Business owners guide to protecting client data.

Many business owners believe they are too small to be at risk of cyberattack. You take basic precautions to detect and protect but don’t believe you’re really a target. Yet that’s forgetting the value of your client data. The personal identification information (PII) clients share is a goldmine for bad actors, and it’s critical that you do all you can to protect client data. This eBook outlines the threat and explores cybersecurity action you can take.

The importance of protecting any proprietary data is obvious to most businesses. Yet too many businesses underestimate the value of protecting the confidential, sensitive data of prospective and existing clients.

Yes, small businesses are targeted. Your business is a hub of information cybercriminals could use to steal funds or identities. Simply consider the number of different accounts someone could access or open by confirming they are your client using that ill-gotten birthdate and address.

Your profession has an ethical duty not to reveal client information without that person’s informed consent. What would you say if your clients’ information was freely available on the internet?

Your business holds the keys for many kingdoms to cyber bad guys. Depending on your niche, and who your clients are, that stolen data could also be used for blackmail purposes.

The Risk is Real

Hackers know small businesses spend less on cybersecurity, so they often make a better target than Fortune 500 enterprises.

Small businesses are attacked at an alarming rate, because many of them have outdated software. Some small businesses develop proprietary systems. Then, there are no updates after the IT staffer who set it up leaves the organisation. Perhaps your office has a system that works, so there’s no incentive to fix it. Those upgrade and security patch notifications? You don’t have the time for that, or you don’t want to invest the funds in the latest version.

However, hackers are highly motivated. You might think of hooded individuals furiously typing away to break down firewalls. But it’s not even that hard.

Cybercrime gangs are using automation to scan millions of computers. They probe for vulnerable networks until they get a hit. Then, they go to work dismantling your business.

Small businesses are at risk of cyberattack, because it is so easy. Plus, the payoff can be a big one.

The Cost of Client Data Loss

You might think, “it’s one little breach, so how bad could that be?” The answer is pretty bad. Consider these significant ramifications:

Lost Revenue. Losing significant revenue is a common effect of a security breach and is common. Consider the revenue you could lose while your website is down and employees can’t access the IT system.

Damaged Reputation. Sure, you may want your business to get more publicity, but landing in the news for a data breach is not going to help.

Prospective and current customers will be reluctant to trust a business with a history of shoddy data security.

Hidden Costs. The loss of revenue will be a hit. Still, you could also encounter costs such as regulatory fines, legal fees, and more; or your business may have to pay higher insurance rates or invest more in marketing to combat the bad press.

According to CloudRadar, more than half of businesses need more than one hour to recover. On average, every hour the business is down costs over £7,000. That can add up quickly!

What Can You Do to Protect Client Data

OK, so you now know you need to protect your client data. The question is how do you do it? These strategies can help.

#1 Keep software up to date

Regularly maintaining your software is a strong security measure. The latest updates often include new code to address known security threats. If you can’t or don’t keep your software current, at least take it offline.

#2 Ramp up network security

Firewalls, antivirus software, and intrusion prevention systems should address every network layer. Encrypt any stored or shared electronic files and documents, both at rest and while in transit.

#3 Limit access to data

Not everyone in your business has the same needs for data access. Limit information access to an as-needed basis. Determine who has what responsibilities and the information they need to access, then assign appropriate access privileges based on their role.

#4 Educate employees

Everyone working at your business needs to understand the value of your client data. You can't expect someone to effectively avoid phishing scams and other social engineering tactics if they don't understand the danger.

Share best practices for internet use. Put policies in place for sharing, storing, and disposing of client data. Require employees to report lost and stolen devices, and make sure every person at your office is maintaining strong passwords. And please don't let anyone keep their password on a Post-It note stuck to their desktop!

CONCLUSION

Given how sensitive your client data can be, your cybersecurity can’t be an afterthought. The risk is real, and the damage could be serious. There are several actions you can take to ramp up your security. You might also turn to a Managed Service Provider (MSP) for help.

As a business owner you know how to do what makes your business great. MSP experts have the tech knowledge needed to handle network setup and tech support. They also deal with the upkeep of your IT systems. Our team can offer the solution to better defend client data against cyberattacks.

Your IT Department

Unit 8 Farrington Way
Eastwood
Nottingham
Nottinghamshire
NG16 3BF

T: 0115 822 0200
E: info@your-itdepartment.co.uk
W: your-itdepartment.co.uk

Follow us on social media: