RAMPxchange

Embracing Collaboration to Strengthen Security Posture Among SMBs

rampxchange.com

Table of Contents

Introduction to Cybersecurity Challenges for SMBs

Small and mid-size businesses (SMBs), or small and mid-size enterprises (SMEs), form the backbone of the global economy. According to the **World Bank Group**, SMEs constitute about 90 percent of all businesses and are responsible for over half of global employment. The **2023 Hiscox Cyber Readiness Report** highlights a disturbing trend: a significant rise in cyberattacks targeting small businesses, especially those with fewer than ten employees. The attractiveness of SMBs to cybercriminals is exacerbated by their sheer number and generally weaker security infrastructure compared to larger corporations.

Understanding the Risks: Why SMBs are Perfect Targets

Financial Barriers

Compared to large corporations with budgets for expansive IT infrastructure, SMBs often lack the financial means to invest significantly in state-of-the-art security system technologies.

Entrepreneurs and startup founders already wear many hats and may want to oversee security operations personally. Burdened with other responsibilities, many often neglect cybersecurity or lack the resources for a dedicated team or individual to focus on cybersecurity measures.

Skilled Labor Shortages

If organizations can afford to add personnel, the industry's looming labor shortage presents another challenge. The **International Information Systems Security Certification Consortium (ISC2)** says the cybersecurity workforce gap is at a record high, with 4 million new professionals needed to safeguard digital assets adequately. For SMBs, this translates into difficulties in hiring qualified cybersecurity personnel, further increasing their vulnerability to cyber threats.

Gateway to Larger Businesses

SMBs are frequently intertwined in partnerships and supply chains with larger companies, making them attractive targets for cybercriminals looking to access broader networks. Breaching less secure small service providers is a gateway to more extensive, lucrative targets, such as massive customer or patient databases and sensitive intellectual property.

Top 5 Cybersecurity Threats to Small Businesses

To best protect themselves and their customers' sensitive data, SMBs must be aware of five of the most significant looming cybersecurity threats facing their organizations:

1. **Poor Password Hygiene**: The use of weak or predictable passwords remains a significant threat.

2. **Phishing:** Phishing attacks remain the largest and most popular cyber threat facing small businesses. Through emails that appear to be legitimate or from a trusted source, scammers work to trick users into providing sensitive information and account details, clicking a malicious link, or downloading a virus-infected file.

3. **Malware:** Often introduced through email or insecure public Wi-Fi networks, malware can wreak havoc on an SME's digital infrastructure by stealing or destroying data, blocking programs, or spying on user activity.

4. **Ransomware:** Ransomware attacks aim to infect an SME's network devices with malware, encrypt company data so its owners can no longer access or use it, and then demand lucrative ransom payments to have the data unlocked and restored.

5. **Insider Threats:** Not all cybersecurity incidents involve malicious hackers and sophisticated cybercriminals. Whether intentional or accidental, internal team members with more access to systems and infrastructure than necessary to do their jobs can significantly compromise company data.

BEST PASSWORD PRACTICES

In it's Annual Cybersecurity Attitudes and Behaviors Report, the National Cybersecurity Alliance researches and recommends practices such as:

****

Increasing password length

****

Check passwords against known breached password lists

****

Avoid the use of password dictionaries or context-specific words

****

Prevent the use of repetitive or incremental passwords

****

Use unique and separate passwords

****

Apply multi-factor authentication

The Power of Collaboration and Strategic Partnerships

"Collaboration" is more than just a team-building buzzword. Cybersecurity professionals have a strong track record of collaborating—largely because it's a more effective way to battle against malicious threat actors who have long organized sophisticated attacks together toward common targets. Companies of all sizes and across industries can benefit from banding together and collaborating in various ways to improve their cybersecurity postures collectively. By working together, organizations can leverage combined knowledge, expertise, and resources to create a more resilient security environment, better protecting themselves and customers from cyber risks.

Elements of Cybersecurity Collaboratives

Open Information Sharing

Local or industry-specific networks enable businesses to exchange threat intelligence and best practices, raising awareness of risks and fostering preventative actions. By joining these trusted networks, organizations can share timely information on threats, vulnerabilities, and incidents, helping to proactively counteract cyberattacks with new defenses. These networks, whether industry-specific or cross-sector, provide access to a wide range of insights and expertise.

In case of a breach, sharing details about attack patterns, mitigation strategies, and recovery processes can minimize damage and accelerate recovery. By learning from each other's experiences within these networks, organizations can avoid common errors and enhance their cybersecurity measures against evolving threats.

Joint Research

Joint research and development projects represent another proactive element of cyber collaboratives. Companies collectively fund research or developments that advance their shared cybersecurity abilities, such as new encryption methods, intrusion detection techniques, or other innovative solutions. Working together, organizations can leverage their collective expertise to develop more robust and effective cybersecurity technologies, best practices, and infrastructure.

Cybersecurity Training

Some collaborative members pool resources and share responsibilities to organize cybersecurity workshops or create engaging security training presentations. Collaboratives and their members may sponsor or offer cybersecurity training to those outside their membership base.

The **National Cybersecurity Alliance**, a public-private partnership, offers **virtual and in-person cybersecurity events** for small business owners. The **Global Cyber Alliance (GCA)**, a non-profit dedicated to reducing cyber risk and making the Internet a safer place, develops free resources such as their **GCA Cybersecurity Toolkit**. The toolkit is a helpful resource for organizations with limited IT expertise or resources.

Common Framework

For similar or related organizations that often work with common networks of third-party vendors or service providers, developing a common framework for evaluating their security practices is beneficial for the cybersecurity posture of all involved.

Cybersecurity frameworks and standards such as the **NIST Cybersecurity Framework**, **PCI DSS**, **ISO 27001**, and **CIS Critical Security Controls** are widely accepted effective templates and guidelines. Risk authorization and management programs encourage quicker collaboration by establishing universally accepted security standards and baselines for providers' products and services.

Advocacy

Organizations within a cybersecurity collective benefit from shared expertise to enhance their security posture and collaborate on advocacy to educate the public and influence cybersecurity practices across industries. These efforts can significantly shape local and federal cybersecurity regulations.

Professional groups and cybersecurity advocates often impact policymaking more effectively than individual SMBs, as government bodies rely on private sector input to shape well-informed cybersecurity policies. The US Department of Homeland Security's Cybersecurity and Infrastructure Agency's **Joint Cyber Defense Collaborative (JCDC)** unites cyber defenders globally to foster public-private partnerships and collective action in cybersecurity.

Benefits of Cybersecurity Collaboration

Strategic collaboration can become any business's secret weapon in strengthening its cyber incident readiness and overall security posture. From local chapters of professional organizations to a vast collection of websites, online message boards, subreddits, LinkedIn groups, and other forums, there are active, collaborative, and flourishing communities of cybersecurity professionals offering insight and expertise. Some key benefits of collaborating follow.

Networking:

Online forums, networking events, and collaborative communities give professionals valuable opportunities to connect with peers and experts across various fields of cybersecurity. By building a network of contacts, businesses can meet individuals or entities that may lead to future security collaborations or business relationships. Connecting with peers from different organizations can also give professionals a broader perspective and insight into other industries' challenges, relevant trends, and best practices.

New Threat Updates:

The cybersecurity landscape constantly evolves, with new threats and vulnerabilities emerging regularly. Community forums and industry collectives can provide real-time updates on emerging threats or newly uncovered vulnerabilities. By monitoring and participating in industry forums and relevant discussions, businesses can stay current with the latest cybersecurity trends and developments and adapt their strategies to defend against new threats.

Knowledge Sharing:

Collaborative communities serve as a holistic hub of shared knowledge where experienced professionals and enthusiasts can share their insights, expertise, and solutions to various cybersecurity challenges. Professionals can use these platforms to collaborate on disseminating best practices and lessons learned, fostering a culture of continuous learning and improvement among the cybersecurity community.

Collective Problem Solving:

Cybersecurity threats are complex, but a community culture of collaboration helps like-minded partners become more resilient and stronger together than they would be on their own. Collaborating allows professionals to seek advice and guidance from a broader community when facing a specific cybersecurity issue. This collective problem-solving approach can lead to quicker, more efficient solutions by providing different perspectives. Professionals can collaborate to find innovative solutions and approaches, strengthening their ability to address emerging cyber threats.

Feedback and Recommendations:

For professionals evaluating cybersecurity tools or strategies, forums can be valuable for seeking input from others who have used or implemented similar solutions. By leveraging the expertise of the larger community, professionals can save time, avoid potential pitfalls, and make informed decisions based on others' real-world experience.

Learn how RAMPxchange helps leverage all the benefits of cybersecurity collaboration.

Proactive Measures: Reporting Cybercrime

While investigating and prosecuting cybercrime can be difficult across legal jurisdictions or international borders, victims or targets can do their part to help bring criminals to justice. Collaboration between cybercrime targets and the appropriate authorities is important in mitigating risk and raising resiliency against additional attacks. The following are some recommended steps to take if you have been targeted.

1

Alert Your Team.

If you have identified a suspicious email or fallen victim to an attack, you may not be the only target within the organization. Alerting your colleagues and the IT department of cybercrime as soon as possible helps thwart further targeted efforts against the company.

2

Gather and Keep Evidence.

The **National Cybersecurity Alliance (NCA)** recommends keeping and collecting all cybercrime evidence, such as copies of phishing emails or social media messages, websites, receipts, invoices, or other related documents.

3

Contact Local Law Enforcement.

Regardless of where a cyberattack or social engineering scam originates, your local police or sheriff's departments can take a formal report. Many local departments have resources focusing on cybercrime or can refer you to other agencies.

4 Report to a Global Cybercrime Fighting Organization.

The **Anti-Phishing Working Group (APWG)** is a coalition of counter-cybercrime responders, forensic investigators, law enforcement agencies, technology companies, financial services firms, university researchers, NGOs, and multilateral treaty organizations. **Report suspicious emails** to APWG for analysis.

5 File a Complaint with the Internet Crime Complaint Center (IC3).

A partnership between the FBI and the National White Collar Crime Center, the IC3 reviews and evaluates complaints as the nation's central hub for reporting cybercrime. The organization refers complaints and reports to the appropriate federal, state, local, or international law enforcement or regulatory agency, issues consumer and industry alerts, and provides ample educational resources and research for online security.

6 Contact Other Federal Agencies.

Recognizing that cybercrime can have serious consequences and cause lasting harm, the **Federal Government** has issued a unified message for cyber incident reporting. The publication includes guidance on what, when, and how to report cyber incidents, as well as key points of contact at cybercrime-fighting agencies such as the US Secret Service, National Cyber Investigative Joint Task Force, National Cybersecurity and Communications Integration Center, and more.

Future Threats and the Need for Collaborative Strategies

Cybersecurity Ventures and Cybersecurity Magazine predict global cybercrime costs to reach $10.5 trillion annually by 2025. While it's impossible to predict and prepare for specific new attacks, there are trends in both the near and distant future that forward-thinking organizations can begin to address now. As they're emerging and evolving concepts on the bleeding edge of development, collaboration today addressing challenges of tomorrow can be beneficial for an SMB's cybersecurity future.

Artificial Intelligence (AI):

Advancements by popular language-based AI tools will continue to simplify cybercriminals' social engineering efforts. Phishing scams have been recognizable for years due to frequent misspellings, grammatical errors, or awkward phrasing mistakes, but modern-day AI can help provide cybercriminals instant access to near-fluency in English.

Emerging generative AI programs can also be used by white-hat hackers for good, and "AI checker" tools are already in use to detect email language that could be lurking as a phishing attack. AI-powered solutions could grow to help identify and respond to cyber threats in real-time or identify vulnerabilities and potential attack vectors, enhancing protection in ways today's traditional security measures can't match. But as the technologies continue to evolve, AI could become one of the most harmful weapons on the horizon.

Quantum Computing:

While widespread, commercially available quantum computing is still considered years away, the timing is uncertain, and research is already underway to mitigate the risks posed by quantum computing. Researchers are developing quantum-resistant or quantum-safe cryptographic algorithms designed to withstand attacks from quantum computers.

Quantum computing is a revolutionary type of computing that leverages the principles of quantum mechanics to process information in ways fundamentally different from classical computers. While classical computers use bits as the smallest unit of data (representing either 0 or 1), quantum computers use quantum bits or qubits. Qubits can exist in multiple states simultaneously, a phenomenon known as superposition. They can also be entangled, which means the state of one qubit can affect the state of another, even if they are physically separated.

Quantum computing has the potential to perform certain types of calculations much faster than classical computers. The speed has implications for many applications, including cryptography and cybersecurity. Quantum computing's impact on cybersecurity is predicated on its capability to exponentially accelerate computations, particularly those used in solving the complex mathematical problems of traditional encryption algorithms. It will pose substantial challenges to traditional cryptographic methods and security infrastructures for encrypting sensitive data. While it may take many years for today's strongest and fastest computers to break down standard security keys, quantum computing of the future looks to shorten that time to just a few hours.

Cybercrime-as-a-Service (CaaS):

In a similar vein to now-familiar cloud offerings such as software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS), the cybercrime-as-a-service (CaaS) model makes the tools and resources for carrying out cyberattacks much more widely available to new customers and threat actors.

The digital underground black markets that rent and sell a range of advanced cyberattack tools, services, and resources lower the barrier to entry and make cybercrime activities more available to a broader range of individuals. For hackers and criminals intent on launching disruptive cyberattacks, CaaS represents an affordable and cost-effective way to do so by utilizing nearly untraceable cryptocurrency payments and a widespread global network of providers.

The emerging cybercrime-as-a-service economy is on the rise. It already accumulates the knowledge, tools, and resources of millions of cybercriminals, making them easily available to any malicious groups or individuals intent on launching an attack. While law enforcement agencies have taken down many CaaS marketplaces, they'll only continue to pop up and operate in the shadows of the "dark web" in the years to come, making it easier for inexperienced cybercriminals to stage increasingly complex attacks or perform sophisticated data breaches.

Cyber-Physical Systems (CPS) Security:

Cyber-physical systems (CPS) security is an emerging critical field focusing on the security of systems that interconnect digital components with real objects and physical processes. CPS applications combine computational and physical tools such as sensors, actuators, and control systems and are often related to products and services utilizing the Internet of Things (IoT). They integrate digital and physical aspects to affect life and businesses across services and applications such as smart buildings, supply chains, e-commerce, and more. Additional examples of combining digital and physical tools include technologies used in autonomous cars, network-connected healthcare devices, building automation, or other online operations and utility infrastructure.

CPS systems introduce new vulnerabilities, expanding cybercriminals' potential attack surfaces and entry points both digitally and physically. Because these systems are highly interconnected, they are more susceptible to cascading failures. An attack on one component can have a domino effect, causing widespread damage. Integration into critical infrastructure makes CPS systems vulnerable and attractive targets, and ongoing adoption will require advanced and innovative cybersecurity solutions balancing safety and performance possibilities.

The Need for Collaborative Strategies:

Gartner cybersecurity analysts predict that by 2025, threat actors will successfully weaponize operational technology environments enough to cause human casualties. For example, a 2021 cyberattack on a Florida water treatment plant attempted to increase the amount of sodium hydroxide in the water supply to potentially dangerous levels. While that intrusion was prevented before it could be carried out, a recent Gartner survey ranked IoT and cyber-physical systems as security and risk leaders' top concerns of the coming years.

Collaboration among SMBs already does and will continue to play a crucial role in addressing emerging challenges in cybersecurity. From fostering a collective approach to research, development, training, incident response, and advocacy, a collaborative mindset is essential and can lead to security advancements that solve new problems and make the most of emerging technologies.

About RAMPxchange

After going through the FedRAMP process and helping found StateRAMP, Knowledge Services ownership learned a lot. RAMPxchange is a result of the ownership's desire to share what they learned to make it easier for public and private organizations to work together. We strive to bring efficiency, transparency, simplification, and cost savings to everyone wanting to improve the cybersecurity posture of our nation.

Our Values

Community

In our knowledge-based economy, the sharing of information is paramount. We rely on each other to communicate and gain strength from our different experiences.

Integrity

In business and in life, we believe honesty is always the best policy. We take pride in our integrity and in doing what's best for the people we serve.

Protection

Technology changes at a rapid pace, and people's lives are affected every day by cyber attacks. Improving cybersecurity for all is about protecting and serving people.

Innovation

Amidst a wave of transformation, we embrace opportunities to create, scale, and elevate our craft. We're empowered by the prospect of making organizations more open and collaborative.

Final Thoughts

In a world where digital threats are constantly evolving, strategic collaboration can significantly enhance a company's cybersecurity measures and competitive edge. Embracing a collaborative approach helps SMBs not only improve their security but also position themselves for sustained success in a digital economy.

Contact us to learn more about the RAMPxchange marketplace, its members and how these experts can help you on your journey.

rampxchange.com/contact/