mimecast

How to build an effective, low-lift response strategy for Insider Risk

Best practices to tackle insider threats and data loss events using Incydr

APRIL 2023

Your response strategy is one of the most critical components to successfully stop data loss from insiders. Unfortunately, addressing Insider Risk is inherently difficult because it involves employees, has the potential to take too much of security's time, and has a large impact on your corporate culture.

This whitepaper outlines what a successful response strategy should look like and provides tips on how the response controls Mimecast offers should be applied to key Insider Risk scenarios.

First, every Insider Risk response strategy should leverage both administrative and technical controls.

Administrative Controls: Used to define expectations and reduce the frequency and intensity of threats.Can be used to establish and change culture.

Technical Controls: Used to contain, prevent, and remediate threats.

But having the controls is not enough. How they are applied is arguably the most important factor to the success of our program. We offer a wide range of technical and administrative response controls – and help you know when to use them – so you can stop data loss from insiders in an effective, repeatable and scalable way. Here's how.

The right response control for every insider activity – from mistake to threat.

Communicate

Set expectations with users on how they should use data and corporate assets.

Acceptable use policy, communications, and trainings

Ideal for:

- Reducing the frequency and severity of risky file activity
- Ensuring employees know and acknowledge expectations

Respond with confidence

1 Communucate

2 Correct

3 Block

4 Contain

Correct

Deliver tailored, microtraining videos to correct everyday mistakes and low-risk actions.

Instructor microtrainings

Ideal for:

- Automating response to low-risk events
- Delivering empathetic correction and ensuring accountability
- Changing user behavior to reduce risk over time

Block

Block your highest-risk users from sending data to untrusted destinations.

Real-time blocking

Ideal for:

- Departing employees, repeat offenders, contractors
- Supporting security and compliance frameworks

Contain

Ensure insider threats aren't able to damage the business.

Access controls, device quarantine, revoke file sharing

Ideal for:

- Active insider threats
- Use during hands-on security investigation

Last year, cloud storage uploads/syncs accounted for 57% of all data exposure events.

Response Best Practices by Scenario

1 Use of unsanctioned cloud applications

Unsanctioned cloud apps is the number one way files leave organizations today. Last year across Mimecast Incydr's customer base, cloud storage uploads/syncs accounted for 57% of all data exposure events. The top 3 unsanctioned (personal) destinations used were:

- Microsoft OneDrive
- Dropbox
- iCloud

Commonly, the files at risk were sourced from locations that house strategic business documents, source code, and customer information. These sources included internal domain sites, Gitlab, Box, Github, Jira, and Salesforce.

Security teams need to be able to address this widespread cloud and Shadow IT risk in an automated way that is effective and scalable. The best way to address this is by implementing administrative controls.

This might look like **implementing an Acceptable Use Policy** that all employees acknowledge regularly. The policy is used to communicate expectations. Mimecast provides our customers with **templated communications** and policies to do this.

Next, users must be held accountable for missteps. This can be done using **integrated training lessons** that are automatically sent to users in order to correct them when Incydr detects files moved to unsanctioned apps.

Because employees know their file activity is monitored and they have been trained to work differently, future events are prevented and risk decreases over time. Employees who do not modify their behaviors become repeat offenders who face additional consequences.

2 Repeat offenders

When employees do not "get with the program" despite clear instruction and training, security teams can put them on an **Incydr watchlist for repeat offenders**. This increases the risk score associated with these employee activities and allows security teams to view and manage their activities separately from other users.

An additional control that could be considered at this time is to add **real-time blocking with the ability for the user to confirm they would like to override the block.** This allows users who are simply working fast to think better of their actions. If they instead choose to move forward with the file upload, it proves intentionality. The user's behavior can then be escalated to a manager, HR representative, or legal team for action, if needed.

3 Departing employees

Incydr product data shows departing employees are often twice as likely to exfiltrate company data than other employees in your organization. That's why we've developed purpose-built workflows to help you manage this common insider risk scenario.

Incydr integrates with HR and ticketing systems to ensure that **departing employees are automatically added to watchlists** for enhanced monitoring. This allows you to manage and review their activity more easily. Incydr will display their departure date and increase the risk score associated with untrusted departing employee activity.

In addition to alerts, Incydr provides security teams with a departing employee risk report for all exiting employees. This allows them to perform consistent and efficient activity reviews for everyone before departure to ensure no corporate data leaves with the employee. While reviewing a user's activity, **Incydr provides you with the exact file that was moved** so you can see its contents and determine its sensitivity.

Security teams can choose to utilize **real-time blocking** for departing employees. This can be a good option to prevent data from leaving and reduce the event volume security analysts need to review. When doing so, security teams should understand that blocking discourages non-malicious activity but can encourage workarounds when users are intent on exfiltrating data. Incydr will surface this kind of high-risk activity through alerts and the departing employee risk report.

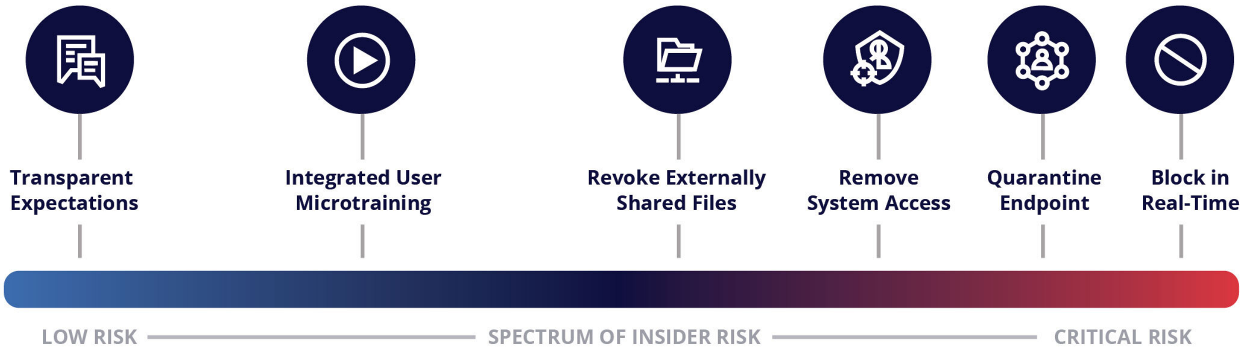
4 Contractors

Organizations in every sector depend on independent contractors, vendor partners and consultants to provide temporary help using their specialized knowledge and skills. However, contractors with authorized access to company data can exfiltrate data and damage the business.

Contract employees should be added to a **Contractor watchlist within Incydr**. Incydr can automatically add them using data from your identity management system. This allows you to manage and review their activity more easily and increase the risk score associated with untrusted contractor activity.

Some security teams will choose to **implement prevention controls** for contractors. For example, you may choose to disable their ability to share files from your corporate cloud collaboration tool (Microsoft OneDrive, Google Drive, Box) to someone outside your organization.

Tailor your response to Every Insider Risk – from mistake to threat



5 Insider threat investigations

Real insider threats can be deterred but will never be completely avoided. The key is to detect, contain, investigate, and remediate these incidents as quickly as possible in order to reduce impact.

While investigating, security analysts may want to **contain active insider threats by quarantining the endpoint or removing a user's system access** by leveraging Incydr integrations with XDR/EDR. This ensures insider threats aren't able to damage the business and perform any further exfiltration.

During an investigation, you can quickly create a Case within Incydr to ensure long-term retention of suspicious events. This includes the exact files and file content involved, which are retained directly in Incydr. Cases allow you to document investigation findings and export them to transfer cases to stakeholders like legal and HR. This purpose-built case management experience drives consistency and collaboration in your insider threat process and ensures appropriate documentation exists should litigation be necessary.

Customers have seen as much as a 36% reduction in low and moderate risk events in just 3 months.

Conclusion

Customers find Mimecast Incydr helps them drive risk reduction in their business in a way that is both more effective and easier to manage than other approaches. It allows security teams to respond to the full spectrum of risk in a way that protects data without disrupting employees or burdening analysts. Incydr allows security teams to get ROI from their programs by driving more secure work habits for employees and ensuring fewer events for security analysts to triage. In fact, customers have seen as much as a 36% reduction in low and moderate risk events in just 3 months.

Only with the Incydr solution, you can:

- Automatically send tailored microtrainings to correct employee mistakes as they happen – driving down event volume and risk to data.
- Contain insider threats and speed investigations, with both integrated case management and access to file contents.
- Block unacceptable data movement without the management burden, inaccuracy, and endpoint impact of content-based policies.

Ready to get started? **Contact us** to learn more or try Incydr in your own environment.

About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.