The biggest security threat to your business is on your payroll

TeamLogicIT
Your Technology Advisor

Revealed:

The real cost of insider attacks – and your strategy to prevent them

Someone working for you right now is also working alongside some of the world's most successful cyber criminals.

And before long, they're going to take down your business from the inside. They'll put your sensitive business data in the hands of your number one enemy.

Where does this leave your business?

Potentially held to ransom to regain control of your data.

Perhaps losing all your data for good.

And having to explain to your clients that their personal information has been stolen...

It sounds like the plot from a movie, doesn't it?

While it could make a great edge-of-your-seat thriller, sadly, this is a very real threat to you and your business.

REASON ONE: The most common reason is that an employee of yours is an accidental double agent.

Their lack of cyber security training means they don't notice the warning signs of a phishing email, dangerous attachment, or spoofed web page. That training gap leads to a click on a bad link, which leaves you open to attack.

This is what we call insider negligence.

REASON TWO: This next reason is scarier – you do have a malicious insider. Someone who is working for you and knows the value of your data.

They know the weaknesses in your business's cyber security, and they know how to access your sensitive data. The motivation of a malicious insider is usually financial gain, but sometimes they may be disgruntled and out for revenge.

REASON THREE: Finally, we have imposter theft. This is what we call it when someone has access to your credentials and uses them to access your business's sensitive data.

~~Credential theft can be the costliest form of attack to recover from.~~

In fact, the cost of an imposter theft can average $871,000 or more. That's almost three times the cost of insider negligence, at $307,000, and even more than a malicious insider attack, at $756,000.

These figures are PER INCIDENT. The expense to defend and recover quickly racks up thanks to monitoring and surveillance, investigation, escalation, incident response, containment, post-attack analysis and remediation.

Just think about what an attack like this would mean for your business.

As loyal as your team are, and as much as you think they know about cyber security, as business owners, we simply can't afford to think like this. Because the threat of an insider attack is very real and incidents are rising year on year.

IBM recently carried out a study of 204 organisations in the United States. Over 12 months, this small group of organisations saw 4,716 insider attacks.

of these attacks were due to insider negligence

were down to malicious insiders

related to credential theft

Businesses with fewer than 500 employees spent on average $7.68 million dealing with the consequences of insider attacks.

So what can we, as business owners, do to prevent and minimise this kind of attack?

Our recommendation would be to create an insider threat strategy. Follow it to the letter and you could instantly minimise the risk to your business.

There are five key areas that must be in your strategy. Just remember every business is unique. To create a bespoke strategy, consult with a trusted IT support partner (hey, we can help with this).

Key area 1: Ongoing education

Training your team is at the core of avoiding negligent insider attacks.

It's absolutely essential that everyone does the training, from the most junior member of staff right up to your CEO. This demonstrates to everyone that senior management is taking their responsibilities seriously.

But also, we find that senior management are most likely to make technical mistakes. Sorry, but it's true! And because they have access to the most data, they are more likely to be targeted by hackers.

Cyber security training isn't a one off thing. Cyber attacks are becoming increasingly sophisticated. Criminals will take advantage of any situation; be it the global pandemic, a change in legislation, or simply a new tax year.

They will tailor their attempts to fool you and your team in any way that they can, and you all need to be aware of the red flags to look out for.

Key area 2: Tailored, multi-layered security

Of course, you need security software. You're being trusted with the private data of your clients and employees.

Realistically, off the rack security isn't going to cut it. You need security that's tailored to your business, the apps and software you use, and the way you use them.

And this will be different for every single business. Following the recommendations of an IT expert is essential to give your data the protection it really needs.

We would highly suggest that you look into multi-layered security too. Different software that works together to create a higher level of security is the best way to keep your data as safe as possible. Implement multi-factor authentication across your apps, where you generate a login code on a separate device. And consider using biometrics across your devices, such as fingerprint scanners.

Consider the risk that lost or stolen devices pose to your business too, and the ways that encryption and wiping data remotely will benefit you.

Key area 3: Restrict access

Do you know who has access to which files within your business? Can everyone access everything, or are your files accessible only by those who really need them?

According to a 2019 global data risk report, 53% of employers found to their horror that more than 1,000 sensitive files were accessible by every employee in their business.

The more people that have access to a file, the more likely it is the file will be breached.

Restrict file access to those who need it. Make sure files are always encrypted. And consider password protection for the most sensitive files.

Don't forget the external partners who may have access to your data.

Key area 4: Business exit protocol

We know that some insider threats are malicious. It's sad, but true. And a percentage of these malicious attacks are carried out by disgruntled employees who will soon be leaving the business.

So what's your protocol for leavers?

If you don't have one, create one, now. You need to ensure that anyone leaving the business:

- Has their access to all accounts blocked
- Can no longer retrieve any files; especially if they've previously accessed them on their personal devices
- Returns any company-owned devices

The same global data risk report we mentioned earlier, also found that 40% of companies had more than 1,000 user accounts that were no longer needed but were still active.

It's little wonder that malicious attacks are possible. Sometimes you can make it too easy.

Key area 5: Good

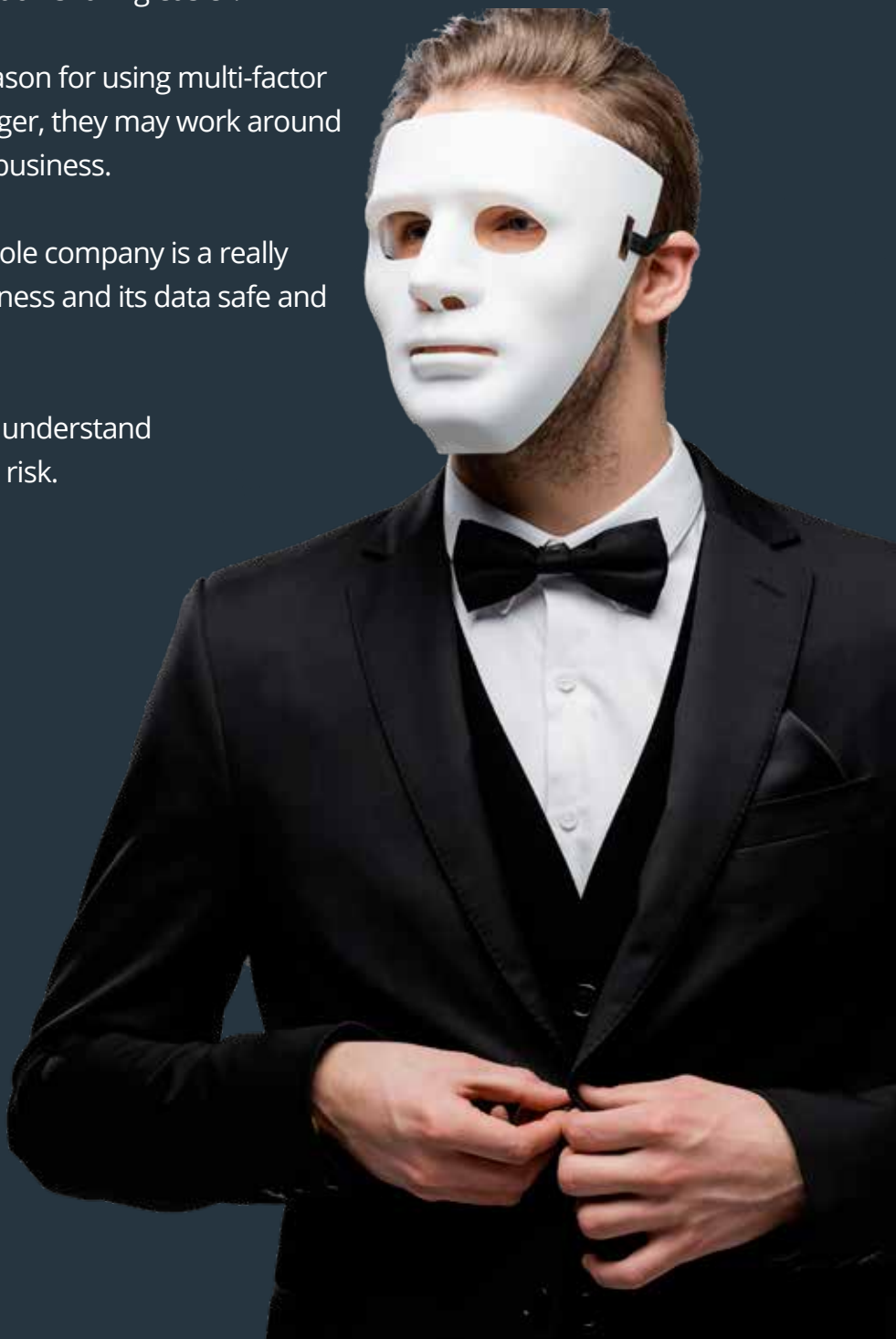
It's likely you already communicate well with your employees. But when it comes to security, it's important that tell everyone why you do things the way you do them. And remind them regularly.

If someone fails to realize that files are restricted and password protected for security reasons, they might give the password to another employee to make information sharing easier.

If an employee doesn't know the reason for using multi-factor authentication or a password manager, they may work around them, creating a security risk in the business.

Clear communication across the whole company is a really important step in keeping your business and its data safe and secure.

If people know what to do but don't understand why they're doing it, that's a security risk.



Those are the five key areas for your insider threat strategy. There may be others depending on the kind of business you run; the data you handle and the

Keeping businesses safe before they have a data security problem is what we do.

How can we help you?