Devolutions

The State of Cybersecurity in 2021-2022 for SMBs: It's a Good News, Bad News Story

IT'S A GOOD NEWS, BAD NEWS STORY

For the second consecutive year Devolutions surveyed IT decision-makers in small and mid-sized businesses (SMBs) around the world, in order to understand the state of their cybersecurity profile — and ultimately see if it is good news story, or a bad news story.

What did we discover? It is BOTH good news and bad news!

DID YOU KNOW

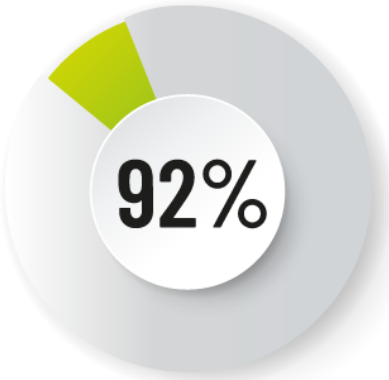
43% of cyberattacks target small businesses.

In 2021, the average cost of a data breach in SMBs has climbed to **USD $2.98 million per incident.**

81% of data breaches are caused by compromised passwords, and **30% involve internal rogue users.**

THE GOOD NEWS

There are some encouraging trends that suggest SMBs are more aware and better protected against cyberattacks. Here are a few of our findings:



of SMBs have a process in place to revoke account access for ex-employees.

74% of SMBs are providing their workforce with cybersecurity training.

****

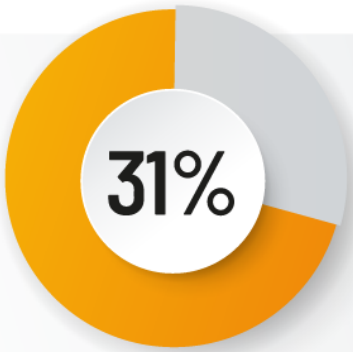
71% of SMBs are using a password manager to store passwords.

> Hackers have increased the attacks against SMBs during the pandemic, and are setting their sights on remote workers who are often much more vulnerable outside of the corporate network environment.

— from the State of Cybersecurity in SMBs in 2021-2022 Report

THE BAD NEWS

On the other end of the spectrum, many SMBs remain highly vulnerable to external and internal cyberattacks. Here are a few of our findings:



Only **31% of SMBs** have a password management policy that covers minimum password length, sufficient password complexity, minimum password history, minimum password age, and mandatory MFA/2FA.

Only **29% of SMBs** are monitoring the full roster of privileged accounts in their company.

Only **13% of SMBs** have a fully deployed Privileged Access Management (PAM) solution in place.

> Not only are hackers targeting SMBs, but they are increasing their attacks for a very practical reason: compared to most large organizations and enterprises, SMBs have weaker — and in some cases, virtually non-existent — defenses.

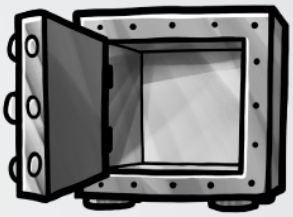
— from the State of Cybersecurity in SMBs in 2021-2022 Report

OTHER INSIGHTS

72% of SMBs are more concerned about cybersecurity now compared to a year ago.

52% of SMBs experienced at least one cyberattack in the last year, and 10% experienced more than 10 cyberattacks.

32%



of SMBs have experienced privileged access violations in the past year.

> SMBs need to keep hackers from invading their endpoints and networks. But at the same time, they must prevent internal users — both those who have "gone rogue"and those who make honest mistakes— from improperly accessing privileged accounts and acquiring or releasing sensitive information.

— from the State of Cybersecurity in SMBs in 2021-2022 Report

RECOMMENDATIONS

1. SMBs need to realize they are not “too small to be attacked”.

2.

SMBs need to proactively protect themselves from the “big 3” cyberthreats: ransomware, phishing, and supply chain attacks.

3.

SMBs need to implement a comprehensive and effective incident cyberattack response plan.

4. SMBs need to implement a password manager solution with the right features and functions.

5.

SMBs need to implement a robust password policy.

6.

SMBs need to implement an effective access deprovisioning process.

7. SMBs need to implement a Privileged Access Management (PAM) solution to bridge the gap between authentication & authorization.

8. SMBs need to protect, monitor & update all privileged accounts.

9. SMBs need to implement 4 essential security principles: principle of least privilege (POLP), segregation of duties (SoD), zero-trust, and defense-in-depth.

10. SMBs need to improve their workforce's cybersecurity awareness.

11. SMBs need to keep remote workers from becoming "the weakest link" in the cybersecurity defense chain.

12. SMBs need a comprehensive cybersecurity audit process.

13. SMBs need support from managed service providers (MSPs) to close the cybersecurity defense gap.

14. SMBs need to increase the proportion of their IT budget that is allocated to cybersecurity.

15. SMBs need to focus on 5 security projects in 2021-2022: secure remote access management, secure digital vault, secure password management, multi-factor authentication (MFA), and automation.

Sources:

https://www.ibm.com/security/data-breach

https://www.einnews.com/pr_news/533310673/global-cybercrime-damage-costs-will-reach-11-4-million-per-minute-in-2021

https://www.cybintsolutions.com/cyber-security-facts-stats/

https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Devolutions
WHERE IT MEETS SECURITY