


TECHNOLOGY INSIDER



Is it time to be more like Alex?

Here's a story about a business owner named Alex. Alex runs a successful marketing agency, and business has been booming. But with growth comes growing pains, and Alex has found himself increasingly bogged down by IT issues.

At first, Alex tried to handle everything himself. After all, he was pretty good with computers. And for a while it seemed to work. Alex managed to fix minor issues and keep things running.

But then, one Monday morning, disaster struck. Malicious software had infected the company's main server, crippling their operations. Alex spent days trying to fix the issue, losing valuable time and money in the process. It was a wake-up call: Doing it himself wasn't a sustainable solution.

Determined to avoid another disaster, Alex decided to train his top employee, Sarah, to handle IT alongside her regular duties. Sarah was smart and quick to learn, but the additional responsibilities quickly became overwhelming. She found herself stretched too thin, and her productivity in her main role started to suffer. Not to mention, the fast-paced tech world was hard to keep up with, and soon, Sarah felt like she was drowning in a sea of updates and security threats.

Realizing this wasn't working, Alex considered hiring an in-house IT team. But the costs were daunting. Recruiting skilled professionals, providing ongoing training, and equipping them with the right tools would require a significant investment. For a mid-sized business, this was a heavy financial burden.

That's when Alex discovered the benefits of outsourcing IT. He found a reputable IT service provider with a team of experts ready to step in.

Here's what Alex found:

- 1. Expertise on tap:** The outsourced IT team brought knowledge and experience. They were always up to date with the latest technologies and security threats, making sure the agency's systems were secure and efficient.
- 2. Cost savings:** Instead of paying salaries and benefits for a full-time team, Alex paid a monthly fee based on the services he needed. This was a much more affordable solution.
- 3. Focus on core business:** With IT taken care of, Alex and Sarah could focus on what they did best – growing their business. Productivity soared, and so did their client satisfaction.
- 4. Scalability:** As the agency continued to grow, the outsourced IT team easily scaled their services to meet the increasing demands. No need for Alex to worry about hiring more staff or buying new equipment.

By outsourcing IT, Alex not only solved his immediate problems but also set the stage for sustainable growth. The agency was now protected from cyber threats and was running smoothly, all without the hefty price tag of an in-house team.

Alex's story is a great example of why outsourcing IT is a smart move. It frees up time and resources, allowing you to focus on what you do best, while experts handle the complexities of IT.

So, if you're still trying to juggle IT responsibilities with other tasks, consider taking a page from Alex's book. We can help you with that, get in touch.

**DID YOU
KNOW...**

**CYBER
EXTORTION HAS
INCREASED BY
108%**

Cyber extortion is when cyber criminals threaten to damage, steal, or expose a business's digital data unless a ransom is paid. **And the number of victims has grown 77% year on year.**

In the US attacks have risen by 108% **and any business of any size is targeted.**

To stay better protected, the usual advice applies: Make sure all software is up to date, back up your data, and implement multi-factor authentication (where you get a code on another device to prove it's you).

Cyber security is a team effort

There are loads of important things you need to think about for your business. Loads. But we're adding another one to your list: Cyber security awareness.

You'd be forgiven for thinking this is an IT problem; something for them to sort out. Sorry to say, but you're wrong. It's something that every single person in your company needs to be on top of, from the big boss to the latest hire.

You see, cyber threats are always changing and getting more sophisticated. A one-time training session just won't cut it. You need to keep everyone in the loop with regular updates. Think of it like this – in the same way you need regular check-ups to stay healthy, your team needs regular cyber security training to keep your business safe.

What does this training look like? There are a couple of ways to do it. First, there's the good old traditional method – you know, lectures and presentations. One way training. These are great for laying down the basics and introducing new concepts. But let's be honest, they can be a bit... boring.

That's why it's a great idea to mix in some interactive training too. Imagine phishing simulations where your team learns to spot fake emails before clicking on them. Or hands-on workshops where they can use the security tools and protocols they've been hearing about. These methods are not only more engaging but also help the info stick better.

Combining these traditional and interactive methods is where the magic happens. Start with some solid grounding through presentations, and then get everyone involved with practical exercises. This way,

Business gadget of the month

Flexispot Electric Standing Desk

We all know that sitting down all day is no good for us, but when you have an office job, it's unavoidable. Or is it?

The Flexispot Electric Standing Desk lets you stand while you work, making it easier to move around and giving your posture a boost too.

It has a silent motor, is quick to assemble, and has a digital keypad that allows you to add height presets (including a sitting position, of course).

\$239.99 from Amazon.



the knowledge isn't just in one ear and out the other – it's learned, remembered, and applied.

Let's talk frequency. Since cyber threats are always evolving, training shouldn't be a once-a-year thing. Regular sessions throughout the year will keep your team sharp and ready to handle anything that comes their way.

Creating a strong cyber security culture in your company is key. This means making cyber security everyone's responsibility. Encourage a culture where if someone spots something fishy, they speak up right away. Communication is super important here.

And remember, this starts at the top. If the leaders in your company are taking cyber security seriously, everyone else will too. So, make sure the big shots are not only participating in the training but also showing how important it is. Lead by example, right?

Cyber security is something that affects the whole business. Every email, link, and password matters. By making sure everyone is trained and aware, you're building a strong first line of defense against cyber threats.

We can help you get your team started - get in touch.



Q: Should I let my employees use company apps on their personal phones?

A: Ideally not, because you have less control over the security of personal devices. If they need to work on a phone, better to provide a company-issued one.

Q: Should I ban my team from working in coffee shops because of public Wi-Fi dangers?

A: You don't have to. Just make sure they're aware of the risks of using public Wi-Fi and that they're vigilant when connecting to new networks.

Q: Should we delete phishing emails, or should they be reported?

A: Any spam or phishing emails should be flagged as such because it teaches your email provider what spam looks like. You can also forward it to the Federal Trade Commission reportphishing@apwg.org

This is how you can get in touch with us:

CALL: +1 604.992.8178 | **EMAIL:** hello@lcsnetworks.com

WEBSITE: lcsnetworks.com

leap Cloud Solutions®