G4S Academy

INSIDER THREAT:
WHAT YOU NEED TO KNOW

TABLE OF CONTENTS

INTRODUCTION: WHAT IS INSIDER THREAT?

Picture a security threat. You think of an attacker coming from the outside, right? But what if the attack comes from within? Insider threats are a serious security risk we can't ignore.

An insider threat is someone who exploits their authorised access for unauthorised purposes. They can get their hands on protected, valuable areas and information.

According to Verizon's 2021 Data Breach Investigations Report, insiders caused 22% of security incidents. These incidents cost organisations millions. They also lead to exposure of sensitive customer and company data.

A global cybersecurity study reported that insider threats cost an average of $15.4 million per year. Plus, over the last two years, the cost and frequency of insider threats has increased. This problem is not going away, and it's getting worse.

In this paper, we'll look at insider threats and their many different aspects. Then, we'll share some of the best practices and strategies we've found for combating this type of threat.

WHAT ARE THE TYPES OF INSIDER THREATS?

Insider threats are a diverse category of risks and attacks. Insiders can have different levels of motivation, awareness, access levels and intent.

So, what are the different types of insider threats? Even though each case of insider attack is unique, we can group the attackers into a few categories. Understanding the motives and types can be key for prevention and mitigation.

Here are the main different types of insider threats and their motivations.

THE MALICIOUS INSIDER

The Malicious Insider is someone who uses their access privileges on purpose to cause harm. They are often motivated by financial gain. Or, sometimes they are stealing company data to gain a competitive edge for a new venture. Usually, they are a lone wolf who acts on their own without any other influences.

For example, a system administrator or database admin may abuse their high level of privilege. They could access valuable items, sensitive information or money.

This is often difficult to prevent. This person is someone the company once trusted with sensitive information and access. But, something happened to make this staff member feel disgruntled and aggrieved. They want to "get even", due to unfair termination, a lack of recognition or some other slight. Or, they may be someone who suddenly finds themselves in difficult circumstances in their personal life. In this case, desperation weakens their personal resilience and leads them to commit malicious acts.

THE CARELESS HAZARD

The Careless Hazard creates a vulnerability due to incompetence or negligence. This is more common than you might think. In fact, according to a 2019 report, careless behaviour causes two thirds (64%) of insider threats.

An example could be an employee who forgets to log out of their work account on a public computer. This leaves it vulnerable for others to access. Or, someone who accidentally loses a flash drive that contains sensitive information. It's easier than you think to mistype an email address and send sensitive information to the wrong person.

Careless Hazards can also be unaware that they are being taken advantage of by others. They might download malware, give information to scammers or click on a link in a phishing email. They might even allow someone to "piggyback" through a secure entrance point. It's as easy as not paying attention to the person entering behind them.

They can also be someone who believes that they are exempt from security policies. For example, they may try to bypass security or skip a procedure because it takes too long. This type of cutting corners leaves data and resources vulnerable.

Although the Careless Hazard may be unaware, their actions are still harmful to the organisation.

THE IMPOSTOR

The Impostor is someone from outside the organisation. They gain access by posing as a third party who gets temporary access to the facilities. For example, they might be a contractor or a consultant.

Like a Trojan Horse, they gain access to the organisation with false good intentions. Then, once inside, they use their access to sabotage, corrupt, destroy or steal. They can be hard to catch, because once they have caused the damage they can disappear.

They might even be someone who gained access a while ago and is still able to use their credentials. Always change passwords, update key cards and provide guests with access credentials that expire.

THE UNDERCOVER SABOTEUR

The Undercover Saboteur is someone who has been "turned" by the malicious influence of a third party. They are colluding with someone outside of the company, using their access in exchange for something else of value.

In this situation, the scammer often appeals to weaknesses in human nature such as greed, anger or a desire for fame and recognition. They may target someone who is desperate due to challenging personal circumstances, which may include addiction, debt or medical issues. Often, the scammer will be manipulating many insiders at once. They can be enabling theft of property, data, espionage or any combination.

As scammers become more sophisticated, they learn how to press all the right buttons. They can convince even high level stakeholders within an organisation to reveal information. When a person with such a high access level gets turned into an undercover saboteur, the company can suffer major losses.

WHAT ARE THE CONSEQUENCES OF INSIDER THREAT?

Insider threats are quite dangerous. The insider has access to the innermost levels of the company, and they can exploit this vulnerability in very harmful ways. So, what can insiders access, and what can they do with it?

The consequences of insider threat depend on the goals of the insider and the types of assets they are targeting. There are four main types of assets an insider can target within an organisation:

- **People:** The people who work within an organisation.
- **Property:** The physical property owned or controlled by the organisation.
- **Information:** Information about the company or its customers.
- **Reputation:** The company's professional reputation in the public sphere.

When they get their hands on the above valuable assets, the perpetrator of the insider threat often wants to:

- **Obtain:** Take the assets for their own purposes
- **Damage:** Disable the assets to sabotage a competitor
- **Destroy:** Erase or get rid of the items completely
- **Deny/Control:** Restrict access to the assets.

For example, if an intruder accesses information, they could expose those secrets to competitors. Or, they could leak customer data to ruin the reputation of the brand. Or, the insider might steal valuable items so that they can sell them for a profit.

And of course, a more complex insider attack may involve doing more than one of these things to many different types of assets. There are infinite ways an insider can harm an organisation with their actions, whether intentional or unintentional. It's important to be wide-ranging and thorough when it comes to developing strategies to prevent these types of attacks.

Did you know?

The damages caused by an internal threat are often much more expensive than those caused by outside attackers.

Based on Ponemon Institute's 2020 Cost of Insider Threats study, the global average cost of an insider threat was $11.45 million. The average cost of a data breach over the same period was $3.86 million.

ARE CERTAIN BUSINESSES MORE VULNERABLE TO INSIDER THREAT?

Are there any particular industries that are more vulnerable to insider threat? The answer depends on the value of the assets (people, property, information, reputation) within the company.

For example, a lot that holds a pile of sand probably isn't a target. But, a data centre attracts a high level of threat due to the value of the personal information there.

The type of industry also affects which sort of insider threat is most prevalent. For example, stealing data to gain an edge is very common in competitive industries such as entertainment and finance. Some industries are more vulnerable to sabotage, while others have more high value items that are targets for theft.

According to the 2022 Cost of Insider Threats Global Report, the financial and professional services industry has the highest cost per incident. This includes a range of companies such as consultancy and accounting firms.

WHY IS INSIDER THREAT SO CHALLENGING TO PROTECT AGAINST?

What makes insider threats different than external threats? Why are these types of threats so much more difficult to prevent?

There are a few reasons. Here are some of the factors that make insider threat a particularly challenging problem to solve.

MANY SECURITY MEASURES FOCUS ON EXTERNAL THREAT

Picture the typical traditional security measures. CCTV cameras, access control, metal detectors, etc. They are all focused on external threats. By themselves, they are not always capable of identifying an internal threat coming from inside the company.

Insider threats often catch organisations by surprise, because they don't always come from where they might expect. Some organisations protect against external threats, but haven't thought about internal threat.

TECHNOLOGY HAS EVOLVED

In the past, insider threats were mainly physical. Companies needed to watch for theft of items or of insiders infiltrating physical spaces. But these days insider threat can be completely virtual.

With the rise of remote work, security threats have become even more complex. We need to think about protecting data and digital spaces from attackers who are able to access them remotely from anywhere in the world. According to the 2021 Insider Threat Report by Cybersecurity Insider, 53% of cybersecurity professionals say detecting insider attacks has become harder since businesses shifted to the cloud.

Technology also makes it easier for attackers to cover their tracks and protect themselves. This opens up the possibility of so many more different types of insider threats.

INSIDER THREATS ARE ALWAYS EVOLVING

Another important factor to keep in mind is that insider threats are always evolving. It's a constant game of cat and mouse for any organisation or security firm to stay one step ahead of them.

Hackers are always looking for new ways to infiltrate businesses. That could mean hacking technology or "turning" employees. They often prey on the worst qualities of others and are always developing a fresh new way to do this.

It's not enough to know the techniques scammers are currently using to infiltrate organisations. It's also necessary to think ahead and figure out what their future techniques will be before they attack. To truly be successful in mitigating insider threat, we must always be several moves ahead.

HOW DO WE MITIGATE INSIDER THREAT?

So, how do we stay ahead of insider threat? What are the best strategies for preventing this type of treat, identifying it when it happens and stopping it in it's tracks?

As mentioned above, we aim to stay one step ahead of the threat and always predict their next move. We do that by using a variety of strategies, both physical and psychological.

Here are a few of the ways we mitigate insider threats:

CAREFULLY SCREENING AND VETTING STAFF

As the old saying goes, "an ounce of prevention is worth a pound of cure." The mitigation of insider threats starts with hiring trustworthy staff who will be less likely to act maliciously against the company.

In the security industry, it is a proven best practice to conduct rigorous background checks for every team member. Yet, sometimes that's not enough. Employees who have had no prior incidents in their background can still get turned when they are on the inside. Or, they can become disgruntled and seek revenge.

To take the screening and vetting process even further than the typical background check, consider conducting psychometric evaluations. These tests screen for the "Dark Triad" of personality traits: Narcissism, Machiavellianism and Psychopathy.

- **Narcissism:** People who believe they are superior to others and are often selfish, arrogant and obsessed with themselves.
- **Machiavellianism:** People who are manipulative and willing to deceive and hurt others in order to get what they want.
- **Psychopathy:** People who are emotionally volatile and don't experience empathy or remorse when they hurt others.

These dark triad traits are effective predictors of job performance. People who have this Dark Triad of traits are more likely to exploit others, even close family or work colleagues, to get ahead.

This is why it's so important to screen for these personality traits within the psychometric assessment process. Considering how much damage one person with these traits can do within an organisation, your organisation can't afford not to.

UNDERSTANDING HUMAN PSYCHOLOGY

There's a certain comfort in outside threats. We can see them coming and we have alarms in place to stop them. But insider threats are more like a game of "Among Us". Everyone claims to be innocent. The challenge is to figure out who's lying.

That's why part of mitigating insider threat is understanding the human psychology behind their

strategies. We dedicate time to learning about the psychological complexities of these attacks.

Most scammers and malicious insiders are charming. They have the right skills to convince others around them that they are innocent. They use gaslighting, deflection and dishonesty to cover their tracks.

But once you understand the psychology behind this type of scam, you'll start to recognise patterns in behaviour. It will be easier to see behind the "theatre" and spot people for who they really are.

SETTING UP ACCESS CONTROL

Another crucial step for preventing insider threat is to set up levels of access control. At your premises, every access should be recorded. All employees, visitors and other personnel should get appropriate access for their status and role.

It's good safety protocol to restrict and control digital and physical access. It's also important to compartmentalise sensitive knowledge and information. This sensitive data should only be shared on a need to know basis.

Yet, if access control is too restrictive or difficult to use, staff may bypass it for convenience or it could restrict business. The ideal sweet spot provides the necessary control while still making it easy for those who need access to do their jobs.

USING CCTV TECHNOLOGY

CCTV technology is also a useful tool for preventing insider threat. When employees know the cameras are on them, it's harder to do anything deceitful.

For example, employees who transport money have cameras on them at all times. They count the money, pack the money and hand it over, all in front of a camera. In many situations, knowing that their actions are being recorded will affect their intentions to act.

Cameras can also help with the issue of people using each others access cards. The CCTV footage will show who actually entered any specific area, and exactly what they did there.

Of course, CCTV will never be enough by itself. It should be a part of a full security system and monitored by a well-trained team.

MONITORING BEHAVIOUR

Any significant change in staff behaviour can be a warning sign for insider threats. A modern AI security system can track this information and detect unusual activity.

With historical data, you can create a baseline of "normal" behaviour for any employee. Once you know the baseline, you can flag any deviations from the norm.

What behaviours should you watch out for? For example, you may notice:

- An employee who was always on time for years, but has now been arriving late.

- An employee who has been recently staying later than usual.
- A staff member who logged in on an unusual day or time, or from a new location.
- Someone with many failed password attempts on their account.
- A staff member accessing areas of the premises with no obvious reason to be there.
- An employee with a large number of data transfers or outbound communications.
- An employee loitering for too long in a particular area.

Of course, these behaviours themselves are not evidence of any wrongdoing. Flag them and look into them, but don't jump to conclusions before hearing the whole story.

For example, the staff member staying later after their shift may be waiting around for a bus. Or the person arriving late might be dropping their child off at a different school further away. Someone could be trying to access a room with with sensitive information. Or, they could have a crush on someone who works in that corridor and they want to say hi.

Monitoring staff behaviour should be the beginning of a conversation. Talk to your team and find out the reasons behind these behaviours, so you can understand what's going on. For this, it's important to align with HR, as they are the ones who will know the employees best.

SETTING UP SOLID SECURITY PROCEDURES

Most accidental insider risk comes from negligence. In other words, things go wrong when staff don't do things properly. This is why it's so important to set up solid security procedures. When all external protections fail, internal procedures are often the only things left to protect you.

For example, this might look like setting up a five step checklist for shutting down a lab or workspace. If this workspace contains valuable information or products, employees must secure those assets. The procedure should be clearly outlined, with no room for confusion. Also, train your employees often and refresh them on these procedures.

Be sure to track these procedures too. There should always be a record of when they were carried out, and by whom. It may take a little extra time and thought to set this up at first, but it's worth it.

ENCOURAGING STAFF TO SPEAK OUT

Train employees to detect risky behaviour among their colleagues and report it. Your team will spot more than you ever would on your own.

Staff members need to feel safe and encouraged to speak up. Give them a confidential way to report, to avoid negative retaliation from colleagues.

Of course, staff will only be willing to share information if they feel valued at the company.

When employees are resentful or disgruntled, they may be unwilling to help. They will be more likely to turn a blind eye and think, "not my problem," when they see something suspect.

Which leads into our next strategy: boosting the health of the workplace culture.

CREATING A HEALTHY WORKPLACE CULTURE

As the saying goes, "rotten barrels make rotten apples." Toxic workplaces foster dishonesty and mistrust.

Disgruntled employees often want revenge on the employer who wronged them. This leaves your organisation vulnerable. Even terminated employees may still have information they can use to cause harm.

So, keep a close eye on employee morale and listen to your team. Act with integrity and show them respect. Make them feel valued, pay them well and give them recognition for their hard work.

Improving the culture of your workplace will not only help to reduce the risk of insider threat. It will also boost your bottom line. You'll attract innovative top talent and they will be more productive. Plus, they will stick around - saving you time and money on recruiting and training.

Monitoring can help with this. When you notice a strange behaviour pattern, reach out and offer support. Encourage communication and show you care, and your team will have your back.

MONITORING FOR LEAKED PRODUCTS/DATA

Another way to halt product theft is to keep an eye out for products that show up elsewhere. For example, a major clothing brand was experiencing an issue with theft from their warehouse and shipping locations. So, they monitored third party resale websites for an influx of their stolen products. They were able to identify the illegal resellers and shut them down.

You can also keep your ear to the ground online. Look for any discussion of your brand on social media and online forums. You might find data or secrets being shared, or discussions by disgruntled potential saboteurs. This type of monitoring should be done regularly. It's an important part of your security strategy.

It's especially important when it comes to data breaches. Often when data gets leaked, it takes businesses months to even notice the breach. According to a report from IBM, in 2022 it took an average of 277 days to identify and contain a data breach. That's approximately nine months! The longer it takes to catch a data breach, the more money will be lost (not to mention the reputation damage.)

WANT TO PROTECT AGAINST INSIDER THREAT?

With the right training, a positive work environment and the latest technology, it is possible to reduce the risk of insider threat. The above best practices are a great start, but the list of strategies is not limited.

When it comes to protecting your company against insider threats, it's important to diversify your approach. Don't rely on a single solution. Instead, take stock of the unique needs of your organisation. Create a system that combines several defences against insider attacks.

To find out more about insider threat and get a custom consultation for your business, talk to an expert on the G4S team. Reach out to us today at www.G4S.com.

VALUE CREATED TOGETHER

CONTACT

GET IN TOUCH WITH THE G4S TEAM – VISIT WWW.G4S.COM