business.com

Home > Technology > Security

Insider Attacks and How to Prevent Them

Andrew Martins
Staff Writer

business.com Staff
Jan 20, 2021

While most cybersecurity threats come from outside your company, internal issues can cause major breaches as well.

When it comes to cybersecurity for your small business, not all threats come in the form of a faceless hacker feverishly working to gain access to your sensitive data. A growing number of threats come from within a company, whether the attack was willfully perpetrated or not. By understanding the potential risk of an insider attack and recognizing any potential telltale signs, you can mitigate those risks and keep your data safe.

What is an insider attack?

An insider attack, or insider threat, is an instance in which someone with legitimate credentials into your business's networks and assets uses their privileged access to cause harm to the company. The Cybersecurity and Infrastructure Security Agency

defines insider threats as data breaches that can include "sabotage, theft, espionage, fraud, and competitive advantage … often carried out through abusing access rights, theft of materials, and mishandling physical devices." Under that definition, an insider threat can happen for many reasons through a range of methods.

While current employees tend to be a common cause of such an intrusion, anyone with access to your company's data poses a security risk. According to a 2020 Ponemon study, the number of insider threats has grown by 31% in the last two years, with costs inflating to $11.45 million. The study also found that the frequency of such incidents spiked by 47% during that same period. With companies now more reliant on digital communications and remote access of sensitive data than ever before, insider threats are likely to become a more frequent and costly occurrence.

Editor's note: Looking for the right employee monitoring software for your business? Fill out the below questionnaire to have our vendor partners contact you about your needs.

Approximately how many employees do you have?

- ○ 1-19
- ○ 20-49
- ○ 50-99
- ○ 100-499
- ○ 500+

NEXT ▷

What is the difference between an insider threat and external attack?

While internal attacks stem from someone within the company already having access to the more sensitive areas of your business, an external attack occurs when someone outside of your organization tries to gain access. While both types of intrusions can happen in similar ways, like phishing and malware, the big difference is who's perpetuating the attack.

What are the different types of insider attacks?

Just as there are several ways in which an outsider can gain access to your company's systems, there is more than one way for an insider attack to take place. In nearly every instance of an insider attack, the biggest differentiator is whether

your employees, former employees, partners or contractors are in on it from the start.

"The greatest risk to organizations remains the human component of security," said Kon Leong, CEO and co-founder of Silicon Valley data governance company ZL Technologies. "While it is possible to lock down permissions and track data movement against all programmatic access, ensuring that humans don't behave maliciously or negligently has become an even bigger concern now more than ever."

According to a 2019 report by Verizon, the five most common types of insider threats small businesses face are "the careless worker, the inside agent, the disgruntled employee, the malicious insider and the feckless third-party."

Kevin Parker, co-founder of vpnAlert, said these attacks can also be classified as the following: pawn, goof, collaborator and lone wolf. In each of those instances, different methods of attack are taken, different individuals may be involved and different steps could be taken to stymie such threats.

Pawn

In the instance of a pawn insider threat, the individual involved usually has no idea they've been targeted or are causing the problem. In most cases, this happens when an employee has fallen prey to a malicious insider attack from an outsider, either through a phishing attempt or social engineering. If this happens, it often means that an external threat has gained access to the pawn's credentials, causing the employee to become a compromised insider.

Goof

When employees fail to follow security measures, leaving your company open to external threats, Parker said they fall into the goof category. Purposeful skirting of company guidelines could be the result of trying to make things more convenient for themselves, or they just don't want to follow the rules, making them a particularly negligent insider. Such an act could be as simple as storing company login information in the cloud, which would be easier to access but significantly less secure.

This insider threat, according to a 2020 Cyber Threats Report by Netwrix, has 79% of chief information officers concerned that "users might ignore IT policies and guidelines, increasing security risk." Though they don't cause the problem with any malicious intent, they often end up accidentally making harmful decisions that

leave the company exposed, leaving a door open for an outsider to gain access, in the process.

Collaborator

While the previous two instances were the result of gross negligence or some other digital mishap, attacks that fall into this category have the potential to create a large amount of damage.

Insider attacks that feature a collaborator see employees voluntarily working with a third party to intentionally harm their employer. Not only does this leave your sensitive data potentially exposed to your competitors, but this type of threat is also a major vector of attack for corporate espionage, leading to major financial losses.

Lone wolf

This type of threat can stem from an angry employee, contractor or someone with privileged access looking to actively harm a company.

What are potential points of attack?

The following are some methods of ingress that either external forces can try to use to gain access to your company's data or how internal members of your team can cause harm.

Internal hacking

This sort of attack is the result of a person making the willful decision to do things like steal data, leak access or alter sensitive data.

Email attacks

Phishing attempts are a common way for people to get access to someone's sensitive data. When this is applied to the business setting, the damage can be compounded, as now it's not just an individual's data at risk, but the entire organization's.

"Given the number of ransomware attacks occurring in recent years, email-based threats are getting most of the attention today," said Richard Long, a business continuity consultant at MHA Consulting. "Phishing, malware and ransomware are all types of attacks that come through email; providing access through these emails is almost always unintentional."

Ransomware attacks

Much like email/phishing attacks, ransomware attacks are unintentional in nature, with downloaded files often acting as the point of entry. These attacks generally result in a company's system getting locked down by a virus, with hackers demanding a payment before the systems can be accessed again. According to Bitdefender's Mid-Year Threat Landscape Report 2020, there was a "715% year-on-year increase in detected and blocked ransomware attacks."

"These attacks can bring a company to a halt by disrupting access to data, shutting users out of their emails and even jamming up phone systems," said Ara Aslanian, CEO of Inverselogic. "Ransomware attacks have shut down critical organizations like schools and hospitals for days, and disrupted supply chains for weeks at a time."

Mobile and cloud storage attacks

With the increased shift to remote work in the wake of the COVID-19 pandemic, employees have relied on mobile and cloud-based storage. With sensitive and personal data both living in the cloud, it's become easier for that data to be compromised. While the existence of this tech isn't necessarily the threat, since it's usually protected pretty well, the problem crops up when people copy sensitive data from a company cloud account to their personal account for easier access.

"Mobile and cloud storage attacks have the potential to be more potent if an employee needs access to data at home; they may put that data in their personal account," Long said. "This puts this information at risk, as many do not have high security on their home systems and networks."

The level of risk depends on how careful the employee is about keeping their personal cloud storage secure, according to Long.

What are examples of insider attacks?

In recent years, several high-profile insider attacks have made international headlines. While the stories sometimes smack of the type of corporate intrigue or international espionage you'd find in a Hollywood blockbuster or New York Times bestseller, these instances are all actual events that took place:

- **Edward Snowden and the U.S. National Security Agency.** Whistleblower and former CIA employee Edward Snowden used his privileged access to smuggle highly classified information in a bid to expose highly invasive NSA activities.

- **Tesla data leaked by "disgruntled" employee Martin Tripp.** In 2018, electric car manufacturer Tesla and its CEO Elon Musk fell prey to an insider attack when a former employee, Martin Tripp, allegedly gained access to the "manufacturing operating system" to steal a significant amount of proprietary data, which was then transmitted to an unknown third party.

- **Former Coca-Cola employee causes a data breach.** Another 2018 incident saw Coca-Cola dealing with a data breach after a former employee was found to be in possession of an external hard drive full of sensitive data. Among that data, according to the massive beverage company, was personal information of up to 8,000 other employees.

How to safeguard your business from insider attacks

There are ways to preempt, identify and stop potential attacks. Though such an intrusion is inherently difficult to recognize as it's taking place, there are ways you can make sure things never get to that point.

Implement employee monitoring software.

There's an entire subsection of business software aimed at protecting your data by keeping tabs on your employees' activities. Through the use of employee monitoring software, an employer can set rules for how data is handled and set triggers that go off when the suspicious activity of a potential insider threat is detected.

"Employee monitoring software can help you spot potential threats by flagging unusual network activity. It can trigger a warning when an employee attempts to access files or databases that are outside of their usual working needs," said Aslanian. "Employee monitoring software can also be used to protect against non-malicious actions that nevertheless expose networks to risk. For instance, it can block access to websites that are high risk for malware."

Establish a "zero-trust" cybersecurity stance.

In many insider attack cases, data became compromised by someone the employer trusted, regardless of whether it was a high-ranking IT manager or someone further down the totem pole. Unfortunately, that may mean that the days of giving someone carte blanche trust over a company's sensitive data are gone.

By taking such a guarded stance, Aslanian said employers should assume that "any device on a network could be compromised and so requires continuous

authentication of users." Those users should also be granted the bare minimum access that they need to do their jobs, he said.

Provide cybersecurity training to employees.

Part of the issue surrounding insider threats is that many times, these incidents occur by accident. By educating your employees about the importance of keeping data secure, Aslanian said you can create an additional barrier against internal attacks – especially when it comes to things like phishing attempts.

"It's vital to train and continuously refresh employees on the latest phishing email scams," he said. "These are becoming increasingly sophisticated, often spoofing names of senior managers or suppliers to dupe workers into clicking on links. I've even known chief IT officers to fall for these types of scams."

Image Credit: Portrait Images Asia by Nonwarit / Shutterstock

Andrew Martins
business.com Staff
See Andrew Martins's Profile ›

I am a former newspaper editor who has transitioned to strictly cover the business world for business.com and Business News Daily. I am a four-time New Jersey Press Award winner and prior to joining my current team, I was the editor of six weekly newspapers that covered multiple counties in the state.

Technology

See More ›

08.20.12

Expert Advice on Business Workflow

Business workflow expert Brian Reale, CEO and co-founder of Colosa...

10.19.20

How Unified Communications Is Boosting Corporate...

UCaaS technology streamlines enterprise communications by...

05.21.18

5 Preventable Human Errors That Leave Your Company...

Most cyberattacks stem from internal human error, but companies...

03.16.20

Preparing Your Business for Remote Work During the...

As more businesses switch to remote work, these low-cost apps help...

09.14.18

VPN and Online Privacy: What You Need to Know...

Using a VPN connection makes your browsing extremely secure.

Resources

Our Company

Our Brands

Contact Us