Playbook

Human Risk Management for Sensitive Data Mishandling

This playbook provides guidance on mitigating risks associated with the mishandling of sensitive data—users who consistently send confidential information to personal email accounts, store sensitive data in unsecured locations, or violate data classification policies. Use this playbook to design and implement controls, policies, and workflows appropriate for your environment and risk tolerance.

Note: This playbook is designed to work across Mimecast Email Security Cloud Gateway, Incydr and Engage – depending on the tools you have deployed you may be able to match functionality in your insider risk/DLP and Awareness training solutions.

Table of Contents

1. Risk Scenarios and Business Impact

Scenario summary

- Users who repeatedly send company-confidential information to personal email accounts, unauthorized recipients, or unsecured/unsanctioned external locations
- Users who repeatedly fail to follow data handling protocols despite prior training and interventions
- Users who consistently ignore data protection warnings and security controls.

Business impact

- Data breaches resulting in exposure of confidential information
- Loss of sensitive customer, employee, or proprietary data
- Regulatory compliance violations and associated penalties
- Financial fraud through unauthorized access to sensitive financial data
- Reputational damage affecting customer trust and business relationships
  Operational disruption due to incident response and remediation activities
- Increased operational costs from repeated security interventions and monitoring
- Legal liability from data protection failures and privacy violations.

Supporting policies, compliance, best practices, or governance

- Policies requiring mandatory training for the mishandling of sensitive data.
- Governance frameworks for escalating interventions based on repeated sensitive data mishandling events.
- Compliance with ISO 27001, NIST CSF, and other relevant standards.
- Best practices for integrating behavioral risk management into security operations.

2. Targeted Security Outcomes

Define high-level control objectives for sensitive data mishandling scenarios

- Raise friction for repeat offenders by implementing progressive enforcement measures that increase security controls and oversight for users demonstrating consistent occurrences of mishandling sensitive data
- Shield users with demonstrable evidence of repeated events with stronger filters through enhanced monitoring, automated detection systems, and protective controls that prevent sensitive data exposure before it occurs
- Add additional protective controls to decrease the likelihood of sensitive loss prior
- Nudge well-meaning but unaware users toward better behaviors using education, just-in-time guidance, and positive reinforcement mechanisms that build security awareness without impeding productivity.

Key outcomes

- Reduce the frequency of offenses
- Foster a culture of accountability and continuous improvement in security behaviors.
- Remove users' ability to claim "I didn't know"
- Minimize the risk of an inadvertent data breach through proactive controls.

3. Control Strategy and Phased Implementation

Mimecast recommends a targeted and phased approach whenever implementing controls that impact users and user productivity. The following outlines how Mimecast email security, Engage and Incydr policies can be applied in a graduated manner to address the risk of data mishandling.

Note: A user's risk level decreases over time based on sustained positive cybersecurity behaviors, typically following a logarithmic decay rate that reduces risk scores from initial incident levels to baseline thresholds within 30 days. This approach ensures that risk-based controls like enhanced filtering, access restrictions, or additional authentication requirements automatically relax as users consistently demonstrate secure behaviors over the decay period, creating dynamic security postures that respond to actual current risk rather than maintaining static penalties based on historical incidents.

Phase 1: Visibility and Nudging

Objective Start by monitoring and gently influencing behavior to establish baseline understanding of data handling patterns.

Enable logging and alerting for key risk behaviors

Alerting for key risk behaviors including unusual data access patterns, large file transfers, and external sharing activities

- Create alerts to monitor for high-risk activity

Apply visual cues

- Apply visual cues that provide immediate feedback without blocking legitimate business activities
- Just-in-time nudges asking "Are you sure you want to share this externally?"
- Introduce user-facing notifications that educate about proper data handling without enforcement mechanisms across their work surface e.g. email, Microsoft Teams or Slack.

Communication

- Consider sending notifications to repeat offenders to advise them of the organizational acceptable usage policies.
- Begin targeted communications campaigns to set clear expectations about data protection responsibilities and organizational policies.

Reference knowledgebase articles:

- [Engage - Behavioral nudges]
- [Incydr – Create and Manage Alert Rules]
- [Incydr - Send Instructor lessons with the Actions menu]

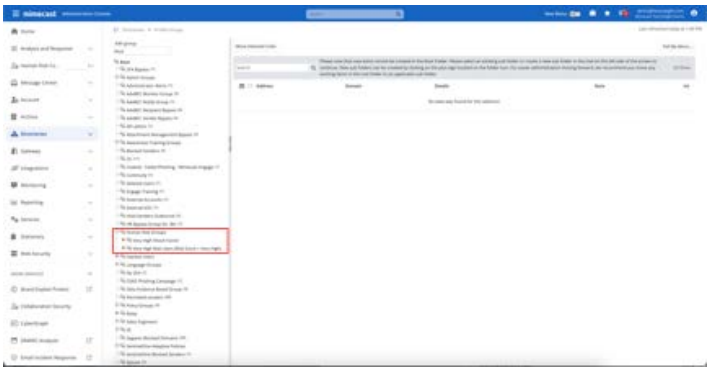
Phase 2: Targeted Enforcement

Objective Introduce friction or oversight without full lockdown.

Policy-based escalation

- ***Auto-escalate based on thresholds:*** Users who trigger multiple risk-based events such as mishandling sensitive data, repeatedly clicking on phishing links or missed awareness

training modules, can be moved to stricter policy groups in both Mimecast and Incydr, increasing oversight and introducing additional checkpoints. The profile groups utilized in this scenario is called 'Very High-Risk Users'.



Require justification for data handling

- Users must provide business justification before accessing designated corporate resources, such as sensitive cloud file repositories or high-risk applications. Incydr captures user-provided rationale and timestamps for audit purposes, evaluating responses against predefined criteria.

Manager or security notification for users who mishandle data

- ***Notification:*** When users exhibit repeated risky behaviors or trigger specific policy violations, generate notifications to designated managers. These notifications should include details about the triggering event, user history, and recommended management actions to facilitate informed decision-making.

Reference knowledgebase articles

[Incydr - Justification prompts]

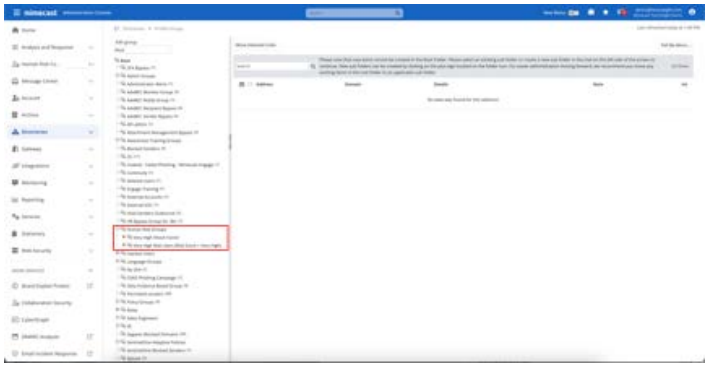
Phase 3: Hard Controls

Objective Enforce high-confidence controls for clear data mishandling scenarios.

Note: While email security systems provide visibility into outbound messages, they remain completely blind to data movement through collaboration tools, cloud storage platforms, and endpoint devices where most sensitive information flows. Incydr leverages real-time behavioral analysis and AI-driven detection to identify risky data handling patterns across all these channels, providing consolidated incident management that correlates activities. This approach delivers the contextual insights needed to distinguish between legitimate business activities and actual data loss events.

Policy-based escalation

- ***Auto-escalate based on thresholds:*** Users who trigger multiple risk based events such as mishandling sensitive data, repeatedly clicking on phishing links or missed awareness training modules, can be moved to stricter policy groups in both Mimecast and Incydr, increasing oversight and introducing additional checkpoints. The profile groups utilized in this scenario is called 'Very High Risk Users'.



Intercept and review outbound messages

- ***Email Security Outbound Monitoring:*** All outbound messages from data mishandling users are intercepted and placed in a review queue before delivery – this could be further refined to freemail domains and competitors to reduce the administrative overhead. Security teams can evaluate message content and attachment safety through the message tracking before releasing emails to external parties. This holding mechanism works through policy-based triggers targeting the specific profile group, creating a human checkpoint that prevents harmful content from being sent by repeat offenders during periods of heightened risk.
- ***Email Security Content Management:*** All outbound messages can be reviewed against a set of predefined words within a content examination policy. This definition should be maintained to contain words relating to sensitive projects and high-risk data types to ensure that the correct data is identified.
- ***Email Security Outbound Hold:*** As final measure, all outbound emails can be held to ensure that an administrative review is undertaken. This is highly admin intensive option but may prevent an exfiltration point. Notifications can be set for end users to advise them of any action taken.

Limit access to corporate resources

- ***Incydr Access Restrictions:*** For users who consistently demonstrate high-risk behaviors despite lower-level interventions, Incydr implements automated access limitations. These restrictions operate through integration with identity management systems, cloud access security brokers, and endpoint protection platforms to enforce granular controls across. Administrators can define specific limitations, including file sharing restrictions, application blocking, or endpoint controls that activate automatically. Access limitations remain in effect until risk scores decrease through sustained positive behaviors.
- ***Incydr Egress options:*** Reduce the ability to move data from managed endpoints through USB drives, airdrop and other exfiltration avenues.

Integration Note: Mimecast and Incydr can be integrated to synchronize user profiles groups and watch lists, ensuring that high-risk users identified in one platform are automatically reflected in the other. This enables a unified, dynamic approach to human risk management, with graduated policy responses that scale from gentle guidance to comprehensive access restrictions.

General Notes for All Policies

Testing and Pilot Deployment:

- It is best to test each policy in a pilot group before full deployment.
- Follow your organizations change control process for implementation of policy changes.
- Monitor dashboards in the Mimecast AdCon to track effectiveness and administrative overhead.

Optimization Period:

- Policy optimization typically requires 2-4 weeks of operational data to fine-tune detection parameters and minimize false positives while maintaining security efficacy.

Reference knowledgebase articles

- [Email Security - Outbound Hold]
- [Incydr - Access Restrictions]
- [Integrating Mimecast Email Security and Incydr]
- [Human Risk Management - Automated Profile Group Assignment]

4. Stakeholder Engagement and Enablement

How to get people aligned, why this is important and how to approach it (from the perspective of the IT or Security practitioner)

Executive Leadership Team (ELT)

- Champion the initiative publicly and reinforce the importance of addressing sensitive data mishandling.
- Approve policy direction and risk tolerance boundaries.
- Request regular updates on metrics and effectiveness.

Human Resources (HR)

- Coordinate targeted communications and awareness efforts for sensitive data mishandling.
- Align behavior-based policies with HR frameworks (e.g., performance management, annual goals, productivity improvement plans.
- Advise on user impact and consequences for users who mishandle sensitive data.

Legal / General Counsel

- Review controls for potential legal/privacy implications.
- Ensure defensibility in case of disputes or regulatory inquiries.

Security Operations

- Design and implement detection and enforcement logic for users who mishandle sensitive data.
- Monitor and tune controls to minimize false positives.

End User Communities

- Engage users who mishandle sensitive data in feedback loops and training programs.
- Help craft end-user alerts and communications
- Encourage participation in pilot testing for new controls.

5. Response and Operational Support

What to do when the control triggers or alert fires.

Detection Logic / Alert Criteria

Alerts Triggered by:

- User shares corporate data to generative AI tools
- Data is shared to non-sanctioned cloud file shares
- Data exfiltration via abnormal egress points e.g. airplay or USB drives

Response Playbook

1. ***Validate Alert:*** Review user context and action history.
2. ***Escalate:*** Notify the user's manager or DLP team.
3. ***Apply Temporary Restrictions:*** Limit access to sensitive resources or enforce stricter controls.
4. ***Educate User:*** Provide targeted training or guidance.
5. ***Document Incident:*** Log the event in the ticketing system or SOAR platform.

Integration Notes

- Export alerts to XDR/SIEM or SOAR for centralized monitoring.
- Integrate with HR systems for automated manager notifications.

6. Continuous Improvement and Effectiveness Measurement

Effectiveness Metrics

- Reduction in the percentage of repeat offenders over time.
- Decrease in high-risk behaviors among repeat offenders.
- Improved detection and response times for repeat offenses.

User Engagement Metrics

- Percentage of repeat offenders completing targeted training.
- Feedback from repeat offenders on the effectiveness of interventions.

Governance & Compliance

- Conduct quarterly reviews of policies for repeat offenders.
- Align controls with compliance requirements (e.g., ISO 27001, NIST CSF).
- Provide regular reports to the executive leadership team and risk committees.

Profile Group Reference Guide

Making use of Groups in Mimecast

While seeming simple, groups provide the ability to heavily alter how Mimecast functions, and how a user's interaction with Mimecast can be changed.

Mail flow

Mail flow actions are organized in proactive and reactive groups:

- ***Proactive groups*** are commonly professional service organizations and financial institutions, where protecting intellectual property, finances and reputation are key factors.
- ***Reactive groups*** are commonly healthcare, where failure to communicate timely could affect the well-being of a person.

Outbound and Internal

Proactive Actions			
Actions	**Example**	**Prevention Type**	**More Information**
Block a user from sending to the customer's top-10 client or vendor group	High-risk user is not able to represent the company	Supply-chain attack, Insider threat	Using a group that contains a high-risk user and another group that contains the "Top-10" list, a Blocked Sender Policy can be created to prevent the first group from communicating with the second group
Block a user from sending any email outbound	User is not able to use email as a point of data-exfiltration to their personal account	Insider threat, Potential leaver	A Blocked Sender Policy can be applied using the group
More strict scanning is applied to URLs (e.g., questionable, but not outright malicious) in all outbound email from a user, to identify attempted supply-chain attack or insider threat	High-risk user is not able to send a link to a domain similar to their own or a client's domain	Supply-chain attack, Insider threat	An alternate URL Protection Policy can be applied
Prevent a user from being allowed to send specific attachment types, regardless of their scan results	High-risk user is not allowed to send out zipped or password-protected zip files	Supply-chain attack, Insider threat, Potential leaver	An alternate Attachment Management Policy can be applied
Hold all outbound emails for a user	High-risk user is not able to represent the company at all, and messages must be reviewed before going out	Supply-chain attack, Insider threat	A Content Examination Policy can be applied, using the hold action
Flag or hold a user's outbound messages which contain some less confident phrases indicating supply-chain attack or insider threat	High-risk user is not able to send emails with phrases or words of urgency sent outbound, and generate an alert if internal	Supply-chain attack, Insider threat	A Content Examination Policy can be applied, using the hold action
A user's ability to send outbound emails can be throttled altogether, or based on specific patterns in the message	High-risk user is not allowed to send emails at a pace that could resemble a spray-and-pray attack	Supply-chain attack, Insider threat, Potential leaver	A Recipient Limitation Policy can be applied

Reactive Actions		
Actions	**Example**	**More Information**
Outbound messages can be sent as Secure Messages, where we retain chain of custody and can revoke access to those message after-the-fact	High-Risk user's outbound emails can effectively be 'recalled' regardless of the recipient's mail platform	A Secure Messaging Policy can be applied
All User's outbound and internal messages are copied to a security team for manual review	High-risk user's messages are BCC'd to a mailbox for review	A Group Carbon Copy Policy can be applied
User's outbound and internal messages matching specific words or phrases alert a security team for review	High-risk user's messages containing words or phrases of urgency are BCC'd to security mailbox for review	A Content Examination Policy can be applied, with the Group Carbon Copy action
Alerts are generated for any lower-confidence scan on outbound emails	High-risk user sending PDF, Office or zip files outbound alert the security team	An alternate Attachment Management Policy can be applied
Outbound emails have a banner applied indicating that the sender's communication should be confirmed via a known alternative communication method	High-risk user's outbound emails have a "Does this communication seem out of the ordinary? Please call our main office and ask to be transferred to this user for verification." banner applied	A Stationery Policy can be applied

Inbound

Proactive Actions		
Actions	**Example**	**More Information**
Low-confidence phishing emails are administratively held for high-risk users, where they would have been otherwise held at a user level or had a banner apply	High-risk user cannot receive emails with only one or two suspicious indicators	An Impersonation Protection policy can be applied, using the Hold action at an administrative level
Remove some of all attachments from emails, regardless of their scan result	High-risk user is not allowed to receive password-protected zip files that cannot be brute-forced for scanning by Mimecast	An alternate Attachment Management Policy can be applied
Apply more strict URL scanning	High-risk user is not allowed to click on links in a message that are similar to the top-10 vendor/client domains	An alternate URL Protection Policy can be applied
Reactive Actions		
Actions	**Example**	**More Information**
Smart tags can be applied where recipient is a high-risk user and the message contains low-confidence indicators	Messages to a high-risk user with words or phrases of urgency are flagged for review out-of-band	A Smart Tag Assignment Policy can be applied
Low-confidence phishing emails to high-risk users generate an alert	Security team is alerted with a high-risk user receives an email that matched only a single phrase	An Impersonation Protection Policy can be applied, with the notification option configured
Apply more strict URL scanning	High-risk user is not allowed to click on links in a message that are similar to the top-10 vendor/client domains	An alternate URL Protection Policy can be applied

Interaction

Access to Mimecast

Users added to a group can have a reduced experience, removing access to features like:

Feature	Information	More Information
Searching the archive	We retain up to 99 years of customers' emails outside M365 and Google Workspace, which may contain company confidential or proprietary information	An alternate Application Setting can be applied, with search options restricted to disabled
Sending or receiving emails through Mimecast (as an alternative to M365 or Google Workspace)	Mimecast have a continuity product, where a customer can continue to send/receive through Mimecast in the event of an issue accessing M365 or Google Workspace	An alternate Application Setting can be applied, with the option to send emails disabled

Access Restrictions

Access restrictions can be applied, such as:

Restriction	Example	More Information
Restrict access based on IP ranges	Access to Mimecast's archive, continuity, and hold queues can be restricted to physical office locations for potentially compromised users	An alternate Application Setting can be applied, which uses an alternate Authentication Profile
Restrict access to web, mobile apps, Outlook plugin altogether or individually	High-risk users are unable to use Mimecast's mobile app to send/receive email	An alternate Application Setting can be applied, which has specific or all methods of accessing Mimecast disabled
Remove the ability to manage held queue items	High-risk user cannot be trusted to release messages held by Mimecast as spam or graymail (also known as bulk mail)	An alternate Application Setting can be applied, which has queue management options disabled
Remove access to Large File Send (LFS), which can be used to send large files or directories outbound	High-risk user cannot try to use LFS as a point of data-exfiltration	An alternate Application Setting can be applied, which has LFS options disabled

About Mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.