COLEMAN
TECHNOLOGIES

ARE YOU PROTECTED AGAINST INTERNAL CYBERCRIME THREATS?

www.colemantechnologies.com

Whether they mean to or not, employees can greatly weaken a business' cybersecurity – so what's the best way to eliminate the threat they pose?

Did you know that more than 90% of cybersecurity incidents can be traced back to human error?

The fact is that what you (and your staff) don't know could hurt you. If your staff isn't up to date on the latest cybercrime scams, then they're putting your data at risk, simple as that.

Furthermore, a disgruntled employee can mean more than a bad review on Glassdoor.com — with access to your data, they can cause a lot of damage. The prospect of an "inside job" can seem more akin to a bad lifetime movie, or schlocky thriller plot, but the reality is that it's far more common than you could imagine.

The key to truly comprehensive cybersecurity is simple, yet often overlooked: the user. The best cybersecurity technology and practices in the world can be undone by one staff member who doesn't understand the role they play in cybersecurity, or another staff member that is actively trying to do damage from the inside.

Insider Threats 101

As the name suggests, insider threats refer to security risks that originate from within an organization. Essentially, an insider threat is someone who is a part of your business network or has access to it.

It could be a current employee, consultant, former employee, business partner or even a board member. Insiders with access to your business' sensitive data can compromise the integrity of the data for any reason that suits them.

Let's take a look at the two types of insider threats you must assess, monitor and mitigate.

1. **The Malicious Insider:** A malicious insider is anyone with legitimate access to your business' network and sensitive data, who decides to exploit the privilege either for financial gain or out of spite.

2. **The Negligent Insider:** A negligent insider is a regular employee who falls prey to a cyberattack. A hacker then exploits his/her mistake to compromise your business' sensitive data. They are said to be negligent because they have either ignored existing security policies or haven't been vigilant enough to identify and protect themselves from cyberattacks.

How To Spot An Internal Threat To Your Cybersecurity

Although accurately identifying and determining insider threats can be difficult, there are some early warning signs you can watch out for to nip them in the bud.

Consider the list below and keep it in mind as you manage your staff. Keeping a keen eye out for these signs and recognizing unusual patterns will help you maintain your business' cybersecurity.

The two types of signs are:

1. **Behavioral:** An employee or a stakeholder could be a potential insider threat if they exhibit any of the following behavioral patterns:
   - ➤ Attempting to bypass security controls and safeguards
   - ➤ Frequently and unnecessarily spending time in the office during off-hours
   - ➤ Displaying disgruntled behavior against co-workers and the company
   - ➤ Violating corporate policies deliberately
   - ➤ Discussing new opportunities and/or the possibility of resigning

2. **Digital:** Some of the digital actions mentioned below are telltale signs you must closely monitor:
   - ➤ Accessing or downloading substantial amounts of data
   - ➤ Attempting to access data and/or resources unrelated to his/her job function
   - ➤ Using unauthorized devices to access, manage or store data
   - ➤ Browsing for sensitive data unnecessarily
   - ➤ Copying data from sensitive folders
   - ➤ Sharing sensitive data outside the business
   - ➤ Behaving differently from their usual behavior profile

How Are Insider Threats So Damaging?

There are a number of factors that contribute to the frequency, damage and potential of malicious insider threats, but the two key aspects are:

- Depending on how duties are assigned, what form of supervision is present, and how often employee *(or even ex-employee)* work is audited, the damage they cause can take a long time to discover. Often, the longer it has been, the harder the damage is to reverse.

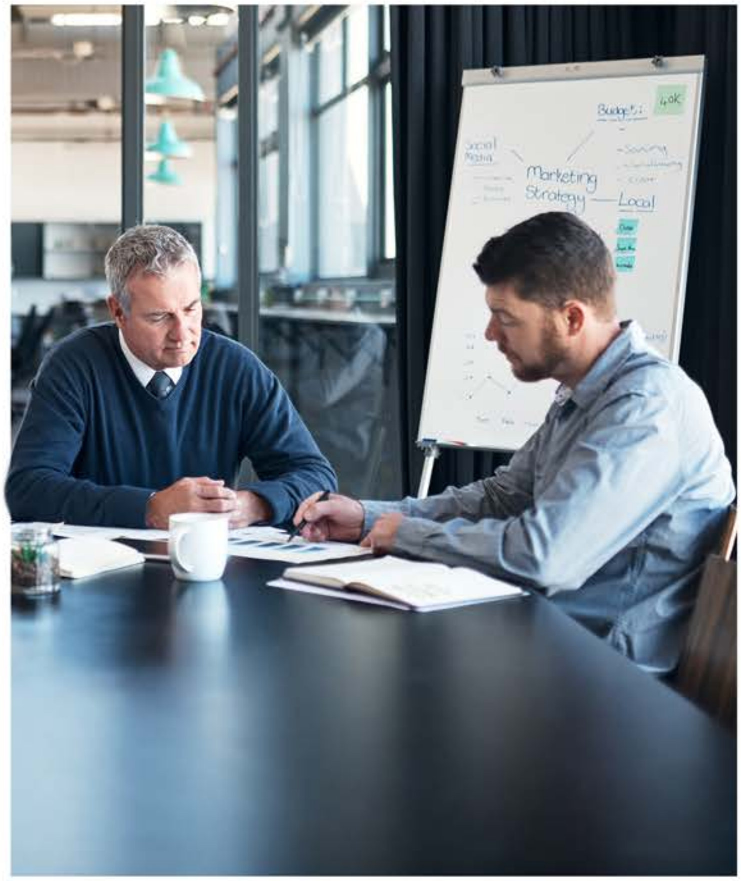
- Once discovered, the response can be difficult to execute. The employee in question can often easily claim it as a mistake, or *(and again, depending on the division of labor and supervision)* can even appear to be doing their job as usual if they're considered the "expert" in that work.

In any case, poor management policies usually leave the door open for disgruntled employees to do damage. Low-level staffers given admin access, third-party vendors provided with authority for data they don't actually need, and login credentials for recently terminated staff members are all common and dangerous occurrences.

The fact is that other security threats — malware, ransomware, phishing, viruses, etc. — simply have more traction with the public's attention than an insider threat does. Why? Because it simply makes more sense.

It's easier to imagine a lone hacker sitting in a basement, targeting a business with their home-brewed cyber weapons than it is to think about what a disgruntled employee might do once they build up the nerve.

Despite this contradiction, the fact is that insider threats are the cause of the biggest security threats, and often cost the most to fix after the fact.



How Should You Defend Against Malicious Employees?

Mitigating malicious insider threats means limiting their ability to damage your business.

Pop quiz: who on your staff is authorized as your local administrator? At most, your organization's local IT manager, or another member of the business' leadership should be set as the admin. If any other staff members have that level of access, it poses a serious risk to your cybersecurity.

The fact is that many businesses give out administrator rights by default. This makes it far easier for disgruntled employees to do serious damage to your systems.

Eliminating this vulnerability can be achieved in two ways:

- ✓ Limiting administrative privileges to those who actually require it. The fact is that the common business user should not require administrative privileges to do their job – whether that's for installing software, printing, using common programs, etc.

- ✓ Protecting administrative accounts. Once you've limited privileges to only a few members of the organization, make sure their accounts have the right protections in place – complex, long passwords, multi-factor authentication, configure alerts for unsuccessful log-ins, and limit administrative actions to devices that are air-gapped from unnecessary aspects of your network.

How Should You Defend Against Negligent Employees?

Cybersecurity Awareness Training is by far the most effective way to defend your organization from phishing, ransomware, and other scams that target unaware employees. This method recognizes how important the user is in your cybersecurity efforts.

A comprehensive cybersecurity training curriculum will train users to ask important questions about each and every email they receive:

- Do I know the sender of this email?
- Does it make sense that it was sent to me?
- Can I verify that the attached link or PDF is safe?
- Does the email threaten to close my accounts or cancel my cards if I don't provide information?
- Is this email really from someone I trust or does it just look like someone I trust? What can I do to verify?
- Does anything seem "off" about this email, its contents, or the sender?

The right training services will offer exercises, interactive programs, and even simulated phishing attacks to test your staff on a number of key areas:

- How to identify and address suspicious emails, phishing attempts, social engineering tactics, and more.
- How to use business technology without exposing data and other assets to external threats by accident.
- How to respond when you suspect that an attack is occurring or has occurred.

We Will Protect You Against Insider Threats

The good news is that you don't have to handle cybersecurity training and management for your team by yourself — **Coleman Technologies** is here to help.

We provide robust cybersecurity training services for our managed services clients. We can also show you how to implement cybersecurity best practices that will limit a malicious employees' ability to do damage to your business.

With our help, your staff will contribute to your cybersecurity, not compromise it.

Here's how to get started:

1. Book a cybersecurity consultation with our team at a time that works for you.
2. Tell us about your organization, its size, and its operations.
3. We'll schedule a cybersecurity training session to show your staff what they need to know to stay safe.

COLEMAN TECHNOLOGIES

(604) 513-9428 | www.colemantechnologies.com