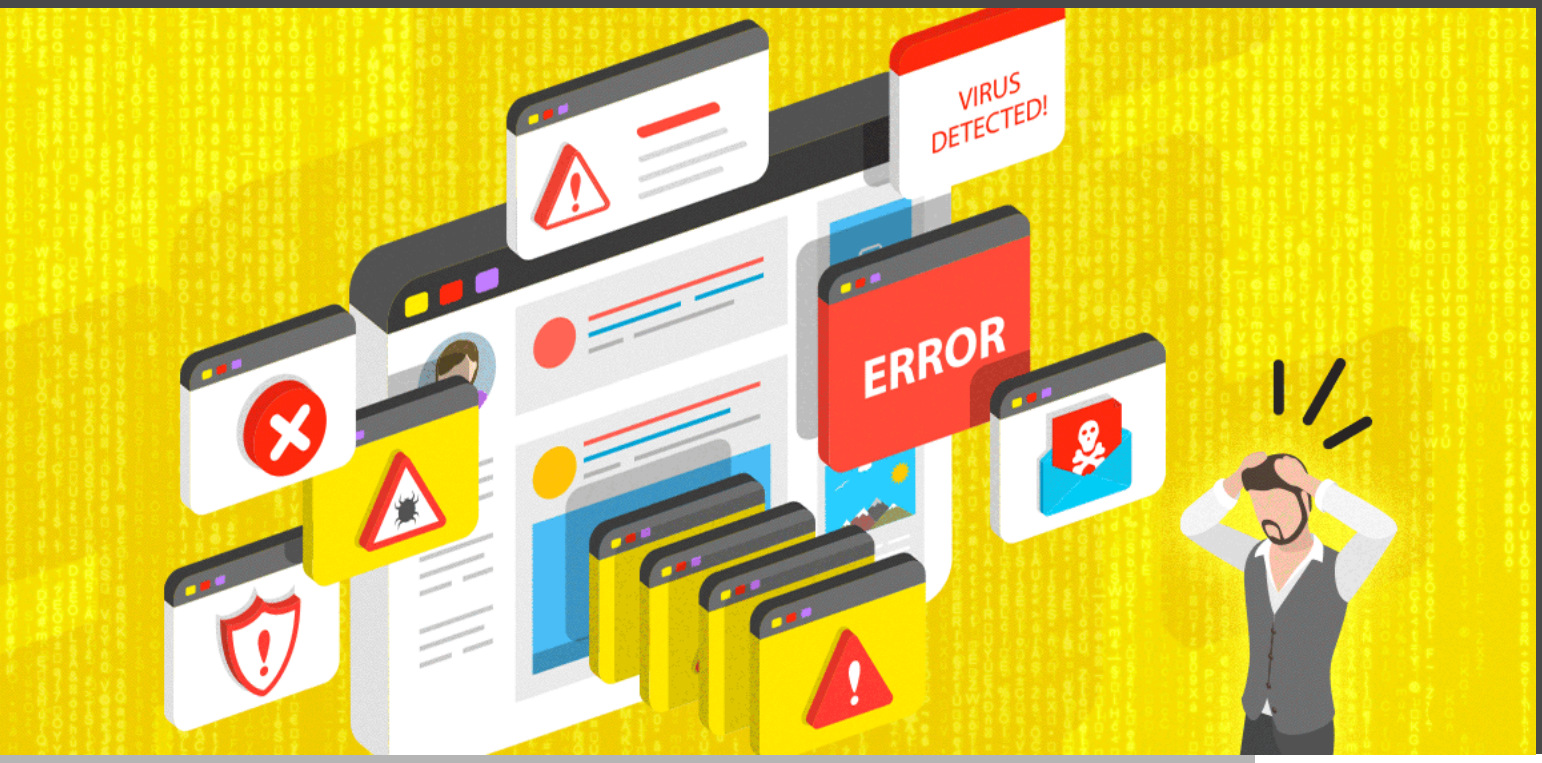
Devolutions

5 Common Cybersecurity Mistakes SMBs Make — and How to Fix Them



MANY SMALL AND MID-SIZED BUSINESSES (SMBS) HAVE SOME CYBERSECURITY-RELATED REGRETS

Legendary crooner Frank Sinatra — and a countless number of inebriated wedding guests who fancy themselves as karaoke superstars — have grabbed the mic and belted out the classic song My Way, which includes the line: "Regrets, I've had a few, but then again, too few to mention."

Well, these days, many small and mid-sized businesses (SMBs) have some cybersecurity-related regrets. But instead of being too few to mention, they are too enormous to ignore. The average cost to investigate and clean-up a breach in an SMB has surged to over $200,000 per incident, and 60% of SMBs go out of business within six months of a cyberattack. Heck, even a fearless warrior like Sinatra would shiver at these statistics.

However, there is some good news: SMBs can proactively strengthen their cybersecurity defenses, and dramatically reduce the likelihood and severity of attacks. To that end, here are five common cybersecurity mistakes that SMBs make — and how to fix them.

1. Thinking they are "too small" to get attacked

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.

As such, when it comes to cybersecurity threat exposure, the first and most important thing SMBs must accept is that their relatively small size is not an advantage. It is actually a liability, because hackers will assume they are vulnerable. It is up to SMBs to demonstrate otherwise, or else it is not a question of if an attack will occur. It is a matter of when and how severe.

2. Not using multi-factor authentication (MFA)

When MFA first arrived on the scene many years ago, it was a difficult product for many SMBs to implement because tools were expensive and difficult to configure. On top of this, end users were either reluctant to adopt it because it was an extra login step that they didn't like, or they didn't have a personally-owned or company-supplied smartphone (these days smartphones are cheap and everywhere, but that hasn't always been the case!).

Now, however, there is no reason — or excuse — for SMBs not to implement MFA, which Microsoft considers "the most effective tool against cyberthreats within an organization." Many robust and credible MFA tools are affordable, and some, such as Devolutions Authenticator, are free.

Does this mean that MFA is bulletproof? No, it doesn't. Sophisticated cyber criminals can hack MFA through tactics like phishing emails, SIM swaps, man-in-the-middle attacks, or even by rebuilding the password generator. However, despite these possibilities, MFA should be seen as mandatory instead of optional. Think of it like securing a home: highly experienced burglars can, given enough time and with the right tools and plans, break into any home. But this doesn't mean that people should leave their doors and windows unlocked. MFA does not totally eliminate the risk, but it certainly mitigates it — and that is a step in the right direction.

3. Poor password management practices

One of the key advantages that SMBs have over large organizations is that they are nimble and agile, because excessive bureaucracy can be fatal. However, sometimes the drive for efficiency can be dangerous instead of profitable, and there is no greater (or worse, if you prefer) example of this than poor password management practices. For example, the Devolutions State of Cybersecurity in SMBs 2020/2021 Survey revealed that:

- 57% of SMBs do not believe that enforcing a minimum password length policy is very useful.
- 47% of SMBs allow end users to re-use passwords across personal and professional accounts.
- 29% of SMBs rely on human memory for storing passwords.

While there are several things that SMBs can — and frankly, must — do to improve password management hygiene, the most essential and high-impact practices include the following:

- Implement MFA (as discussed earlier).
- Use a reliable and credible password management tool (click here for a comparison of various popular options).
- Use a secure vault for password sharing.
- Use passphrases.
- Change passwords after evidence of a compromise.
- Compare passwords against a list of known weak and compromised passwords.
- Eliminate password re-use.
- Enforce a password history policy.
- Enable copy/paste passwords.
- Enroll end users in a cybersecurity training platform.

4. Not auditing and monitoring privileged accounts

As noted by international and independent analyst organization KuppingerCole Analysts: "Privileged accounts are given to admins and other users within an organization to access critical data and applications. However, if these are not managed securely, SMBs can find themselves having accounts still open for people who have left, or for people who no longer need access or simply giving too many people privileged accounts."

And so, how can SMBs follow this advice and securely manage their privileged accounts? The answer is to implement a PAM solution that checks all of the following boxes:

- Easy to deploy and manage.
- Available in multiple licensing models and affordably priced.
- Provides a secure password vault.
- Supports comprehensive logging and reporting.
- Features built-in 2FA.
- Supports account brokering (i.e. authorized end users can log into accounts/access network areas, but without needing to see passwords).
- Supports role-based access to credentials.
- Backed by responsive technical support.

5. Trying to do everything in-house

The funny thing about job titles in SMBs is that nobody ever has just one. Sure, they may have something like "Project Manager" or "Software Developer" on their email signature and business card, but in reality they perform various roles and wear multiple hats. That is just how things go in the SMB world. Everyone must be flexible and versatile.

However, there are scenarios where it is necessary to get some outside help. For many SMBs, this means working with a Managed Services Provider (MSP) to relieve the impossible burden placed on their "IT Guru" who, in addition to managing the infrastructure, is tasked with running the cybersecurity program. An MSP shoulders some of the load and fills in the gaps — which makes the difference between having a strong defense and being vulnerable to attack. Click here for tips on how to choose the right MSP.

The Bottom Line

As we have been dramatically reminded during the pandemic, SMBs are the backbone of the economy. For example, in the U.S., SMBs generate 66% new jobs and deliver 43.5% of GDP. And in many other countries, the impact is even greater. In Canada, SMBs represent over 99% of the economy, and employ almost 90% of the total private labor force.

However, to remain strong and optimize growth potential, SMBs cannot just focus on their marketplace and supply chain. They also need to pay attention to their cybersecurity profile, and if necessary, make some rapid and essential improvements. Waiting until "something bad" happens before taking action is unwise — because by then, unfortunately, it may be too late.