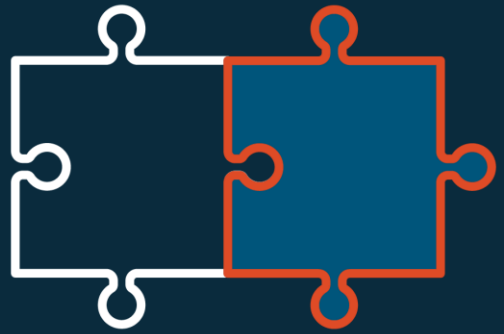
Introduction

We started SensCy with a simple goal - ensure that SMOs can proactively understand and develop their cybersecurity resilience. In our inaugural Cybersecurity Readiness Report, we share findings of the state of cybersecurity amongst SMOs. These findings are the result of hundreds of cybersecurity assessments and SensCy Scores delivered to SMOs. This report aims to not just disseminate statistics but achieve three objectives:

1. Simplify and demystify the cyber landscape

1. Share observations and insights how organizations can build a strong foundation for defending against cyber attacks

1. Empower employees to remain vigilant stewards



Businesses, especially small and medium businesses are ripe targets for hackers. As modern day AI technologies like ChatGPT become widespread, hackers now use them to cause havoc via phishing attacks and demands for ransomware. The average payout for a ransomware attack keeps growing each year. At the same time, current cybersecurity tools are complex, expensive and need sophisticated analysts and teams to manage them effectively. For many businesses in their growth years, affording to hire a Chief Information Security Officer (CISO) is a luxury they cannot afford, nor do they have a budget to buy expensive tools and technologies. Amidst these constraints, SensCy has developed a platform to affordably address these complexities.

SensCy is a trusted transparent partner to SMOs. We use jargon-free simple language to empower people to defend themselves. Above all, we believe in relentless positive action, not fear uncertainty and doubt, which are often associated with domains of cybersecurity. The co-founders of SensCy have built businesses that have scaled globally to over ten thousand employees, and worked in cybersecurity domains in both public and private sectors. We are passionate about helping businesses mitigate risk by implementing a strong cybersecurity culture.

First We Measure, Then We Manage:

From the start, we have been gathering data and insights from businesses to measure, understand, and help improve their cybersecurity posture. To help achieve this, we developed the SensCy Score, a proprietary algorithmic approach based on the NIST framework.

As you may know, NIST, or The National Institute of Standards and Technology (NIST) is a nonregulatory federal agency that is part of the U.S. Department of Commerce. NIST's mission is to advance measurement science, standards, and technology to improve quality of life, enhance economic security, and promote U.S. industrial competitiveness.

Recently, NIST released Version 2.0 of Cybersecurity Framework, which was originally created in 2014. We have incorporated the latest guidelines in our offerings to help businesses easily measure, understand and adopt best practices.

What The Data Says:

In our first annual cybersecurity survey, we present findings that show the state of cyberhealth and resilience across multiple verticals. The high level overview of our assessments are as follows:

1. **77%** of assessed companies do not follow baseline cybersecurity practices. Thus they remain prone to phishing and ransomware attacks.

1. The median SensCy cyber risk score falls at **488** which is considered to be poor.

1. Companies that adopted best practices were able to improve their score by **4X to 10X** within a matter of months.

Call To Action:

Our goal in presenting the data is two fold - to create awareness and to help you as business stakeholders to take action. In our section following the findings, we share some best practices that you can implement within your businesses.

We encourage you to review these findings and start using technologies and developing processes that will empower and strengthen your employees and organizations from cyberattacks. The hackers are at work, now aided with machine learning automations. We have to build our defenses. Our median scores need to get much higher, well above the passing grade.

Cybersecurity is reducing business risk, and following best cyber hygiene practices can significantly reduce that risk. This report examines areas of risk associated with cyber hygiene and best practices as identified by NIST.

Call To Action:

Building cyber resilience for our businesses, infrastructure and our society is an ongoing, consistent proactive effort.

The journey begins with a single step. It doesn't have to be complicated, all it takes is the will to get started. . .

Rick Snyder,
Co-founder and CEO
Governor of Michigan (2011-2019)

Executive Summary & Findings

In measuring cyber risk and resilience, we developed the following framework:

01. People: How can people be empowered and excited about building cyber resilience?

1. The role of CEOs, Owners and leadership in creating policies, governance, and a security-minded culture
2. The role of employees - training, culture and awareness
3. The role of technology personnel in helping install and deploy the right tools

02. Processes: What processes need to be in place to ensure our cyber resilience?

Just as we conduct fire safety drills, and know the way to designated tornado shelters, have businesses developed appropriate strategies to protect their businesses?

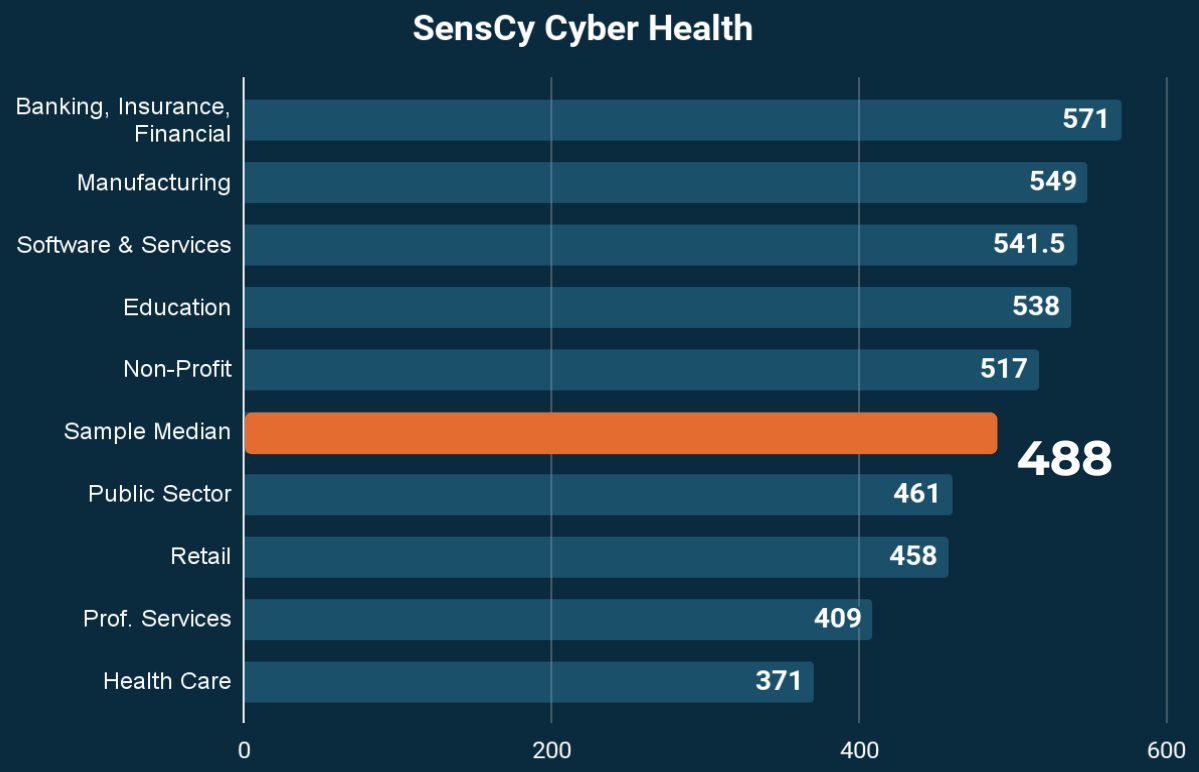
03. Tools & Technologies: How do we pick and adopt the relevant tools in a cost-effective fashion?

Do businesses and employees use appropriate tools and technologies, or are they showing up with a knife to a gunfight?

Assessment Findings

Our findings suggest a concerning lack of preparedness among SMOs regarding cybersecurity measures. Cybersecurity health and risk reduction best practices vary across sectors.

The median SensCy score is 488, which is well below the acceptable grade of security. **To understand the magnitude of this, imagine having a 488 credit score.**



Assessment Findings

A significant number of SMOs do not have cyber insurance, leaving them vulnerable to financial losses in case of a cyberattack, with even fewer having specific coverage for ransomware incidents. Furthermore, a majority do not regularly conduct cybersecurity briefings for executives, leaving decision-makers potentially unaware of critical security risks. Employee training and awareness programs appear lacking, with a sizable portion of respondents not conducting phishing exercises or providing regular training sessions. This is compounded by the high number of employees clicking on phishing links, indicating a need for more robust training efforts.

Additionally, incident response planning and testing seem inadequate, with a notable lack of updated plans and infrequent penetration testing. Despite some positives such as widespread use of firewalls and endpoint protection platforms, significant gaps exist in asset inventory maintenance, multi factor authentication adoption, and password policies. This highlights the need for organizations to prioritize comprehensive cybersecurity strategies to better protect themselves against evolving threats.

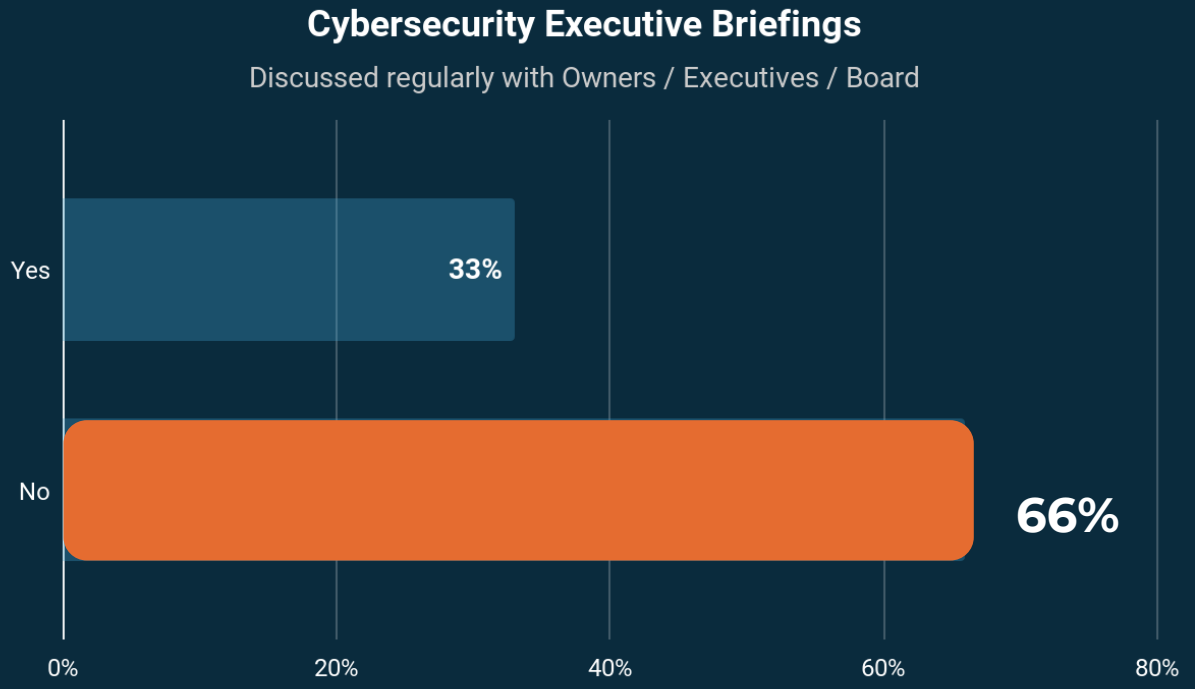
1. People: Role of Leadership

Protecting The Business

- **39%** of respondents do not carry cyber insurance
- **67%** of respondents do not carry ransomware insurance or are unaware if they are protected from ransomware

Measuring What Matters

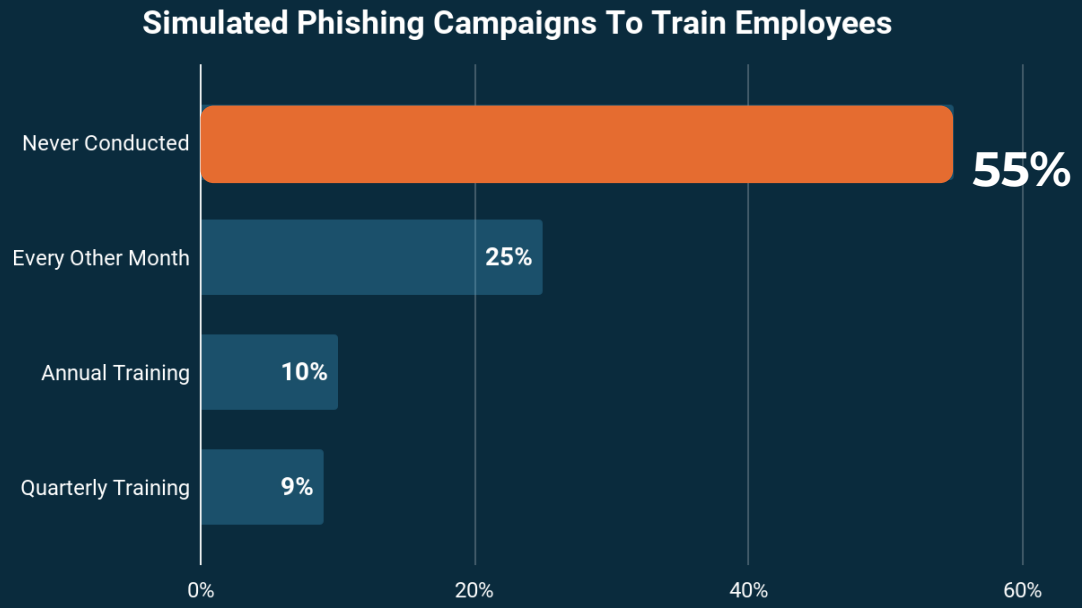
- **44.8%** of respondents did not conduct any internal or external vulnerability scans.
- **70% +** of respondents had no way of regularly checking if their credentials such as username / password were leaked and available for sale on the dark web.



Empowering Your Employees

This past year, SensCy sent over 12,000 phishing email campaigns to clients. Employees clicked on almost 400 email phishing links, essentially putting themselves and their organization at risk.

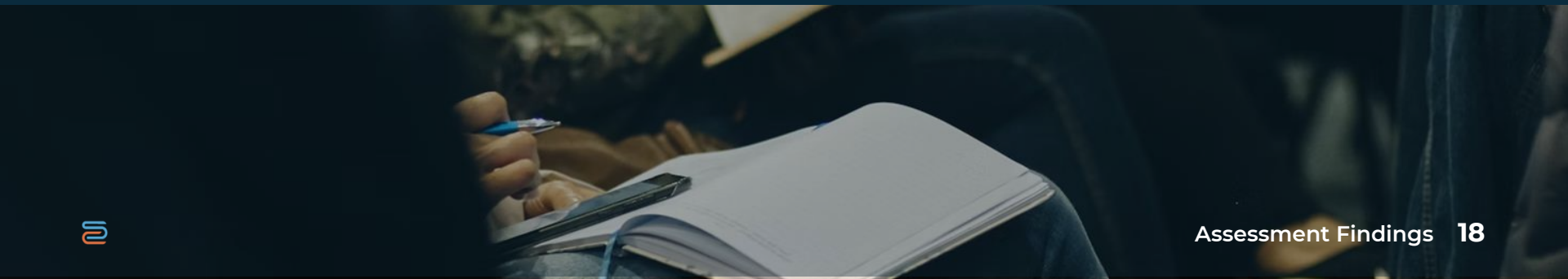
- **49%** of businesses do not conduct any awareness and training programs for employees.
- **65%** of companies have no formal policies to train employees.



02. Processes

- **69%** of companies did not have a formal process to train employees on policy.

- **59.2%** of the respondents did not have an incident response plan. Of those who had a plan, only 18.8% updated such plans annually.



03. Tools & Technologies

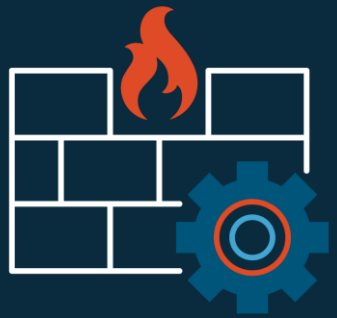
- **83%** of companies do not conduct penetration testing at least annually.
- **62%** of companies do not maintain an updated inventory of technology assets. such as software installed and hardware in use.
- **40%** do not use Multi Factor Authentication for email access.
- **30.3%** do not use Multi Factor Authentication for access to Privileged User Accounts.
- **44%** of respondents did not use 2FA / MFA for all employees, contractors, and systems..

- **30% +** have no password policies for complexity, nor any password management tools.
- **48%** of respondents do not use an endpoint protection platform.
- On the positive side, **70%** have a firewall and have configured it to disallow inbound connections.

Passwords

Endpoint Protection

Firewalls



Call To Action

How can businesses improve their awareness and risk posture? Small and medium-sized businesses (SMBs) have become prime targets for cyberattacks, as evidenced by alarming statistics. Reports show that a staggering **43%** of all cyber attacks are directed at SMBs, yet a concerning **47%** of these businesses lack the know-how to adequately protect themselves.

Despite the prevalent threat, a significant **54%** of SMBs mistakenly believe they are too inconspicuous to be targeted by cybercriminals. However, the harsh reality speaks otherwise, with a staggering **82%** of ransomware attacks involving companies with fewer than 1000 employees.

The consequences of such attacks are devastating, with the average cost of a compromised email attack hitting $383,365 and a **23%** average loss of revenue experienced by SMBs in the year following an attack.

Looking ahead, the outlook remains bleak as there was a jaw-dropping **424%** increase in cyber attacks against SMBs in 2023, underscoring the urgent need for robust cybersecurity measures within this vulnerable sector. To make sure 2024 reverses this trend, we offer a brief outline of recommendations as follows:

- We believe security starts at the top and we encourage business owners and CEOs to take the first step to measure, monitor, and correct the course toward building resilience.

- Secondly, we recommend businesses start to proactively empower their employees. This can be achieved in a number of ways which are simplistic but essential.

- Finally, using the appropriate tools and technologies is a necessary step in recovering from attacks. As they say in cybersecurity, it is not a question of if, but when.

Future Outlook & Conclusion

The emergence of new AI tools and technologies have sparked a paradigm shift in cybersecurity, affecting organizations of all sizes and sectors. Rapid advancements in cyber intelligence capabilities are driving innovation are reshaping the landscape of cybersecurity. The World Economic Forum points out that the landscape of cyber threats will include more sophisticated artificial intelligence techniques, such as advanced phishing campaigns and deep fakes, for which organizations must prepare. In 2023, the landscape of global data breaches significantly intensified with a **72%** increase in the number of data compromises over the previous high in 2022.

How should businesses big and small prepare and integrate cyber risk awareness, intelligence, and resilience into their defense strategies?

Our findings reveal that many companies are open to not just measuring and understanding their risk but rapidly developing their resilience with programs, policies and technologies. However, a large number of businesses still lack the necessary awareness, budget, expertise and tools to effectively defend their businesses or infrastructure.

Adopters of proactive cyber risk management are already reaping benefits such as higher immunity or rapid recovery from attacks. Other benefits include accelerated response, enhanced incident detection, and improved collaboration across teams, leading to heightened resilience and reduced risk exposure. We are excited about the growing recognition of the imperative to be proactive, to empower employees and to embrace more advanced cyber intelligence techniques to stay ahead of evolving threats.

At SensCy, our mission is to measure and accelerate the awareness of cybersecurity risk and identify solutions to empower culture change for all companies big and small. In pursuit of this mission, and moving away from hype and jargon, into meaningful cybersecurity endeavors, we present our first report. Our ongoing commitment is to provide you with actionable insights into the realities of the cyber landscape, empowering and aiding you in defending and protecting your businesses as they grow.

Glossary Of Terms

Cybersecurity Tools & Technologies

Just as any home has security cameras, a fence, indoor motion detectors and more, the world of cybersecurity has similar products.

Before purchasing any cybersecurity product, carefully assess your business's specific security needs, budget constraints, and regulatory requirements. Start with a cybersecurity assessment to help you understand your current cybersecurity posture, Consider consulting with a cybersecurity expert to help evaluate your options and implement a comprehensive cybersecurity strategy tailored to your organization's needs.

Depending on the number of employees, type of business (manufacturing, services, education, etc.) and location (on-site versus remote), some cybersecurity products businesses should consider include:

01. Endpoint Protection

Software that is installed on the laptops and between devices acts as an antivirus/antimalware solution is essential for protecting your systems against known and emerging threats. Endpoint visibility, threat hunting, and automated response actions enhance your defense against malware, fileless attacks, and other advanced threats.

Anti-malware Products offer real-time scanning, threat detection, with automatic updates, quarantining, and behavior-based detection to safeguard against a wide range of malware, including viruses, ransomware, and spyware.

02. Firewall

Depending on the type of network, a firewall is essential. It serves as the first line of defense against unauthorized access to your network. Consider deploying a next-generation firewall (NGFW) that offers advanced features such as intrusion prevention, application control, and VPN support. A properly configured firewall can help block malicious traffic and prevent cyber attacks from reaching your internal network.

03. Data Backup & Recovery Solution

In the event of a cybersecurity incident, such as a ransomware attack or data breach, having reliable data backup and recovery capabilities is essential for restoring critical business operations. Invest in a backup solution that provides automated, regular backups of your data, both onsite and offsite, and offers features such as encryption, versioning, and disaster recovery capabilities. Regularly test your backup and recovery processes to ensure they can effectively mitigate the impact of potential security incidents.

04. Asset Inventory

Many SMOs do not have clarity on what is connected to their network. Asset inventory is like making a list of all the stuff you have connected - computers, servers, software, and anything else important. We cannot protect it if we do not know that we have it.

05. Vulnerability Scanning

Like using a digital magnifying glass to find weak spots in your digital stuff, scanning checks computers, software, and networks for any holes that hackers could sneak through to cause trouble.

06. Threat Feed Monitoring

Patching our software and hardware with the latest security updates is critical to preventing attacks. Monitoring for real time zero-day vulnerabilities/known breaches and understanding how to remediate them prevents us from being an easy target to hackers.

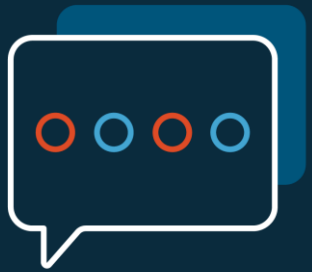
Types of Attacks: Phishing, Vishing, Smishing,

Hackers will try to gain access to your network by pretending to be a trustworthy person or organization to trick you into giving them sensitive information, like passwords, financial, or credit card numbers. They often do this through **fake emails, phone calls, messages**, **or websites** that look real. Institute a program for consistent cybersecurity awareness training and phishing campaigns to educate your employees.

Phishing

Vishing

Smishing



Scammers call you pretending to be from a legitimate company or vendor, or a charitable organization, trying to trick you into revealing sensitive information or sending money. They might use fake caller IDs or impersonate someone you trust to make their scam seem legitimate.

Other scams - Tax, Charity, Dating, Urgent Money Transfer all try to create a sense of urgency and panic while attempting to extracting financial details. A good training program will help your employees become a first line of defense against these attacks.

Cyber Insurance

Cyber insurance, not covered by your typical liability / errors and omissions insurance, is designed to protect businesses from financial losses and liabilities arising from cyber threats and incidents. It typically provides coverage for expenses related to data breaches, cyberattacks, ransomware, and other cybersecurity incidents, including costs associated with legal fees, notification to affected parties, and potential financial losses. Invest in a good cybersecurity insurance policy that covers ransomware and business email compromise. But remember, insurance alone is not a cybersecurity strategy. The reputational damage that comes from a cyberattack can be catastrophic to your business.

What Does A Typical Policy Entail?

First-Party Coverage	Third-Party Coverage
Ransomware Recovery of / Loss of data Loss of Income Extortion Legal Costs to determine notification and regulatory Compliance Fines and Penalties Customer Notification	Losses incurred to third parties ***example:** SMB vendor is breached leading to a breach of a larger enterprise. Claims and Settlements Litigation / Regulatory costs

Watch for exclusions and understand your claims process as well as understand your deductible and annual premium costs.

Cybersecurity Policies

01. Employee Related Policies & Training

Training & Awareness Program: Regular cybersecurity training sessions for employees are essential for raising awareness of security threats and best practices. Topics may include phishing awareness, safe browsing habits, and recognizing social engineering attacks.

Employee Acceptable Use Policy (AUP): This policy outlines acceptable and unacceptable uses of company resources, including computers, networks, and the internet. It should address appropriate employee behavior, such as prohibiting unauthorized access to data, downloading unauthorized software, or visiting malicious websites.

02. Organizational Policies

Data Protection & Passwords: This policy outlines how sensitive data should be handled, stored, and protected. It should include guidelines for data encryption, password protection, access controls, and data backup procedures. A strong password policy is crucial for preventing unauthorized access to company systems and accounts. This policy should specify password requirements, such as length, complexity, and expiration periods.

Network Security Policy: This policy addresses measures to secure the company's network infrastructure, including firewalls, intrusion detection systems, and access controls. It should also cover guidelines for remote access and wireless network security.

Incident Response Plan: This plan outlines procedures for responding to cybersecurity incidents, such as data breaches, malware infections, or system outages. It should include steps for identifying and containing the incident, notifying appropriate stakeholders, and restoring normal operations. It is important to note that a cybersecurity incident response plan is different than a business continuity plan or disaster recovery plan. **A good cybersecurity incident response plan will guide leadership through an incident to ensure an expedient recovery while preventing mistakes that can lead to a protracted and expensive recovery.**

Contractor / Vendor Management Policy: If your business works with third-party vendors or contractors who have access to company systems or data, a vendor management policy is necessary to ensure they meet security standards and comply with relevant regulations.

Executive Briefings

Executive briefings are concise presentations or summaries designed to provide top-level executives with key information and insights relevant to cyber risk and resilience.

They typically highlight critical issues, trends, and recommendations to help leaders make informed strategic decisions. Cybersecurity is risk mitigation. Risk mitigation is culture change. Leadership must be engaged.

Cybersecurity Executive Briefings

Who?	The participants: Business Owners and Leadership, Security /Technology leads.
When?	Executive briefings to the leadership team should be done at least annually. A lower risk score necessitates more frequent briefings as you work to improve.
Why?	To build a better culture and reduce your risk. A ransomware can cause a business shut-down or loss of revenues / brand and trust. By better awareness, proactive actions and healthy practices, you can mitigate risk.
What?	The cyber risk executive briefing agenda includes: **(1)** An assessment of the organization's cybersecurity posture , **(2)** New threats on the landscape , **(3)** Actionable recommendations for enhancing resilience , **(4)** Readiness for incident / ability to response readiness , **(5)** Employee training updates , **(6)** Requirements of Tools and Technologies / Budgets , **(7)** Regulatory compliance (if necessary) updates.

Thank you for your interest in our Annual SMO Cybersecurity Readiness Report

Please feel free to share this report with your networks. Cybersecurity is a team sport and we all need to work together to make the world a safer place from cyber criminals!

Use this QR Code to request a free cyberhealth evaluation for your company!