THE DEVIL YOU KNOW:

INSIDER THREATS

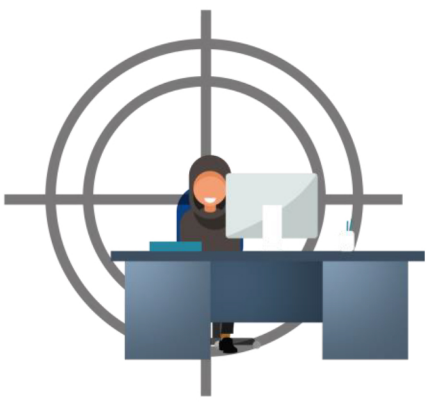
TO BUSINESS CYBERSECURITY

DEFEND YOUR I.T. FROM INSIDER THREAT RISKS

POWER up BOSTON

The frequency of insider threat incidents is on the rise. Between 2018 and 2020, they spiked by 47%, according to the Ponemon Institute. No business wants to believe their cybersecurity risk is internal, yet denial doesn't keep networks and systems safe.

This guide will help you understand, detect, and prevent insider security issues.



It's the stuff of horror movies. An innocent's eyes widen in fear when the police track a threatening call and report, "it's coming from inside the house!" For businesses, the idea of cyber threat coming from within their walls is as scary, yet insider threats are a real concern.

What is Insider Threat?

Insider threat is someone misusing their access to business network, systems, and data. In a malicious incident, the bad actor intentionally accesses information for financial or personal gain. It might be sabotage, corporate espionage, or intellectual property theft.

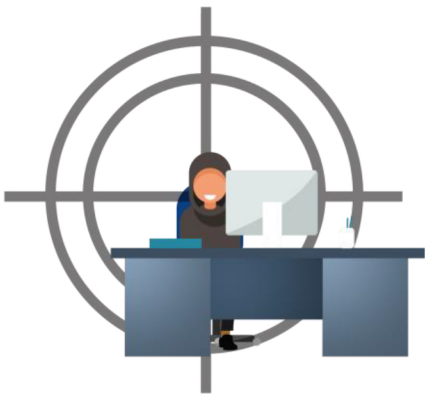
Part of the problem? Insider threat isn't always intentional. Yes, this validates your belief that your people mean well, yet a security incident caused by human error or carelessness can still be damaging. When someone inside your business clicks on a phishing

email or downloads malware, that's also an insider threat.

Fast fact: *The average global cost of insider threats rose by 31% to $11.45 million from 2018 to 2020 — Ponemon Institute*

Who can be an insider?

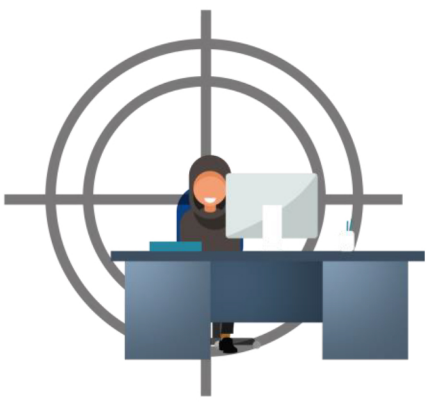
- a current employee;
- a former employee;
- employees involved in a merger or acquisition;
- a third-party vendor;
- a contractor;
- partners;
- in reality, anyone with authorized access to your network, systems, and data.



Fast fact: *In the 2020 Ponemon Institute Insider Threat Costs Report, containing an insider threat incident cost an average of $211,533 annually. Plus, the cost of investigating these situations is scaling up, too. In 2020, investigations cost organizations "a whopping 86% more than they did only three years ago."*

Insider Threat Incident Example

In 2019, an Amazon engineer used insider knowledge of a misconfigured firewall in a Capital One cloud server to access customer records. She stole 40,000 Social Security numbers and 80,000 linked bank details.



Who is at risk of insider threat?

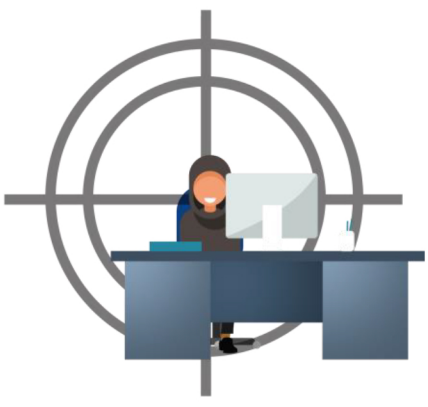
In brief: every business is at risk of insider threat.

Top industries at risk of cyberattack include:

- financial services;
- telecommunications;
- technical services;
- healthcare;
- government.

Yet, considering insider threat can come from a simple mistake, any industry is at risk.

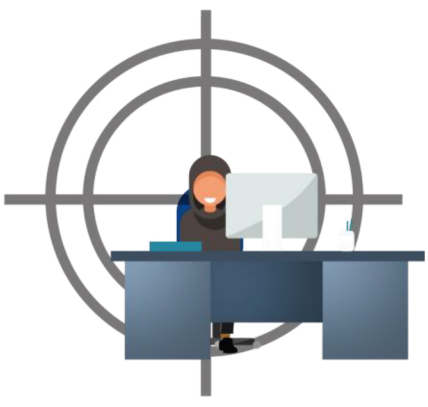
Fast fact: *Insiders were responsible for 50% of incidents where private or sensitive information was unintentionally exposed — SANS*



How to Detect Insider Threats Earlier

When there's evidence of a break-in or an error, the incidents are quickly contained. Yet, insider privilege misuse is one of the slowest breaches to be discovered, according to Verizon. That’s because the insider has the know-how to access infrastructure and data unnoticed. Plus, the business trusts them.

This is particularly painful, as “the longer an incident lingers, the costlier it gets,” according to Ponemon. The average incident is contained in 77 days. Yet, when it takes more than 90 days, it costs an "average of $13.71 million on an annualized basis.”

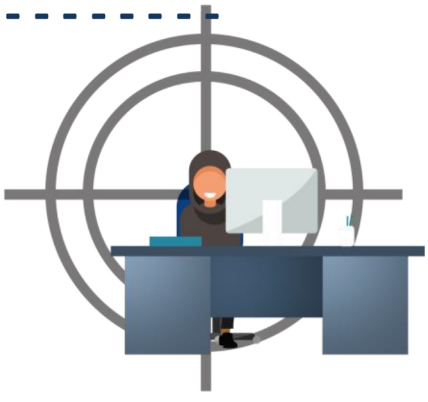


So, what can your business do to detect insider threats?

- Monitor activity and system activities.
- Check access logs for any anomalies.
- Use data analytics to learn baseline behaviors.
- Anonymize user data to protect employee and contractor privacy and meet regulations.
- Investigate any suspicious activity now, not later.
- Audit servers to find any data with global access groups applied.
- Archive or delete stale data.

Insider Threat Incident Example:

A former employee of Waymo, Google's self-driving-car startup, stole 14,000 confidential files and took them to his new job at Uber.

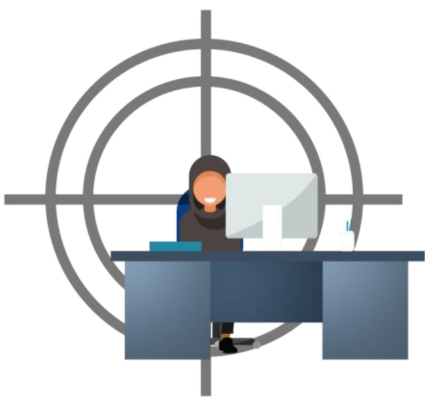


Consequences of Insider Attacks

"I didn't know," says the employee after connecting a thumb drive preloaded with ransomware in at work. Yet whether the insider meant to do it or not, insider attacks can be devastating.

Your business could suffer:

- revenue loss;
- loss of critical business and customer data;
- disclosure of trade secrets;
- brand reputation damage;
- customer dissatisfaction;
- regulatory fines;
- legal action;
- drop in market value;
- decreased productivity.



Fast fact: *A data breach incident carried out by two Shopify support team members team caused a 1.61% fall in the ecommerce network's stock price.*

Preventing Insider Attacks and Threats

We can't be the first people telling you about the possibility of insider threat, yet in a SANS survey on insider threats, only 18% of respondents had "a plan for responding to insider attacks."

Prevention starts with strong access controls and good cyber hygiene. In a global 2019 Varonis study:

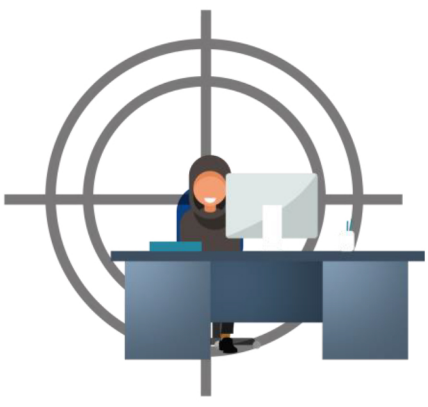
- 53% of companies had over 1,000 sensitive files open to every employee;
- 17% of all sensitive files were accessible to all employees;
- an average of 22% of all folders were available to every employee;
- only 5% of folders were properly protected.

That's asking for trouble. We recommend implementing least-access privileges. Instead of organization-wide access, people can access only what they need to do their jobs, no more.

It's also a good idea to segment network access. If a bad actor does get access to, say, payroll's database, that's bad news. But with segmentation, they can't then leapfrog into customer data, too.

Regularly changing access credentials is another important step. In the Varonis study, 61% of companies found over 500 users with passwords that never expired. Sure, that means they won't forget, but it also means someone compromising an administrative account could have indefinite access.

Also, avoid incidents involving retired or fired employees. Have a policy in place to revoke credentials for users no longer with the company.

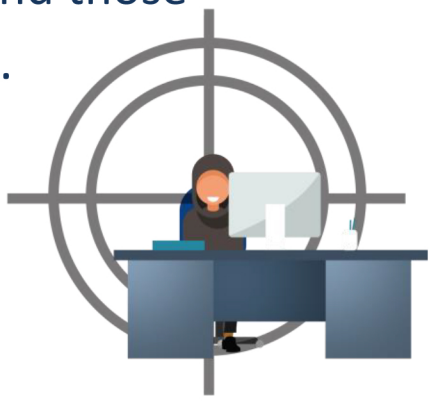


Insider Threat Incident Example

An employee at the Australian National University fell for a phishing scam email. As a result, 700 megabytes of data related to staff and students was stolen. The data included names, addresses, phone numbers, dates of birth, tax file numbers, payroll information, bank details, and academic records.

How Work from Home Complicates Things

Insider threat may also be rising because more people are working from home. In the past, the business needed to protect a network and devices only on its own premises. Today, it is critical to secure an online environment for those working in the office and those who are remote or working in a hybrid model.

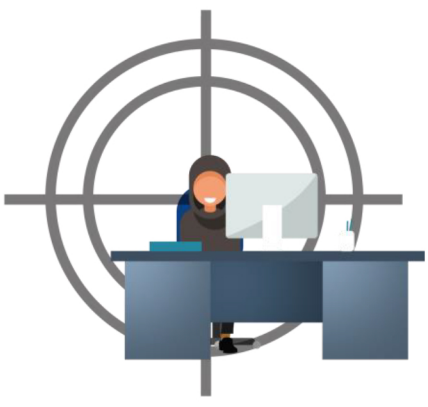


In one 2020 survey of C-suite executives, the 260 senior leaders surveyed found “remote workers significantly improved their productivity since working remotely.” There were several reasons for their “increased efficiency”:

- commute eliminated;
- workplace distractions minimized;
- flexible work hours.

But employees working wherever they are, whenever they want, increases your exposure.

Applying extra preventative controls such as encryption can help protect your data in transit. It’s also a good idea to use two-factor (2FA) or multifactor authentication (MFA). These can help verify user identity via many factors before granting remote access to systems or data.

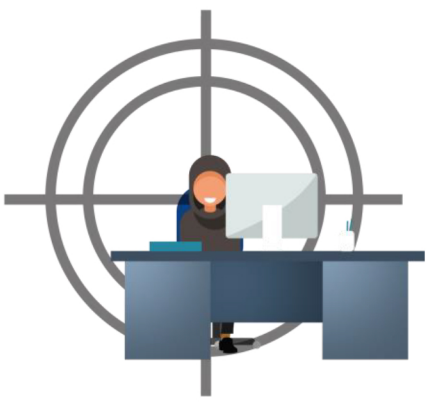


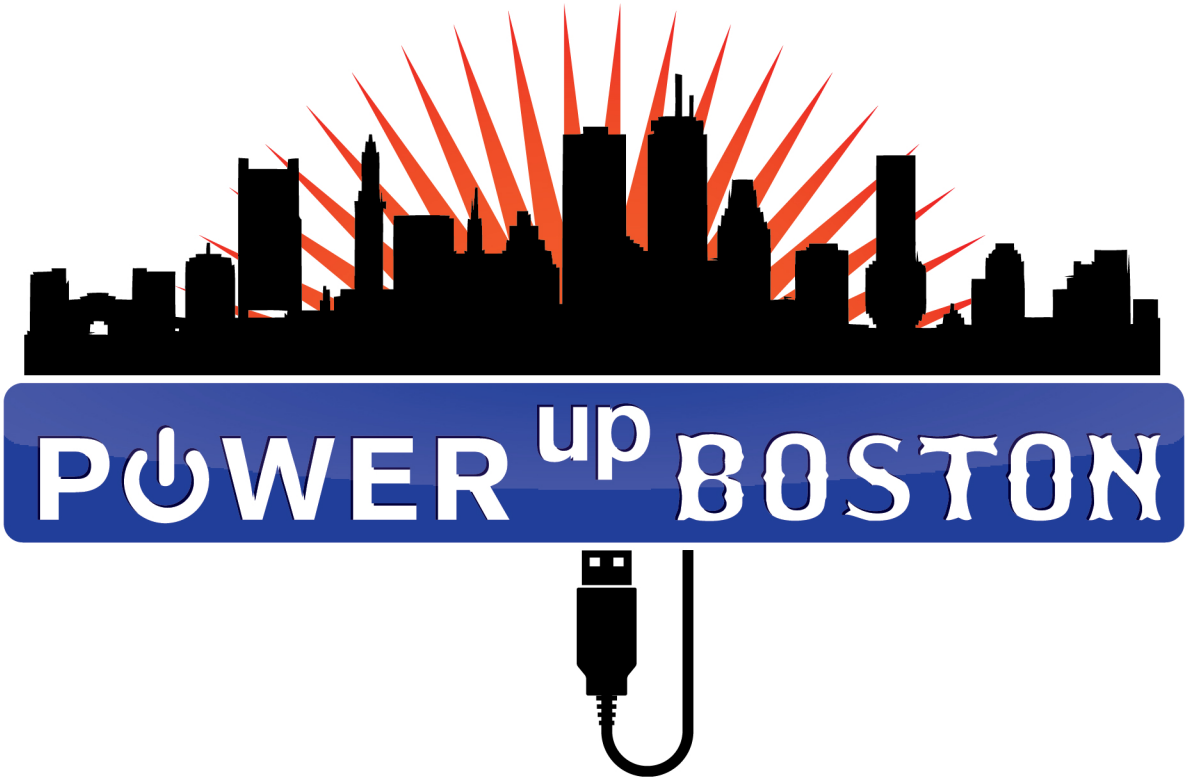
Insider Threat Incident Example

An employee of a medical device packaging company lost his job in March 2020 due to COVID-19. He hacked the company's customer network. He granted himself administrative access and edited or deleted nearly 120,000 records.

Secure Your Business with an MSP

A managed service provider (MSP) can install security controls to defend against insider threat risks. Working with an MSP, you add an IT expert to help monitor your systems, network, and data to detect and mitigate your exposure. Contact us today.





Phone: (508) 617-1310

Email: info@powerupboston.com

Web: www.powerupboston.com

Facebook: facebook.com/powerupboston