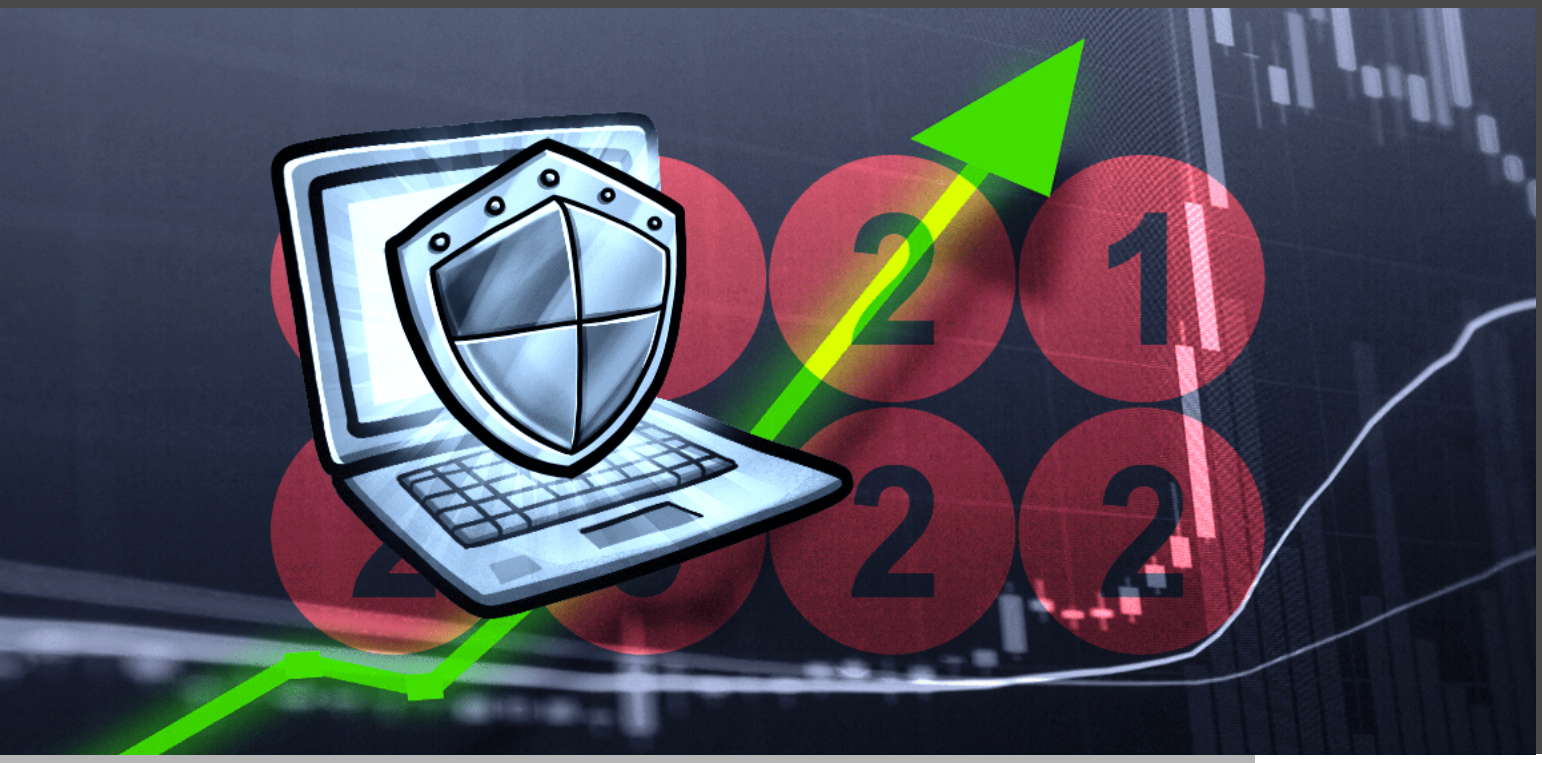
Comparing the Devolutions' 2020-2021 & 2021-22 State of Cybersecurity in SMBs Surveys



WE CAN COMPARE RESULTS FROM THIS YEAR'S VERSION TO LAST YEAR'S VERSION

Now that we have crunched the numbers for the **Devolutions State of Cybersecurity in SMBs in 2021-2022 Survey** (click to download the PDF report), we can compare results from this year's version to last year's version, and glean some valuable and interesting insights.

We identified six key data points that prompted a deeper look, which are related to:

- **Cybersecurity concerns**
- **Most worrisome threat**
- **Password manager usage**
- **PAM usage**
- **Cybersecurity training**
- **Cybersecurity audits**

1. Cybersecurity Concerns

Findings: In the 2021-2022 survey, 72% of SMBs said they were more concerned about cybersecurity now than they were a year ago. In the 2020-2021 survey, 88% of SMBs said they were more concerned about cybersecurity than they had been the year before.

Insight: What this finding suggests is that more SMBs are making efforts and investments to strengthen their cybersecurity posture, which in turn is dialing down their overall anxiety. This is one of the two significant positive developments that the survey identified (the other notable improvement has to do with the frequency of cybersecurity audits, which we discuss later in this article).

However, there is another possible reason for this decrease — and one that provides far less cause for optimism: Over the past year, some SMBs have fallen into a false sense of security because they think they are too small to get attacked. Or, they believe that the pandemic has somehow disrupted the plans and efforts of hackers (just as the pandemic has disrupted virtually everything else).

Unfortunately, both of these assumptions are false. Hackers have stepped up their attacks against SMBs during the pandemic, and they are especially motivated to target SMB remote workers who are often much more vulnerable outside of the corporate network environment.

2. Most Worrisome Threat

Findings: In the 2021-2022 survey, SMBs said that ransomware was the cyber threat they were most concerned about. In the 2020-2021 survey, SMBs said they were most concerned about cloud computing vulnerabilities.

Insight: It is not surprising that ransomware now holds the dubious distinction of being the most feared cyber threat. Consider that:

- Ransomware is expected to attack organizations once every 11 seconds by the end of 2021.
- 20% of ransomware victims are SMBs.
- The average ransom paid out has climbed to $170,704 per incident, and only 8% of victims who pay a ransom get 100% of their data back.

With all of this in mind, SMBs cannot afford to focus exclusively on thwarting malware while neglecting other threats, such as phishing and cloud computing vulnerabilities — including (but not limited to) supply chain attacks. We provide advice on how to proactively defend against these threats in the recommendations section of the 2021-2022 Survey report.

3. Password Manager Usage

Findings: In the 2021-2022 survey, 71% of SMBs said they used a password manager to store passwords. In the 2020-2021 survey, 81% of SMBs said they used a password manager to store passwords.

Insight: Why are 10% fewer SMBs using a password manager now vs. a year ago? The most likely reason is (as discussed above) a mistaken belief among SMBs that they are not as vulnerable as large organizations and enterprises. Another way to look at this is that some SMBs are saying to themselves, "we have not been hacked yet, and therefore the methods that we are using to store and share passwords must be safe and reliable."

As we all know, this belief is not rooted in reality any more than a homeowner or car owner who leaves their door unlocked is somehow safer. It is only a matter of time before this vulnerability is exposed by burglars. Yes, good luck is always helpful. But it is not a cybersecurity strategy!

As we discuss in the recommendations section of the 2021-2022 Survey report, all SMBs — not 71%, not 81%, but 100% — should have a robust password manager in place that has the following:

- End-to-end strong encryption
- Multi-factor authentication (MFA)
- Secure password vaulting (i.e., sharing)
- Strong password generator
- Role-based permissions

4. PAM Usage

Findings: In the 2021-2022 survey, 13% of SMBs said they had a fully-deployed PAM solution in place. In the 2020-2021 survey, 24% of SMBs said they had a fully-deployed PAM solution in place.

Insight: The most likely reason for this 11% year-over-year dip is that some SMBs are turning to password managers as a PAM substitute. While this may seem expedient, it is an enormous mistake!

A robust password manager plays an important role in the overall security mix. But this tool is fundamentally not built to manage access to privileged accounts, and cannot provide the visibility, control, and governance required to:

- Safeguard sensitive data
- Support compliance requirements
- Manage at scale

5. Cybersecurity Training

Findings: In the 2021-2022 survey, 74% of SMBs said they are providing their workforce with cybersecurity training. In the 2020-2021 survey, 88% of SMBs said they are providing their workforce with cybersecurity training.

Insight: Not surprisingly, the most likely root cause for this 14% drop is the pandemic. Dealing with rapid and unprecedented change has forced many SMBs to focus exclusively on core business activities. However, providing their people with cybersecurity training is part of this focus! As noted, hackers have increased the attacks against SMBs during the pandemic. And it only takes a single misguided, negligent, or careless user to trigger a very costly data breach.

6. Cybersecurity Audits

Findings: In the 2021-2022 survey, 50% of SMBs said that they perform at least two comprehensive cybersecurity audits a year. In the 2020-2021 survey, 38% of SMBs said that they perform at least two comprehensive cybersecurity audits a year.

Insight: We started our comparison by highlighting a positive trend, and we can finish in the same way: It is encouraging to see that more SMBs have realized the wisdom of detecting vulnerabilities and gaps on their own — instead of waiting for hackers or rogue/negligent users to do it for them.

Still — and not to be pessimistic, but rather pragmatic — the proportion of SMBs that conduct at least two comprehensive cybersecurity audits a year should be 100%. The most likely reason that half of SMBs are ignoring or downgrading this priority is that they do not have the in-house expertise. In these cases, SMBs are strongly urged to partner with an experienced and reputable MSP for a few key reasons:

- An MSP has the skills and tools to carry out a comprehensive cybersecurity audit.
- An MSP can carry out the audit in a manner that poses minimal/no disruption to day-to-day operations.
- An MSP is a third-party, and as such does not have a bias that could skew findings and recommendations.

In the recommendations section of the 2021-2022 report, we provide advice on what SMBs should look for when evaluating potential MSPs.

Looking Ahead

The most important takeaway for SMBs is that the cyberthreat landscape is getting worse — and the need to be proactive vs. reactive is more vital than ever. Consider that in 2021, the average cost of a data breach in SMBs climbed to a staggering $2.98 million USD per incident.

Establishing a strong, managed, and monitored cybersecurity profile — one that is supported and optimized with the right technologies, tools, and training — is not just an IT priority. It is an organizational necessity.

We invite you to download the Devolutions State of Cybersecurity in SMBs in 2021-2022 Survey report [PDF] for more insights and recommendations on protecting your SMBs' data, customers, and reputation — and making your company's journey ahead safer and more successful.