BIZCOMMUNITY

8 important ways to improve security in your business

By Craig Lebrau , issued by Lebrau Press

8 Mar 2021

Cybersecurity is one of the most important strategies for modern businesses. Without the right cybersecurity upgrades, your business could fall victim to any one of several schemes and attacks, ultimately, failing your customers, your personnel and your stakeholders.

Image credit: FLY:D on Unsplash

Fortunately, while cybersecurity is complicated, the most powerful tactics for improvement are both simple and accessible. Even businesses with limited knowledge, experience and resources can take advantage of them.

Why is cybersecurity important?

Cybersecurity is important for several reasons:

- **Legal compliance.** In some industries and in some areas of the world, cybersecurity is a legal requirement. You may be required by law to keep your customers' data secure or be compelled to keep certain files safe.
- **Financial risk mitigation.** A data breach can cost a company an average of $3.9m. The cost to recover data, repair damage and effectively manage the situation can be exorbitant. It's much more cost-effective to prevent this from being a problem in the first place.
- **Reputation management.** A data breach or similar cybersecurity problem can cost your business dearly in terms of reputation. Investing in cybersecurity will help keep your company's image in good standing.

Important ways to improve security in your business

So what are the best ways to improve your business's digital security?

1. **Choose stronger platforms.** Your first job is selecting the right platforms for your business. Chances are, your business relies on dozens, if not hundreds of cloud-based platforms and third-party software tools to operate

efficiently. Each of these tools is a potential vulnerability, so you need to do your due diligence and ensure that these software developers are doing everything possible to keep your data secure.

2. **Backup your files.** As the ultimate failsafe, it's vital to backup your files in the cloud regularly, and preferably on an automatic basis. That way, if your company is ever the victim of a ransomware attack or another breach that renders your systems inoperable, you can revert to a previous instance and avoid losing any precious data.
3. **Select strong passwords.** Oftentimes, hacks and breaches aren't the result of a brute-force attack, instead, they're the result of a common, weak password that was easily guessed or discerned. It's important to choose strong passwords for all your platforms and all your users, with a diverse mix of upper-case letters, lower-case letters, numbers and special symbols. You also should never use the same password twice.
4. **Avoid common phishing scams.** Cybercriminals frequently use phishing schemes to lure users into voluntarily forfeiting their login credentials or giving up other valuable information. These scams are easy to spot if you know what to look for, so familiarise yourself with the approaches that are most common – and avoid them at all costs.
5. **Secure your network.** If a cybercriminal gains access to your network, they can hypothetically gain access to all your inbound and outbound traffic. The tragedy is that it's remarkably easy to set up a more secure network. It's also important to have a solid bring your own device (BYOD) policy in place, so your employees don't introduce new vulnerabilities by bringing their own devices from home.
6. **Use firewalls and VPNs.** Firewalls are designed to help your organisation filter out potentially harmful sources of traffic – and prevent your employees from accessing inappropriate or dangerous types of content. Virtual private networks (VPNs) can allow for secure remote access. These tools aren't foolproof, but they can provide you some additional layers of security.
7. **Watch for social engineering tactics.** Some 'hackers' bypass the technological route altogether, and instead focus on social engineering tactics. They may call your employees, pretending to be an official representative of a company you trust and ask for their login information. Despite its simplicity, this is one of the most effective tactics – and one you should be specifically prepared to guard against.
8. **Train your employees.** Remember, each member of your team is another vulnerability and another potential source of a breach. Your organisation is only as strong as its weakest member. Accordingly, it's important to invest in ongoing employee training, providing employees with the knowledge, guidance and tools necessary to defend themselves against the most common types of attacks.

There's no such thing as a 'hack-proof' business and these strategies are just the beginning of a more robust, advanced cybersecurity approach. However, most cybercriminals are unskilled opportunists, looking to prey on easy, common targets; even the simplest security measures are often enough to deter these would-be thieves.

Seeking professional advice

If you want to upgrade and support a more comprehensive cybersecurity strategy, your best option is to seek professional advice. Consider hiring dedicated security staff or working with a security consultant to find the best strategies for your business.