mimecast
The Connected Human Risk Management Platform

5 Ways the Damage from Insider Threats is Hiding in Plain Sight

The rapid shift to cloud-based systems and remote work environments has significantly expanded the risks of insider threats. The challenge lies in the fact that insider threats often seem less harmful compared to external ones – which makes them much harder to identify and address effectively.

WHAT YOU MIGHT SEE | **WHAT'S HIDING BENEATH**

Actor

Trusted colleagues

Instead of highly organized and resourced nation state or criminal actors, insider threats come from employees and contractors with shared interests and values.

Authorized access raises no alarms

Inside actors don't have to hack in — they already have the keys to move about without arousing suspicion.

Intention

Rarely Malicious

Most employees are genuinely trustworthy and are just trying to work faster and smarter.

Damaging regardless of intent

Exposing IP or sensitive data causes serious damage to the business — regardless of intent.

Speed & Breadth

Isolated incidents

Insider threats are typically isolated incidents involving a specific set of files.

Undetected and persistent

Insider threats typically go undetected for months — or years — giving your IP or sensitive data more time to fall into the wrong hands.

Incident Response

Shared responsibilities

Security teams aren't on their own — HR and Legal play a critical role in response.

Collaborative response depends on full visibility

Security needs to detect the issue and give definitive context to HR and Legal ASAP to enable effective response.

Business Impact

Won't bring business to a halt

There's rarely an urgent race to block insider threats, which require a more nuanced approach to understand the context.

Losing IP = losing competitive advantage

Insider threats target the most valuable information in your business: your IP. Day-to-day business will keep running, but leaked IP can be exponentially more costly in the long run.

The Way we Work has Changed. It's Time Data Protection Changed Too.

60%

of employees in midsized businesses admit to moving work files to their personal accounts.

$15M

The average cost of a single insider threat incident.

99%

of companies are using traditional DLP solutions, but despite this, insider-driven data events are increasing.

See the Incydr Approach

Security teams need a new approach that gives you the visibility, context and controls needed to stop valuable data from going to places you don't trust without slowing the business down. **Learn More About Incydr**

mimecast

| US-07275