Common Pitfalls to Business Security and How to Address Them

SmartVault

We hear about high-tech security breaches all the time. Ransomware, encryption malware, elite hackers, and cyber warfare make for great news. The related news segments typically use a lot of tech jargon and leave business owners fearful. After all, how can you protect yourself against threats you can barely understand?

However, day-to-day business security is much more down-to-earth and understandable than you think. You are far more likely to lose your data to poor security practices within your company than to any high-tech attack from the outside.

Here are the most common pitfalls to business security and how you can address them.

Lacking employee training

Poor security protocols are the most common reason for data breaches. These can be predatory (i.e., an employee falls for a phishing attack) or opportunistic (i.e., an employee using unsafe passwords).

The good news is that training your employees in a simple set of best practices will prevent over 90% of breaches from happening. Training is vital for non-technical staff that nonetheless need access to data. Your software developers are unlikely to fall into online traps, but your customer service reps or your accountants might make better targets.

In the simplest terms, your employees should always:

1. Use safe passwords.
2. Use multi-factor authentication.
3. Log out of devices when leaving them unattended.
4. Avoid connecting through unsafe networks.

An essential part of training is preparing to fail - meaning your security system should assume that mistakes will happen and demand an extra step from intruders. In that regard, it's crucial to insist on multi-factor authentication across the board - this significantly limits the danger of a careless employee sharing their password.

Single points of failure

Most prudent business owners know better than to allow single points of failure in their technology stack. Common sense tells us to avoid having a single piece of hardware/ software that our entire business depends upon.

But many make the mistake of allowing single points of failure in their personnel. Is there a person in your company whose illness or resignation would make you unable to maintain your business's day-to-day operations? If yes, have this person train a potential replacement or two, and make sure no piece of data is locked away somewhere where nobody else can find it.

> Note: this includes yourself and any other owners/directors.

Unnecessary complexity

Even the best employees make mistakes in a complex enough environment. Complexity makes errors more likely, rules more ambiguous, and breaches a matter of time.

Your data access policy should ideally be simple enough to be displayed in a single Excel sheet. You can use the columns to display tiers of data (confidential, sensitive, public, etc.) and the rows to indicate types of employees.

Thus, we can see at a single glance what level of access each employee should have and give them the appropriate credentials and training. The simpler, the better.

Access should be assigned sparingly on a need-to-know basis. The less data each employee can access, the smaller the effect of a potential breach.

Physical security

You do everything right: you backup your data, you train your employees well, you have a strict data access policy, you're vigilant, and you keep up with technological advances.

Then, one day, a disgruntled employee sticks a USB drive in your server and walks out of the door with all the data your company has been carefully safeguarding.

Maybe one of your computers needs to go to a 3rd-party company for repairs, and anyone there can extract your precious data from the machine.

The lesson here is that restricting access to the hardware is just as important as software security. User terminals should log any attempt to copy data to external devices and notify the relevant personnel immediately. Broken machines should be fixed on-site with supervision - or simply retired. This issue isn't a calamity if the machine in question isn't a single point of failure like we discussed above.

No disaster recovery plan

Let's up the ante. Instead of a machine breaking down, what if there's a natural disaster and your entire office is destroyed?

Such black swan events often find businesses completely unprepared. To minimize damage to yourself and your customers, prepare a disaster recovery plan.

First, set a goal for your company: how long should it take to be fully operational after a disaster? Think about what sort of downtime your customers can tolerate. If you're a financial institution, this time window is dramatically shorter than if you're a landscaping company.

Then, implement processes and fail-safes that will make that goal reachable. Always keep your data in the cloud and back it up regularly. Ensure that new devices can be configured to access the data safely and ensure your employees know what to do. Redundancy saves the day again.

Summary

The world of business security is complex. It is continually evolving and requires effort to stay up-to-date; on the other hand, the primary security paradigms never change.

Many business owners make the mistake of focusing too much on advanced threats and too little on basic principles. We hope that this article can help you define a structured approach to security that can be used as a strong foundation for whatever threats arise in the future.

Some parting tips:

- When your employees work from home, assume they're working from public places like coffee shops and airports. Make sure you factor this into your security training.
- Redundancy is crucial, but it can create security loopholes in the sync/backup process. Approach the security of your backup/fallback systems with the same rigor as your primary system.
- Don't let overconfidence be your downfall. Apply the same rules to yourself as to your subordinates.
- Don't assume that hackers only target major corporations. Around 70% of small businesses experience data breaches at some point.