Category: Cybersecurity Awareness

Protect Your Business from Within: Defending Against Insider Threats

You might be thinking that you've done everything to protect your business from cyberthreats. You have the most advanced security solutions to defend against external threats, but are you equally protected against internal threats?

Knowingly or unknowingly, your employees, your vendors, your partners and even you could pose a threat to your business. That's why it's crucial to know how to protect your business from within. In this blog, we'll discuss various internal threats, how to identify red flags, and most importantly, how to avoid them.

Common insider threats

There are various types of insider threats, each with its own set of risks.

Here are some common threats:

1. **Data theft:** An employee or someone who is part of the organization downloads or leaks sensitive data for personal gain or malicious purposes. Physically stealing company devices containing privileged information or digitally copying them are both considered data theft.

.

   Example: An employee of a leading healthcare service provider downloads and sells protected patient information on the dark web.

.

2. **Sabotage:** A disgruntled employee, an activist or somebody working for your competitor deliberately damages, disrupts or destroys your organization by deleting important files, infecting an organization's devices or locking a business out of crucial systems by changing passwords.

   Example: A disgruntled employee of a coffee shop deliberately tampers with the machine, causing malfunction and loss of business.

3. **Unauthorized access:** This is essentially a breach of security when malicious actors such as hackers or disgruntled employees gain access to business-critical information. However, individuals can mistakenly access sensitive data unknowingly, too.

   Example: A malicious employee uses their login credentials to access privileged information and then leaks it to competitors.

4. **Negligence & error:** Both negligence and error lead to insider threats that can pose a security risk. While errors can be reduced through training, dealing with negligence would require a stricter level of enforcement.

Example: An employee might click on a malicious link and download malware, or they might misplace a laptop containing sensitive data. In both cases, the company data is compromised.

5. **Credential sharing:** Think of credential sharing as handing over the keys to your house to a friend. You can't predict what they will do with it. They might just take some sugar or they might use your home for hosting a party. Similarly, sharing your confidential password with colleagues or friends throws up a lot of possibilities, including an increased risk of exposing your business to a cyberattack.

   Example: An employee uses a friend's laptop to access their work email. They then forget to sign off and that personal laptop gets hacked. The hacker now has access to the company's confidential information.

Spot the red flags

It's crucial to identify insider threats early on. Keep an eye out for these tell-tale signs:

- **Unusual access patterns:** An employee suddenly begins accessing confidential company information that is not relevant to their job.

- **Excessive data transfers**: An employee suddenly starts downloading a large volume of customer data and transfers it onto a memory stick.

- **Authorization requests:** Someone repeatedly requests access to business-critical information even though their job role doesn't require it.

- **Use of unapproved devices:** Accessing confidential data using personal laptops or devices.

- **Disabling security tools:** Someone from your organization disables their antivirus or firewall.

- **Behavioral changes:** An employee exhibits abnormal behaviors, such as suddenly missing deadlines or exhibiting signs of extreme stress.

Enhance your defenses

Here are our five steps to building a comprehensive cybersecurity framework that will ensure your business stays protected:

1. Implement a strong password policy and encourage the use of multi-factor authentication wherever possible.
2. Ensure employees can only access data and systems needed for their roles. Also, regularly review and update access privileges.
3. Educate and train your employees on insider threats and security best practices.
4. Back up your important data regularly to ensure you can recover from a data loss incident.
5. Develop a comprehensive incident response plan that lays out the plan of action on how to respond to insider threat incidents.

Category: Cybersecurity Awareness

Don’t fight internal threats alone

Protecting your business from insider threats can feel overwhelming, especially if you have to do it alone. That’s why you need an experienced partner. An IT service provider like us can help you implement comprehensive security measures.

Let us help you safeguard your business from the inside out. Reach out and we’ll show you how to monitor for potential threats and respond effectively if an incident occurs.

Note to MSPs: To ensure your content doesn’t get tagged for plagiarism, add the “no index” meta tag.

About Powered Services

Powered Services sales and marketing resources and tools are provided to aid and promote the sales and retention of customer prospects and clients. Resources are meant as guidance and instruction and do not account for any laws, regulations or restrictions. We suggest you seek legal counsel where applicable.