proofpoint®

E-BOOK

Best Practices for Human-Centric Insider Risk Management

Strategies for working cross-functionally to balance privacy, security and culture

Insider threats are a C-level priority

Over a third of global CISOs perceive insider threats as their biggest cybersecurity risk.[1] And they're right to be concerned. According to Forrester, internal incidents are the cause of 22% of data breaches.[2] The problem is that every organisation is open to harm from insiders. They are everywhere—businesses can't get work done without trusting people with access to sensitive data, systems and networks.

It doesn't matter if an insider means to cause harm or does so unintentionally. The result is the same: significant brand and financial damage. This is why insider threat management (IRM) programmes are so important. They can help organisations proactively address insider threats and minimise potential harm.

To be effective, a programme must have processes, procedures and guidelines for handling user data, protecting privacy and keeping intellectual property safe. But establishing all these policies can require quite a balancing act. Given the wide-ranging implications of an enterprise-wide programme, IRM is often referred to as a team sport.

First and foremost, people across the enterprise must be on board. Executive sponsorship is key for ensuring organisational buy-in. And the human resources (HR) and legal departments should be an integral part of the steering committee. But how do you get everyone on the same page to create an effective programme?

In this e-book, we'll provide five best practices for getting teams to work cross-functionally on a human-centric IRM programme that balances privacy, security and culture. This will ensure that your programme is successful.

22%

of data breaches are caused by internal incidents[2]

1 Proofpoint. *Voice of the CISO*. 2024.
2 Forrester. 'Internal Incidents Cause Almost a Quarter of Breaches, With More Than Half Intentional'. 14 March, 2024.

Privacy, security and culture: finding the right balance

Digital transformation has produced a tidal wave of data in recent years. At the same time, intellectual property and sensitive business information has become more vulnerable due to work-from-home policies as well as the proliferation of devices. While it is important to track and secure this data, organisations must do so while balancing user privacy.

In response to these challenges, governments across the globe have issued numerous regulations. Many focus on how to collect personal and sensitive data while protecting user privacy.

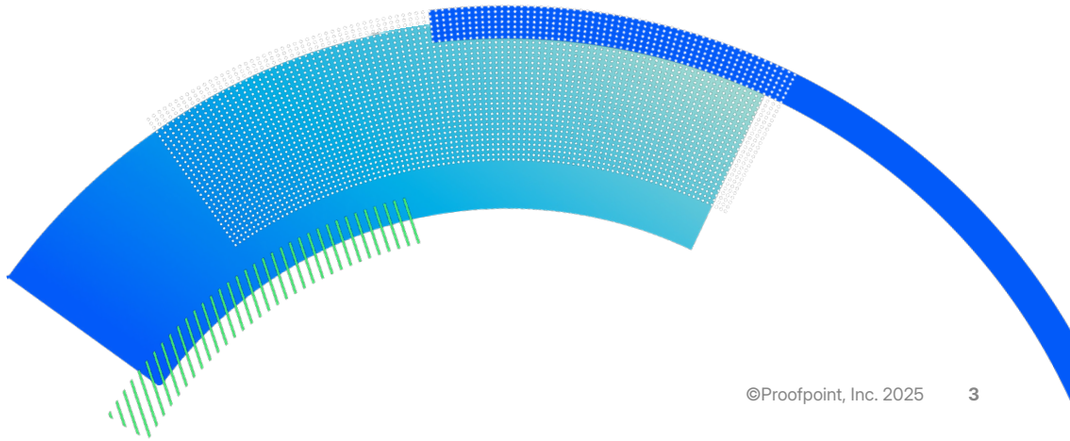
Some examples include:

- **GDPR** (General Data Protection Regulation)
- **CCPA** (California Consumer Privacy Act)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- **LGPD** (Brazil's General Data Protection Law)

As the regulatory environment grows bigger, it also grows more complex. Unsurprisingly, this has meant compliance has become a top concern for HR and legal. To gain their support, you need to address their concerns and questions as you build your IRM programme.

Here are some common questions:

- How will data be collected, used and retired?
- How will user privacy be ensured?
- What checks and balances will be put in place?
- How can intellectual property be protected to minimise risk to the business?
- How can we ensure that the programme reflects our company culture?



5 Best practices for cross-functional IRM programmes

Diverse perspectives ensure that a programme is well-rounded and comprehensive. However, it can be difficult to get multiple departments to agree when there are often conflicting agendas. The following best practices will help you build trust and gain buy-in as you set up your IRM programme.

1: Establish data collection processes

When operationalising your IRM programme, you need to set up processes for collecting and handling personal and sensitive data. These processes are required for compliance reasons. What's equally important is that having these processes helps build trust with departments across your organisation. This data can help present a holistic view of a user—so without them, teams may be hesitant to share their data.

For example, HR systems house employee data that can help with identifying high-risk users and groups, such as departing employees, employees on watch lists and poor performers. Data from multiple teams is a valuable part of any IRM programme as it helps provide context and indictors that help detect risky behaviour. This is why articulating your robust data collection processes is so essential. It helps build confidence in your programme and ensure collaboration.

Your processes must align with your compliance requirements. They should also reflect your company's culture.

It helps to keep these tips in mind:

- Be transparent about the reasons for your IRM programme.
- Be clear about what monitoring entails and how it will operate.
- Review personal data regularly to check whether it still needs to be monitored.
- Create a policy that explains how long personal data should be kept.
- Establish a clear, well documented security and acceptable use policy; ensure that it is checked regularly, reviewed by HR and legal and is kept up to date.
- Inform people about the measures that are in place to protect their data; tell them when any significant changes occur.
- Make sure that only staff who need to view personal data have access to it and are trained how to use it properly.

Having data collection processes helps to build trust with departments across your organisation. This data can help present a holistic view of a user—so without them teams may be hesitant to share their data.

2: Protect user privacy

Clearly, it's important for an IRM programme to identify and address privacy requirements as part of the initial programme design. But while user privacy may be needed to meet compliance requirements, it also has other benefits. When you protect user privacy, you also protect employees' rights and eliminate bias from investigations. As advocates for employees, HR and legal want to ensure that everyone's privacy is valued and protected.

When it comes to protecting user privacy, there are some general focus areas that you should consider.

When you protect user privacy, you also protect employees' rights and eliminate bias from investigations.

FOCUS AREAS	DESCRIPTION
Data minimisation	Limit data collection to essential information relevant to security. Consider what kind of activities should be collected and in which scenarios. Define strict collection policies for screenshots and content inspection.
Transparency and disclosure	Inform employees about the types of data collected and why. This ensures full transparency and reduces privacy concerns.
Data subject rights	Set up an engagement group to evaluate the security data that's being collected and educate employees in submitting requests for data review.
Data security	Safeguard collected data with granular access controls to ensure it's accessed only for the stated purpose and by authorised security operators.

An IRM solution that's built with privacy by design will include technical controls that focus on ensuring privacy. When you're evaluating IRM solutions, look for these features.

SUGGESTIONS	DESCRIPTION
Model data collection on approved policies	Streamline compliance by aligning user activity monitoring (UAM) data collection with existing, pre-approved data collection protocols.
Local data storage	Store data locally within countries to comply with regional data residency rules. This minimises cross-border transfer complexities.
Data anonymisation	Anonymise personal data where possible and only use information that identifies an individual when it is necessary.
Dynamic policies	Allow for flexible endpoint controls so that data is only collected when behaviour is risky. This approach ensures privacy and is based on identifying risky behaviour not specific users or user groups.
Granular access controls	Implement role-based access, restricting data use to specific risk-management roles with clear data-use limitations.
Logging and auditing	Maintain logs of UAM data access and use with regular audits to ensure policy compliance and prevent misuse.

It's important to engage stakeholders early in the planning phase. Start discussions with worker councils, privacy specialists and local legal experts to gather their input and align on goals so that you can effectively address their concerns. You will also want to work with them throughout the process of developing your data collection policies as well as guidelines for access controls and data usage.

3: Implement checks and balances

All insiders pose the risk of becoming an insider threat. And security personnel are no exception. For this reason, a formal system of checks and balances—often referred to as a 'watch-the-watcher policy'—needs to be established. This will be particularly important to the legal team, which wants to minimise cybersecurity risk.

The goal of a watch-the-watcher policy is to ensure that no insider has unmonitored access or control. That's why the policy establishes a process to review and validate the actions of insiders with privileged access, like security administrators and analysts.

Elements of a formal policy include:

- Monitor the activities of those who are responsible for oversight and compliance; apply IRM monitoring to all security admins and analysts.
- Review the work of this group and check for errors or inconsistencies.
- Test assumptions and methodologies to ensure accuracy.
- Establish clear guidelines for conduct and responsibilities.
- Conduct regular performance reviews.
- Ensure independence and impartiality in oversight activities.
- Investigate any complaints that are raised about conduct or performance.
- Ensure auditors have resources and authority to perform oversight duties effectively.
- Encourage reporting of any suspected misconduct or violations.
- Ensure security and confidentiality of sensitive information.

Make sure that you have a document trail by running audit reports every week. It is important to pay close attention to security analysts and admins who exhibit unusual behaviour. This could include an analyst who looks into user activity that did not originate from an alert. Or it could also include an analyst who clears their own alerts, which would effectively make the alerts go undetected.

For oversight, designate a security auditor. They can review analyst-, admin- and manager-generated events and clear them weekly. And with their elevated permissions, they will be the only one who can see events within their scope. For another layer of control, events can be reviewed with an internal or external auditor.

It is good practice to create a formal case handling process that recognises exceptions. This process can include everything from not tagging incidents in the tool, which may tip someone off, to documenting events outside of the case management system.

All these practices enable a proactive approach to insider threat management and help to build confidence in the programme.

4: Protect intellectual property and minimise risk

Stakeholders agree that the primary objective of any IRM programme is to protect the crown jewels. Doing so minimises risk and enhances an organisation's security posture.

Unfortunately, insider threats can have wide-reaching consequences, ranging from business disruption to loss of customer trust to financial damage. That's why minimising risk is a top priority for any company's legal team. For this reason, it is common for IRM programmes to be under the purview of legal.

To protect an organisation's intellectual property, legal should work with HR and the security team on acceptable use policies. With these policies documented, employees are aware of the right way to handle sensitive data. Employees who are leaving and joining the company are the most likely to violate these policies. Legal should work with HR, security and other teams to ensure they are thoroughly trained on acceptable use policies so that this doesn't happen.

When an incident occurs, legal will be involved with the escalation and response process. They will want to ensure that all evidence is maintained according to legal standards. Often the forensic evidence captured as part of a security incident will be used in the legal case against the employee. Because the process of maintaining a proper chain of custody is so crucial, it should be developed with the legal team.

To promote trust, make sure that everyone understands the security benefits and privacy safeguards of your IRM programme.

5: Align your programme to the corporate culture

The first step for any successful IRM programme is to gain executive sponsorship. Doing so communicates how important the programme is to the rest of the company. It also helps get other stakeholders on board. And, most importantly, it helps to set a tone for the programme that protecting the company is everyone's responsibility.

Often there can be confusion about the purpose of an IRM programme. Employees may fear that they are being monitored for no reason and that their rights and privacy are being violated. HR will want to preempt and alleviate any concerns. For these reasons and more, it is important to follow these best practices:

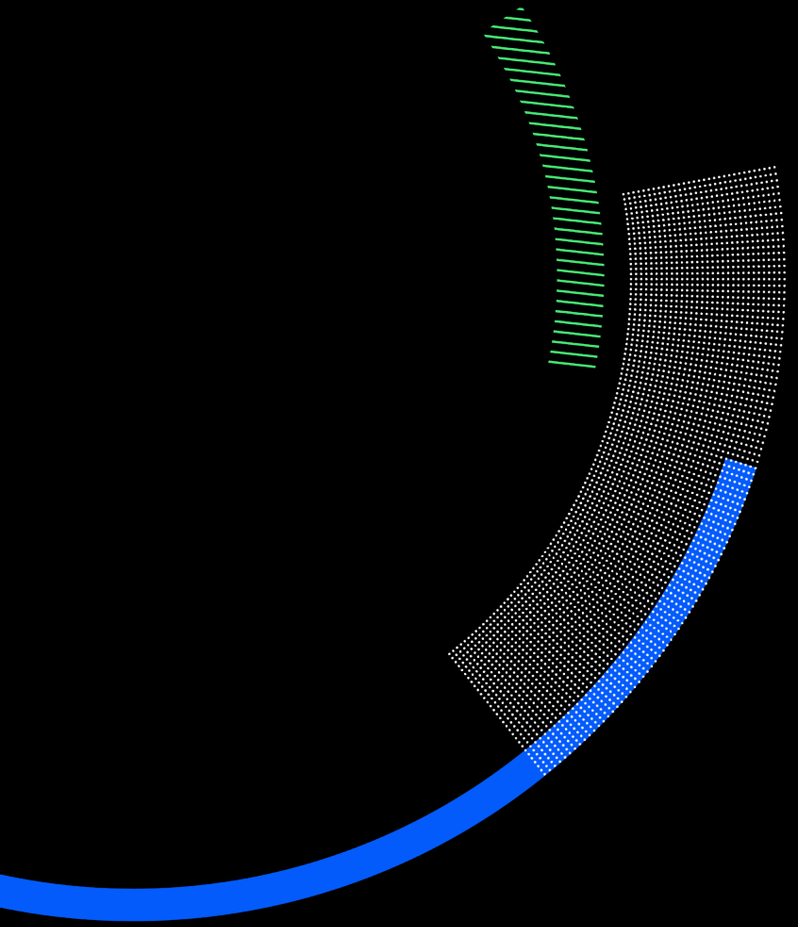
- **Choose a name that fits your culture.** There is no one size fits all when comes to naming your programme. 'Insider risk' and 'insider threat' are common choices. However, some companies have begun to shift away from putting 'threat' in their programme's title. Instead, they're choosing a more inclusive or less aggressive name like 'insider trust'. The name of your programme will also depend on your company's objectives and goals, so it should be reached collaboratively.
- **Explain what monitoring entails and why.** What's the difference between insider threat monitoring and surveillance tools? It is important to clearly communicate how they are different to employees. Insider threat monitoring is focused on the riskiest users. It tracks users on an as-needed basis for security reasons only. In contrast, surveillance tools may be used to monitor employee productivity and provide a holistic picture of the person.
- **Keep communication channels open.** It's important to give your employees ongoing training and support. To promote trust, make sure that everyone understands the security benefits and privacy safeguards of your IRM programme. This will also help remind them that they should take an active role in identifying potential insiders who may be behaving unusually.

Conclusion

A human-centric IRM programme works to balance user privacy with keeping data secure. As you work to set yours up, one of the most important—and challenging—aspects of the process will be striking a balance between security, privacy and culture. The importance of getting this right cannot be overstated.

The key to being successful is gaining executive buy-in. Another critical step is helping teams establish strong partnerships. As everyone works together, they can help to implement policies and procedures that both meet compliance requirements as well as reflect your company's culture. This, in turn, will lay the foundation for a successful programme for years to come.

Learn about Proofpoint solutions for protecting your organisation from insider threats at proofpoint.com/us/solutions/combat-data-loss-and-insider-risk.



proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyberattacks. Leading organisations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.

Connect with Proofpoint: X | LinkedIn | Facebook | YouTube

DISCOVER THE PROOFPOINT PLATFORM →