THE TRUE COST OF NOT IMPLEMENTING AN I.T. SECURITY STRATEGY

KJ TECHNOLOGY

www.kjtechnology.com

You're at that point where you've had to change office passwords so much that you're considering using swear words. We all become frustrated when our office computer passwords have to be changed. We all groan at the office firewalls slowing things down. All of us get irritated with our office IT security measures. But at the end of the day, we know we still need them, and our frustration is brief – as long as we can continue working.

Firewalls, antivirus measures, password changes and the like are good for day-to-day protection and fending off the low-level phishing scams. What about cyber espionage and fraud – what about those phishing scams and ransomware that are more sophisticated? Most small to medium-sized businesses create an IT security system on an ad-hoc basis. This is good enough to get by on initially, but it won't be enough to protect your business from the more aggressive or unpredictable threats.

Many businesses don't have a complete disaster recovery plan!

It's common for business owners to think they are unlikely to experience a major IT security breach. Major security breaches like fraud and cyber espionage don't happen every day. But they do happen precisely because of a primarily reactive approach to network security. When they happen to you, it only takes one major breach to bring your business to its knees.

This can cost thousands of dollars to undo, and by then it may be too late. Doing business without an IT security plan won't hit you just once. This will continue to plague your business over and over again.

Impact on Your Employees

Your employees are your greatest asset. Without them the business does not run. Naturally, there will always be a turnover in your staff as someone finds a job where they fit in better or that aligns more with their interests or work schedule. Whatever the case, workers come and go and you hire new staff members. But you care about all your employees – they're motivated and they keep your business competitive, because they know you care.

What happens to your team when your IT security isn't up to par? Security breaches will happen, and when they do your employees' livelihoods and personal information are compromised. You can fix it once, but it keeps happening. More and more employees become dissatisfied and leave your company. They may review your company online or by word of mouth, and what they have to say is not kind. Finding the most qualified staff is harder when no one is interested in working for a business that puts employees' IT security at risk.

Especially if you're a small to medium-sized business, every single one of your employees is essential to running a profitable organization. You cannot afford to lose their contribution or their trust. Making sure you have a proper IT security strategy in place is the right way to maintain their confidence and provide the protection they deserve. Your employees will know you care, and potential hires will know too. Your ability to keep everyone safe will help you maintain business growth and stay competitive.

The Cost of Fixing IT Networks without a Security Strategy

Let's talk money!

If your plan for IT security is created on an ad-hoc basis, you probably have not hired a managed services provider to deliver proactive security solutions. This means that you are fixing breaches in your IT network after they happen, or you are paying an IT service that charges for on-demand repairs. When you have to take time and staff from your business operations to address problems with your cybersecurity – that's slowing you down and costing you money.

> **It's common for business owners to think they are unlikely to experience a major IT security breach.**

Without a proper IT security strategy hacking attempts will continue. Hackers will find new ways around the hole you patched and then they will find a way around that patch...

Hackers are already a step ahead of your commercial antivirus product!

If you are using an IT company who charges for as-needed services, your business is spending even more time and money on the problem. An on-demand IT service provider is in the business of fixing IT breaches, not preventing them. The more holes in your IT network, the more money it makes them. Before you know it, you are beholden to an IT service that isn't really helping your business.

Without a proper network security strategy, you will continue to be constantly under the threat of malware, ransomware, phishing and human error. This will keep stalling your business week after week, draining your capital. Your staff will struggle to keep up with the churn, and an on-demand service provider will keep you in a state of constant semi-repair and potential risk.

What Is the Extent of a Major Network Breach?

A data breach itself can cost you big financially, and the cost can be immeasurable in terms of reputation and customer loyalty. Besides the cost of repairs, a data loss event introduces a risk of losing customers. No one wants to do business with a company that has poor IT security and cannot protect their data.

Pretty soon there could also be government fines for not achieving proper compliance, and potential lawsuits from clients and employees. Paying damages for lost information, marketing/PR campaigns to make it go away, and depending on the state you are doing business in (New York among them), you may be required to notify clients of a data breach, at your own expense. The financial cost of a data breach can snowball quickly and it's not unheard of for a loss in the thousands to reach into the millions of dollars. The bottom line is that your business cannot afford to operate without an IT security strategy.

Implementing the Right IT Security Strategy

The risks are too great to delay implementing a full-circle approach to IT security. A major security breach will happen at some time: Studies show that a business will experience at least one major security breach, like cyber espionage, in its lifetime if it is not properly protected.

A managed IT service provider can help you develop and roll out an IT security strategy that is custom-suited to your business. You won't have to worry about whether you are in compliance with key regulations or about monitoring your network 24/7. A managed IT services firm does all of that for you. Your network will be protected, your employees will remain productive, you will save money in the long run, and your business will continue to grow without the worst kind of interruptions.

So when you're looking to implement an effective IT security apparatus, give KJ Technology a call. We will work with your company to make sure that your business is protected and prepared for any eventuality. Your business deserves that.

247 West 36th Street
5th Floor
New York, NY 10018

646-556-6500

www.kjtechnology.com

KJ
TECHNOLOGY