Petri IT Knowledgebase Resource
A BWW Media Group Brand

PETRI
WE GET IT

Petri Whitepaper
November 10, 2022

Essential SMB Cybersecurity Preparation

Sponsored by
Devolutions

Overview

Cybersecurity is one of the top concerns for most IT organizations and implementing an effective cybersecurity strategy has never been harder.

Today's IT cybersecurity threats are more frequent and more sophisticated than at any time in the past.

Digital transformation and Ransomware-as-a-Service bring new IT security challenges

There are several reasons for the rise in cyberattacks. First, over the past few years most small and large businesses, organizations, and even governments have been in the midst of a digital transformation, requiring them to update their computer systems and adopt new technologies. This has resulted in the introduction of technologies and new devices that don't always fit into the traditional security model.

Secondly, the emergence of Ransomware-as-a-Service (RaaS) has fueled the rise in ransomware. Just as technology has progressed for businesses, it has also progressed for cybercriminals. Today's cybercriminals are sophisticated and they have an array of easily accessed hacking tools at their disposal.

Ransomware-as-a-Service (RaaS) providers bring the ability to launch ransomware attacks within the reach of cybercriminals that lack the high-level technical skills that would otherwise be required to create and use ransomware.

On top of this, the pandemic fueled a rapid and massive increase in the remote workforce - substantially increasing the organization's attack surface and bringing in a mix of poorly secured personal user devices. It's clear that businesses will need to cope with these conditions in the foreseeable future.

It's important to note that cybercriminals are not limiting their attacks to large organizations. Increasingly, they are targeting SMBs and exploiting other vulnerable organizations like schools, hospitals, manufacturing firms, and even infrastructure providers like gas pipelines and electrical power plants. According to research by IBM and the Ponemon Group, the cost of a data breach for organizations of all sizes has climbed to an average of $4.24M USD per incident - the highest amount in history. For just SMBs, the financial toll can range from $120,000 USD to $1.24 million USD per incident.

It's clear that IT security and cybersecurity are both expensive and growing problems. It's also important to understand that security is not just a technology issue. Nowadays, it is fundamental to ensuring business survival. Let's take a closer look at some of the essential areas SMBs need to focus on.

Assessing IT security and cybersecurity threats

Security threats and the severity of those threats are growing. In the Devolutions State of IT Security in SMBs in 2022-2023 survey, executives and decision-makers in SMBs worldwide were asked to describe their overall perspective on IT security. They were asked, ***"Compared to last year, how concerned are you about cybersecurity threats toward your organization?"*** Two thirds (67%) replied ***"We are more concerned than last year,"*** 28% replied they had the ***"Same level of concern,"*** while 5% were ***"Less concerned."***

That 67% of companies were more concerned shows that most are preparing for increased cyberattacks. However, nearly a third showed the same level of concern, indicating they may not be taking adequate precautions for future escalation of attacks. The decrease in concern in the 5% can maybe be attributed to many companies calling remote workers back into the office since the pandemic's decline, enabling companies to tighten security controls.

Not surprisingly, when asked about the types of cybersecurity threats that they were most concerned about, most businesses (81%) were worried about ransomware followed by:

- phishing (69%)
- malware (38%)
- and insider threats (21%)

Considering the continued growth of ransomware, it's clear that this is one area where SMBs need to prepare for increased attacks.

Securing third-party software and the supply chain

One important area that was not reported as a top concern was third-party software or supply chain attacks. The recent SolarWinds/Solarigate supply chain attack, which affected thousands of businesses, clearly illustrates the need to stringently vet third party software to ensure it follows best security practices.

13% of SMBs taking no measures to prevent cyberattacks

Assessing your cybersecurity threats is an important first step toward understanding and appropriately responding to the dangers of different cybersecurity attacks. While most organizations are preparing for an increase in ransomware, phishing, and malware attacks, the survey also revealed that 13% of SMBs were taking no measures at all to prevent these types of attacks.

While SMBs are limited in their resources, it's clear that cybersecurity is an area that cannot simply be ignored, or you do so at your own peril.

Implementing Privileged Access Management

Privileged Access Management (PAM) refers to the management of administrative accounts and accounts with elevated security rights that can perform maintenance, make system changes, and execute other types of privileged operations. These privileged accounts are often the target of cyberattacks because they have access to highly sensitive, confidential, and proprietary information.

This makes the protection and management of these privileged accounts a high priority. PAM solutions address this problem. PAM reduces security risks by protecting accounts with elevated privileges, as well as lowering operational costs and increasing the visibility into the usage of these types of accounts.

When the ***Devolutions State of IT Security in SMBs in 2022-23*** survey asked, ***"How do you primarily manage access to privileged accounts in your company?"*** only 12% of organizations reported that they have fully deployed PAM solution in place. Another 9% reported that they have a partially deployed PAM implementation, where they are using some of the capabilities but not all of them.

A follow-up question probed the reason why some SMBs are not deploying PAM solutions. The survey found that 28% of businesses reported that they do not have the budget. While an additional 12% thought that PAM solutions are too complex to implement and manage. These perceptions are understandable. However, they are outdated and no longer true.

Privileged Access Management solutions are now affordable and simple to deploy

Originally, PAM solutions were priced for large organizations and SMBs could not afford them. What's more, SMBs could not afford a team of in-house cybersecurity specialists to configure and use these older solutions. However, that has changed over the years. There are now several easy-to-use PAM solutions that are affordably priced for the SMB.

Implementing a PAM solution is a vital step in preparing for stronger SMB cybersecurity. The survey also revealed that the three most important features that SMBs need from a PAM solution are:

1. automatically expiring privileged access
2. built-in multifactor authentication (MFA)
3. password rotation and reset

Today's PAM solutions provide this type of automation making them efficient and well suited to the needs of SMBs.

Promoting security awareness for end users

Unfortunately, most cybersecurity measures can be circumvented and defeated by your end users. They are the weakest link in the IT security chain. And there are a multitude of ways that users can sabotage even the best security plans.

Some of the biggest issues are weak passwords (like "password"), reusing passwords on multiple sites, sharing passwords, writing passwords down, clicking on phishing links that download malware, and accessing corporate resources through insecure public Wi-Fi connections.

The variety of ways that end users can cause security exposures is nearly endless. According to the Verizon Data Breach Investigations Report (DBIR) for 2022, 82% of breaches in the past year involved the company personnel.

The best way to address end user security issues is through security awareness training. The ***Devolutions State of IT Security in SMBs in 2022-23*** survey asked, ***"How does your company primarily educate end users about IT security?"*** About a third (30%) rely solely on resources like videos, articles, and webinars. Another third (31%) use online training. And a much smaller number (16%) use live training and workshops or simulations (5%). While 12% do nothing at all. No end user training is virtually the same as inviting some type of security exposure.

The vast majority of SMBs (88%) are providing some form of user education, which is good. Considering the high costs of a cybersecurity break-in and the knowledge that most exposures come from end users, these factors underline the essential fact that this is one of the areas where increased investment will result in improved protection. The costs of user education are trivial compared to the costs of a successful cybersecurity attack, which could put an SMB completely out of business.

Securing Remote Access Management

Over the past couple of years, the pandemic caused the use of remote access tools to skyrocket for businesses of all sizes. While this allowed remote workers to access corporate resources and applications from home, it also greatly expanded the organization's attack surface.

Remote access enables employees to connect to local office systems to perform their work or for administrators to undertake various management tasks remotely. As you would expect, IT administrators and managers often require privileged credentials. Weak passwords, which are easily guessed, or reused passwords that can be harvested off other sites can open the door to hackers. Once a cybercriminal has gained access to your network, they can potentially access other systems laterally across your networks.

To gauge the current usage of remote access the survey asked SMBs, ***"What is your organization's employee deployment situation right now?"*** Not surprisingly, the majority (75%) are allowing hybrid work, where employees split their time between the office and home. Only 19% have all their employees working in the office full-time and a few (6%) were totally remote. These results show that remote work and remote access technologies remain in widespread use and probably will be that way for some time to come, if not indefinitely.

A follow-up question dug into the tools and technologies that businesses were using to secure and manage remote access. The three most popular solutions were:

- Virtual Private Network (VPN)
- Multifactor Authentication
- Devolutions Remote Desktop Manager (RDM)

The pandemic significantly increased VPN usage for remote workers. And many businesses used MFA as an extra layer of security as remote workers must verify their identity by providing their login credential along with some other external piece of information like a code sent to a cell phone.

Devolutions RDM not only organizes your remote connections, but also strengthens remote security through its password management capabilities. RDM's password management supports password policies requiring password length, complexity, and restricting password reuse. Additional tools, like a password generator and a password analyzer, can make it easier for users to create and use strong passwords.

With RDM, passwords are centrally stored in a secure location, eliminating the need for users to come up with their own haphazard and insecure password storage schemes. RDM can also provide an overview and log of all your organization's remote desktop activity.

IT cybersecurity management planning

Comprehensive IT cybersecurity management consists of strategies, policies, processes, technologies, and tools that ensure the protection, integrity, and availability of IT systems. The ever-increasing levels of threats combined with the influx of new technologies to secure might make you think that security would consume a significant percentage of the SMB's IT budget. However, surprisingly that is not the case.

When asked how much of your organization's IT budget is allocated for security, a third (32%) responded that it was less than 5%. While the amount an organization needs to spend on cybersecurity varies greatly for different businesses, 5% doesn't seem to be in line with today's threat levels.

58% responded that it was less than 20% and only 10% allocated more than 20% of their budget for security. 49% did report an increase in security spending but 45% replied that it was the same. At first that may seem inadequate. However, businesses also must consider the overall business environment.

The pandemic resulted in an unprecedented amount of financial damage for many businesses. Between April 2020 and April 2021, a study conducted by the Federal Reserve estimated 200,000 SMBs in the U.S. permanently closed as a direct result of the pandemic. For many SMBs, reducing IT security spending was a matter of necessity rather than what they might wish to do.

The top security projects that businesses were looking into for the future included: PAM solutions, 2FA (two-factor authentication, a.k.a. MFA), providing end user training, updating VPN strategies, implementing automatic password rotation, and expanding password management. All of these frequently mentioned IT security projects are related to identity and access management, which are two core foundations for effective cybersecurity.

Preparation for protection

Nowhere is the saying "proper planning prevents poor performance" truer than in cybersecurity. Businesses today are at an important tipping point as the digital footprint of organizations continues to change and evolve, making many older established cybersecurity measures obsolete; and at the same time threats increase, and new threats emerge.

The importance of cybersecurity for SMBs will continue to grow and they need to prepare for these new threats. But at the same time, SMBs need to be sure that they are getting the most value for their security investments.

Today's cybersecurity preparation requires a combination of factors to deal with current threats like ransomware, malware, and phishing. Planning for cybersecurity preparation requires SMBs to reassess the security technologies that they have in place to address today's sophisticated new threats.

Strong passwords and password policies, like the ones supported by Devolutions RDM, provide an essential level of protection by eliminating weak and reused passwords. And implementing a PAM solution, like Devolution's Server, helps to ensure that privileged accounts are monitored and that users have the appropriate levels of security to effectively do their jobs.

It's important to stress security awareness for end users to provoke more secure ways of working. In addition, businesses today need to ensure their supply chains are protected and that the companies they do business with have strong IT security measures and best practices in place.

For more insights into the state of SMB cybersecurity, you can check out the ***Devolutions State of IT Security in SMBs in 2022-2023*** survey report.

Additional Information

For more detailed information about SMB cybersecurity challenges and solutions, be sure to check out Devolutions State of Cybersecurity in SMBs in the 2021 report.

Devolutions