cyberhaven

The Risk You Already Trust: Managing Insider Threats at Scale

The Insider Threat Landscape

While ransomware and external exploits grab headlines, insiders are an increasingly significant risk, as many complex data security incidents involve trusted users, such as employees, contractors, and partners, who already have legitimate access to sensitive systems. The human layer has become a primary source of exposure and a predictable outcome of distributed, cloud-connected organizations.

Insider risk occurs when authorized users inadvertently expose sensitive data — through oversharing, unsafe file handling, or unapproved tools. When that risk turns into harmful action, whether deliberate theft, sabotage, or exploited credentials, it becomes an insider threat. The key difference isn't intent, but impact: insider threats cause real damage.

These threats are hard to detect because they come in many forms — carelessness, convenience, malice, or external compromise — and often look the same without context. Traditional security tools, built for external attacks, can't assess intent, interpret behavior, or intervene at the moment it matters most.

Insider threats are now an expected dimension of modern data security. Addressing them effectively requires a structured approach that prioritizes context, behavior, and timely intervention, reducing risk without slowing the business.

34%
of breaches involve internal actors

**Verizon Data Breach Investigations Report 2025*

Insider Risk Doesn't Just Persist – It's Accelerating

Insider risk isn't rising because organizations trust employees too much, it's rising because modern enterprises are harder to govern. Data is more distributed, access is more dynamic, and work spans more tools, devices, and environments than ever before.

At the center of the challenge is data sprawl. Sensitive information no longer resides in a few well-defined systems; it moves continuously across cloud platforms, collaboration tools, endpoints, and third-party services. Maintaining visibility into where data lives, who can access it, and how it moves is increasingly difficult. Without that visibility, risk accumulates quietly until it becomes an incident.

$4.27M Threat

Insider threats carry a significant financial risk, averaging $4.27 million per incident.

IBM Cost of a Data Breach Report, 2025

The nature of work has also changed. Remote and hybrid work, widespread personal device use, and reliance on AI and generative tools expand how data is accessed, transformed, and shared. AI accelerates the movement of sensitive information, allowing it to be copied or transmitted instantly, often outside traditional controls.

The challenge is accelerating with the adoption of AI and generative tools. AI dramatically increases how quickly data can be copied, transformed, and shared, multiplying exfiltration paths and compressing the window for detection. As productivity rises, so does the need for visibility and control over how sensitive data is used.

Insiders know where valuable data lives and how controls work; without behavioral visibility and unified workflows, early warning signs are easy to miss.

As organizations become more data-driven and open, insider risk is inherent. Managing it requires modern controls that unify data visibility, identity context, and behavior — so risk can be identified and addressed before it escalates.

Who Are These Insiders? Ten Threat Actor DNA Types

Not All Insider Threats Are Malicious — But All Are Risky

	Type	Motivations	Description
01	**The Flight Risk** "I'm already halfway out the door."	Leverage Resentment Employment Advantage	A trusted employee with who quietly hoards high-value data "just in case." With broad access to sensitive information and strong technical competence, this insider can walk away suddenly, taking critical knowledge with them.
02	**The Maverick** "The rules slow me down, AI gets results."	Speed Productivity Innovation	A high-output employee who embraces GenAI, builds their own tools, and prioritizes efficiency over security. By bypassing guardrails or feeding sensitive data into AI systems, this insider creates invisible data exposure and new risk surfaces.
03	**The Negligent Employee** "It's just a token, what could go wrong?"	Convenience Speed False Sense of Safety	A well-meaning employee with poor security hygiene who mishandles secrets such as tokens, credentials, or keys. Driven by convenience and complacency, this insider unintentionally creates paths to compromise.
04	**The Adventurer** "Work is wherever I am."	Convenience Poor work-life balance Flexibility and Freedom	An employee who blends personal and corporate environments. From using personal tools and accounts to accessing sensitive data over public Wi-Fi or while traveling, this insider creates unmanaged copies of data and dissolves traditional perimeters.
05	**The Crown Jewel Collector** "The most valuable assets are mine for the taking"	Profit Power Leverage	A privileged insider who methodically identifies and exfiltrates the organization's most valuable data. Skilled at blending into normal workflows, this insider targets core IP, proprietary algorithms, and mission-critical databases, selling or trading them to competitors, nation-states, or other willing buyers.

Who Are These Insiders? Ten Threat Actor DNA Types

Not All Insider Threats Are Malicious — But All Are Risky

Type	Motivations	Description
06 **The Collaborator** "I was just trying to help."	Teamwork Efficiency Goodwill	A teamplayer who often over-shares data, grants broad access, and makes it easy for data to accidentally spread outside a"need to know" framework.
07 **The The Malicious Insider** "If I can't be seen, I can't be stopped."	Financial Gain Secrecy Chaos	A stealthy insider who knows how to move through an environment and intentionally evade controls. Is able to cover their tracks while exfiltrating data.
08 **The Privilege Creep** "Accumulated permissions are an operational necessity, not a risk."	Efficiency Convenience Complacency	A well-meaning employee who accumulates excessive access over time due to role changes, exceptions, or stale entitlements — creating silent, high-impact data and access exposure.
09 **The Retaliator** "If the company wronged me, I owe it nothing."	Resentment Revenge Personal Gain	A trusted employee motivated by resentment or perceived injustice who intentionally misuses legitimate access to steal, leak, or sabotage organizational data or systems.
10 **The Temporary Insider** "This isn't my workplace, so I don't have to be careful."	Efficiency Carelessness Convenience	Includes contractors, vendors, temps, or partners with elevated access who may be more prone to data risks due to shorter loyalty, less training, or weaker controls.

Insider Threat In Action

One of the most damaging insider threat patterns involves **The Flight Risk**. In a recent case, Cyberhaven observed a former engineer stole advanced AI technology by downloading an entire codebase, zipping it to stage the data, and uploading it to a personal cloud storage account just before resigning to join a competitor.

Cyberhaven IRIS: Build and Mature Your Insider Risk Program

Cyberhaven Insider Risk Intelligence Service (IRIS) is an ongoing intelligence cycle designed to reduce the likelihood and impact of data loss by staying ahead of emerging insider trends. Powered by the deep research from Cyberhaven Labs, the service provides:

Policy Packs: Standardized, best-practice policies covering all major exfiltration mechanisms, updated quarterly.

Insider Threat Patterns: An exclusive framework of real-world patterns

AI Risk Research and Governance: Cutting-edge research from Cyberhaven Labs to identify and hunt for emerging AI-driven risks.

Program Recommendations: Expert guidance on operationalizing your insider threat program across HR, legal, and other business units.

IRIS includes quarterly deliverables on top of our existing Analyst Services, including:

- Quarterly insider threat patterns
- Quarterly Insider Risk Program Maturity Assessment
- Program and Workflow Consultation
- Biannual Executive Insider Risk Review
- Insider Risk Community Access

Delivered by Cyberhaven Senior Analysts, IRIS combines threat intelligence, program assessment, and prescriptive workflows to help you operationalize insider risk across your business.

Learn more about Cyberhaven IRIS.

cyberhaven