Building an effective insider risk management program

pwc

Microsoft

Table of contents

Executive summary

The digitization of the business ecosystem has generated new opportunities for growth and transformation of organizations across industries. This digital revolution has also introduced new risks to business operations as cybersecurity threats evolve and proliferate.

While organizations have long prioritized external cybersecurity risks, many are now considering the risks posed by trusted insiders due to the potentially greater damage they can cause. Consequently, organizations are beginning to recognize the importance of establishing controls to combat insider risks.

Several high-profile incidents attributed to insiders have contributed to increased awareness. Recent examples include theft of sensitive data from a leading technology company and sabotage of an automotive manufacturer's operations. Regardless of industry, the impacts of insider incidents are potentially devastating—and financially steep. The average cost of insider incidents has climbed to $8.76 million, according to a study by the Ponemon Institute[1].

Overall, cybersecurity has evolved from an information technology (IT)-centric function to an organization-wide risk management issue. While insider risk management is evolving in a similar way, current market adoption strategies emphasize use of additional tools and technologies to address insider risks without including the underlying principles of risk management

$8.76 million
The average cost of insider incidents across industries[1]

50% of organizations have experienced insider incidents, and frequency has increased over time[2]

[1] The Ponemon Institute, "2018 Cost of Insider Threats: Global Organizations," April 2018.
[2] Crowd Research Partners, "Insider Threat 2018 Report," 2018.

These tools often generate a flood of data—and noise—that obfuscates real insider risk activity. A more targeted approach that focuses on key insider risk scenarios can help reduce noise and enable organizations to rapidly address risks.

Doing so requires an approach that focuses on non-technical elements, such as governance and policy, to guide the effective implementation of technical tools. Organizations that disregard these nontechnical components are unlikely to maximize the value of their technology investments and become frustrated with its output. Tool and technology implementation should follow identification of nontechnical components—and not vice versa.

Successful insider risk management programs are built on a framework that identifies insider risks, quickly takes actions against those risks and matures the program through progressive iterations. This paper charts the journey organizations should follow to successfully combat insider risks. We also include a simulated case study on how the Insider Risk Management tool in Microsoft 365 can help address theft of sensitive data by outgoing employees.

The insider risk landscape

Definition of an insider

Insiders are commonly defined as members of an organization's workforce or as business partners, current or former, with authorized access to, or knowledge of, an organization's assets, facilities, information or people.

Actions of insiders can be intentionally malicious or inadvertently malevolent; regardless of intent, they can cause significant harm. Carnegie Mellon University's Software Engineering Institute Computer Emergency Readiness Team (CMU CERT), a leading insider risk research institution, includes both intentional and unintentional motivations in its definition.[3]

Primary types of insider risks

Insider risks commonly span five categories: espionage, fraud, loss of sensitive business assets (intentional or unintentional), sabotage and physical violence.

Insider risks vary by industry. In healthcare, internal fraud is the most frequently cited type of risk[4], while sabotage represents the greatest risk to IT businesses.[5]

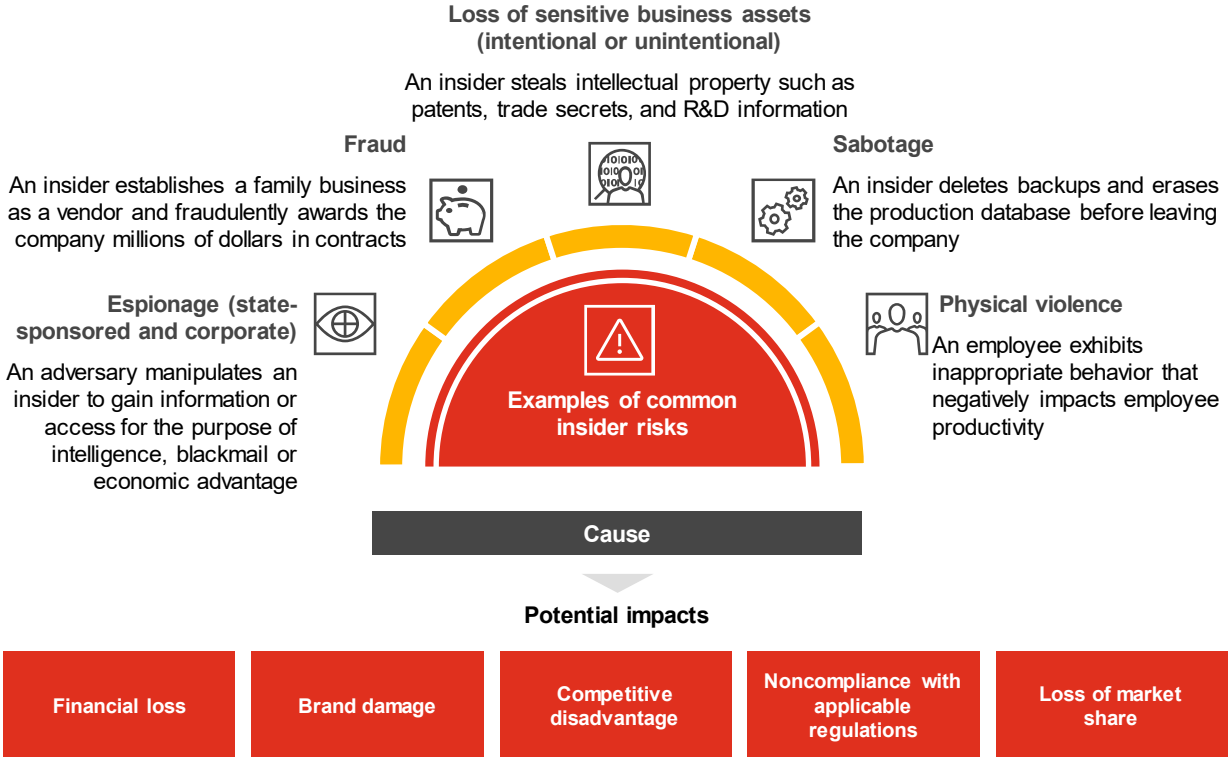
The most common insider risks include espionage, fraud, loss of sensitive business assets, sabotage and physical violence.

[3] Carnegie Mellon University, "CERT Definition of 'Insider Threat' Updated," March 7, 2017

[4] Carnegie Mellon University, "Insider Threats in Healthcare", February 2019. https://insights.sei.cmu.edu/insider-threat/2019/02/insider-threats-in-healthcare-part-7-of-9-insider-threats-across-industry-sectors.html

[5] Carnegie Mellon University, "Insider Threats in Information Technology", February 2019 https://insights.sei.cmu.edu/insider-threat/2019/02/insider-threats-in-information-technology-part-6-of-9-insider-threats-across-industry-sectors.html

The impacts of insider risk also vary by industry and can include financial loss, damage to brand and reputation, competitive disadvantage, noncompliance with regulations, and loss of market share.

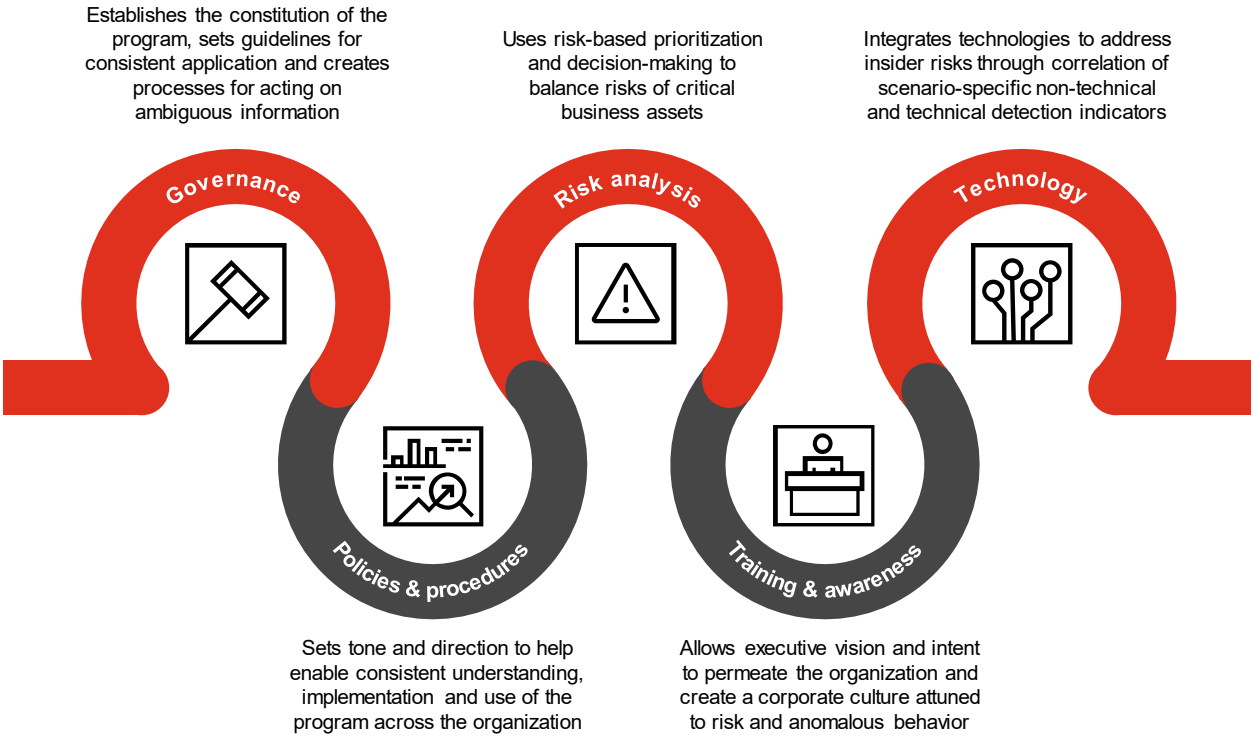


An enterprise-wide risk management challenge

As with many types of cybersecurity risks, it is all but impossible to completely eliminate insider risks. A holistic program that involves key stakeholders across the organization can help to reduce insider risk. Effective insider risk management programs leverage key stakeholders to identify risks and tailor technical controls to address them.

insider risk management programs often focus exclusively on implementing tools and technology without incorporating the necessary organizational, risk management, and cultural considerations. Without using those considerations to fine-tune the collection, the tools are not able to discern between relevant and non-relevant data, essentially searching for the needle in the proverbial haystack. Technology plays an important role, but is just one component of an effective program.

We consider the following five elements critical to an insider risk management program: governance, policies and procedures, risk analysis, training and awareness, and technology.



Effective programs identify and address risks early

Effective insider risk management programs are driven by a cross-functional team that identifies critical assets and related insider risks. These programs typically establish high-risk insider scenarios and identify additional risks as they evolve. They are designed to proactively identify insider activity, achieve early intervention and help reduce negative impacts.

Building a formal insider risk management program is the first step in achieving early intervention.

Building an insider risk management program

1. Establish governance fundamentals

Governance is a foundational element of any successful insider risk management program. Fundamental components include the overall constitution of the program, guidelines for consistent application and processes for acting on ambiguous information.

It is essential to carefully consider culture when drafting the program scope and goals. Culture varies significantly between organizations, industries and geographies, and what may be feasible for one organization may be inconceivable for another. A flexible insider risk management program should address both cultural and geographical concerns.

Culture should be considered when defining the program scope and goals. The program should protect the organization, people, and critical assets without being perceived as an overbearing authority or impeding the organization's goals and operations.

Identify a program owner

One of the first steps includes identifying a program owner (either part-time or full-time) who, alongside executive sponsors, will lead the insider risk team. The owner will be responsible for setting the strategy and direction of the program, as well as providing decision-making oversight and reporting standards.

Program owners need not be aligned with a specific functional area. While ownership can fall under information security, legal, human resources (HR), or physical security, it is critical that the program has broad cross-functional participation and support.

Define an insider risk management program charter

An insider risk management program charter documents the mission, scope, objectives and ownership of the program. The program charter should outline roles and responsibilities among cross-functional teams, executive sponsors and key stakeholders consistent with the organization's culture and operating environment.

Start with the basics: outline the mission, scope and objectives of the program and identify stakeholders.

The program charter establishes a precise definition of insider risk for the organization and outlines coordination among business units and provides a singular organizational view on operational insider risks, budgets, impacts and metrics.

Assemble an insider risk team

The insider risk team facilitates the identification of key risks, implements processes to address risks, conducts investigations and actions lessons learned to help build continuous improvement consistent with the program charter terms.

Begin with stakeholders from business units, HR, legal, privacy and IT. Include additional functional areas as necessary.

The insider risk team should include stakeholders from both the business and corporate support functions. Assembling a working group to determine the operational and day-to-day aspects of the program may be appropriate for larger organizations.

Set key policies and procedures

Policies and procedures help set the tone and direction of insider risk management and help ensure that the program is consistent with the organization's culture.

Start with a few tactical policies and procedures and iterate over time.

The insider risk team should help draft key policies and procedures and enforce consistent application across the organization based on an insider risk perspective. Clearly documented policies and procedures can help prevent ambiguities and set expectations for employee behavior, interactions and use of company assets.

Insider risk policies and procedures should be reviewed periodically and updated as additional risk areas are identified. Examples include:

Insider risk investigative playbook

Outline procedures for conducting insider risk investigations, including escalation, priority matrices and communication protocols

Nondisclosure agreements (NDA)

Serve as a legal contract between the employee and the organization to restrict the use and distribution of confidential data

Off-boarding procedures

Provide a consistent checklist of tasks, including logical and physical access termination, employee and vendor/contractor monitoring and exit interviews

See the insider risk case study to learn more about the role these documents play when an outgoing employee steals information - a common risk scenario.

2. Identify key insider risks

Once governance fundamentals are in place, the insider risk team should identify key insider risks based on the organization and critical assets.

Identify relevant risks

The insider risk team should focus on the organization's most critical assets and how insider risk scenarios could impact them. Scoping discussions should be conducted with the insider risk team and be consistent with the organization's potential risk and culture. Consider any existing controls to help detect and prevent risks. This information can help organizations launch insider risk monitoring.

When identifying insider risks, starting with a pilot business unit can be an effective approach.

Scope the user population

Organizations may be hesitant to implement an insider risk management program that targets a broad base of employees. Many find it more effective to focus on a subset of users who pose greater risk, while also taking into account organizational culture and workplace dynamics.

When scoping the user population, consider the following user attributes:

Role

Focus on roles associated with critical processes, services and sensitive data within the organization

Access

Determine which access profiles are associated with high insider risks; focus on roles that have elevated access to critical assets and data

Behavior

Identify behavioral attributes or events that could heighten a users' risk profile

3. Address identified risks

After key risks are identified, insider risk teams should focus on implementing controls to address them. A first step is to understand the capabilities of the organization's current tools and technologies—and how to quickly utilize them.

Traditional tactics include collecting and correlating logs within a single tool. This approach can be overwhelming, however, and requires significant resources to roll out agents, deploy infrastructure or reduce false positives.

"…insider risk teams should focus on scalable tools that use predefined rule sets or templates specific to the organization."

Instead, insider risk teams should focus on scalable tools that use predefined rule sets or templates specific to the organization. For example, the Insider Risk Management tool in Microsoft 365 offers policy templates designed to help target an organization's key insider risks and can scale with an organization's program.

Insider Risk Management in Microsoft 365 offers built-in scenario-focused policy templates to address insider risks. The Insider Risk Case Study below highlights how to get started.

A foundation for the future

A program that identifies insider risks and uses a blend of technologies and processes to address them is critical to safeguarding an organization's data, users and systems. Given the increasing frequency and severity of insider risks, an insider risk management program can help target risks that potentially have the most significant impacts on business operations. Conducting training and awareness exercises for the insider risk team and relevant stakeholders can help enforce the application of key policies and procedures.

Simulated case study: Theft of sensitive data by employees leaving the organization

One of the most common insider-risk scenarios involves employees who leave an organization —and take sensitive business information and intellectual property with them. This simulated example describes how an organization can build on the insider risk management programmatic elements discussed above to address this risk.

Theft of sensitive data by outgoing employees is a significant risk for organizations across industries.

Insider risks to a global business

Contoso Corporation is a fictional multinational conglomerate that manufactures, sells and supports more than 100,000 products. Following high-profile media reports of insider risks to industry peers, the company appointed a program owner to establish an insider risk management initiative.

The program owner assembled an insider risk team to formalize and ratify an insider risk management program charter. The team included stakeholders across functional areas, including primary business units such as manufacturing, sales and support.

Team members established key policies and procedures that are aligned with the company's strong organizational culture. The scope of Contoso's insider risk management program is limited to employees exiting the organization and requires that employee identity remain pseudo-anonymous unless proper authorization is obtained.

The team conducted workshops with relevant business units to identify key insider risks to critical products and services. Not surprisingly, theft of sensitive data by outgoing employees was identified as a leading concern. Contoso chose the Insider Risk Management tool within Microsoft 365 Enterprise to help address this risk.

Implementing detection controls

The Insider Risk Management tool in Microsoft 365 can apply insider risk management policies to specific users.

Contoso's insider risk team worked with the organization's IT department to implement the insider risk management controls built into Microsoft 365's Insider Risk Management tool. The company implemented a departing employee data theft policy template that included these detection indicators:

Resignation date set

Identifies the resignation date for individual employees

File(s) printed

Determines the number of files printed and the data labels applied to the printed files

File(s) copied to USB Drive

Determines the number of files copied to a USB device and the data labels applied to the transferred files

File(s) downloaded from SharePoint Online

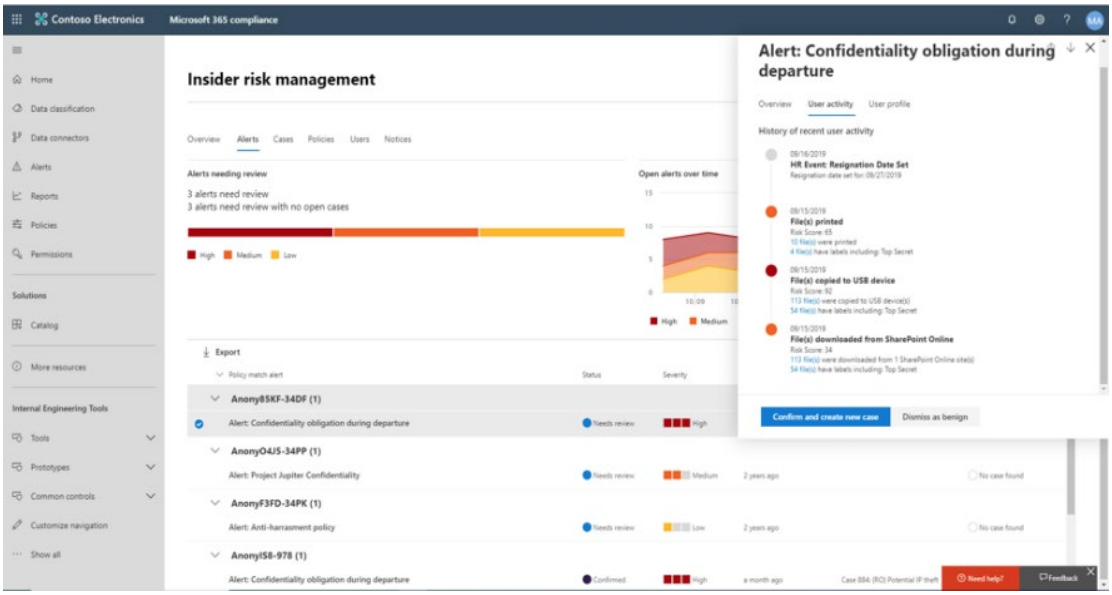
Determines the number of files that were downloaded from SharePoint Online and the data labels applied to the downloaded files

Responding to policy match alerts

Insider Risk Management's policy-match alert feature generated an alert for a departing employee who downloaded files from SharePoint Online, printed documents and copied files to a USB drive. A number of these files were designated as Top Secret using sensitivity labels.

Insider Risk Management curates numerous signals to produce scenario-specific alerts.

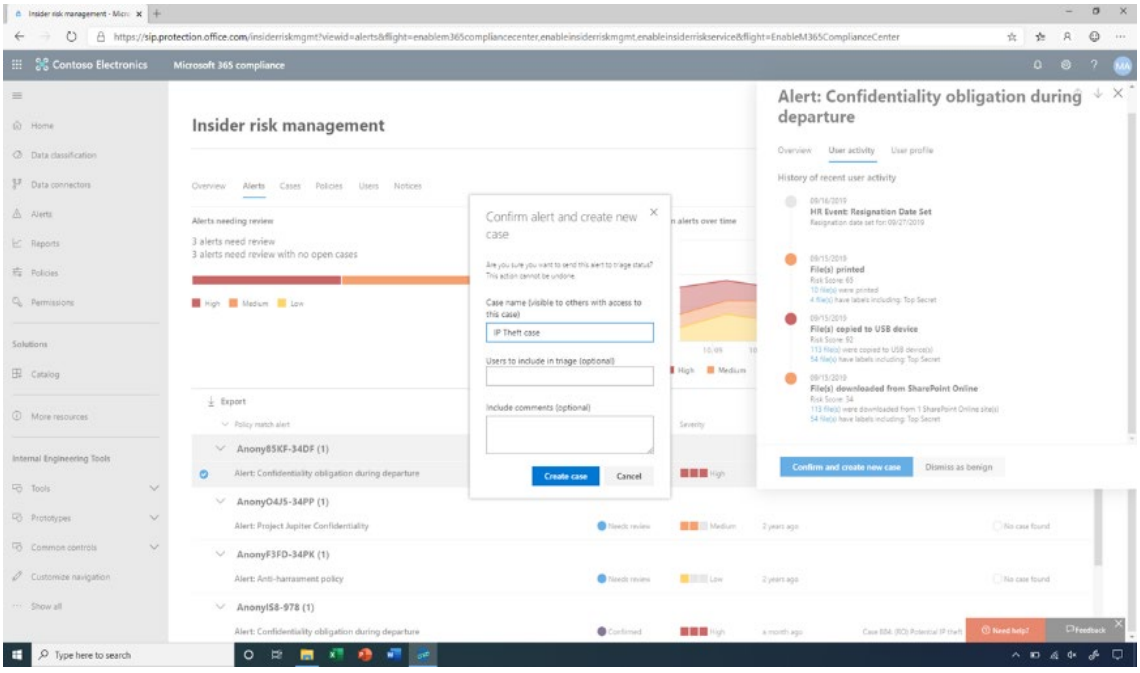
A member of the insider risk team initiated an investigation based on guidelines outlined in Contoso's investigative playbook. Per Contoso's pseudo-anonymity policy, the user's identity was unknown to the investigator.



Creating a new case

Not all alerts are associated with intentional malicious activity. Unintentional activity can result from a lack of awareness on data protection policies.

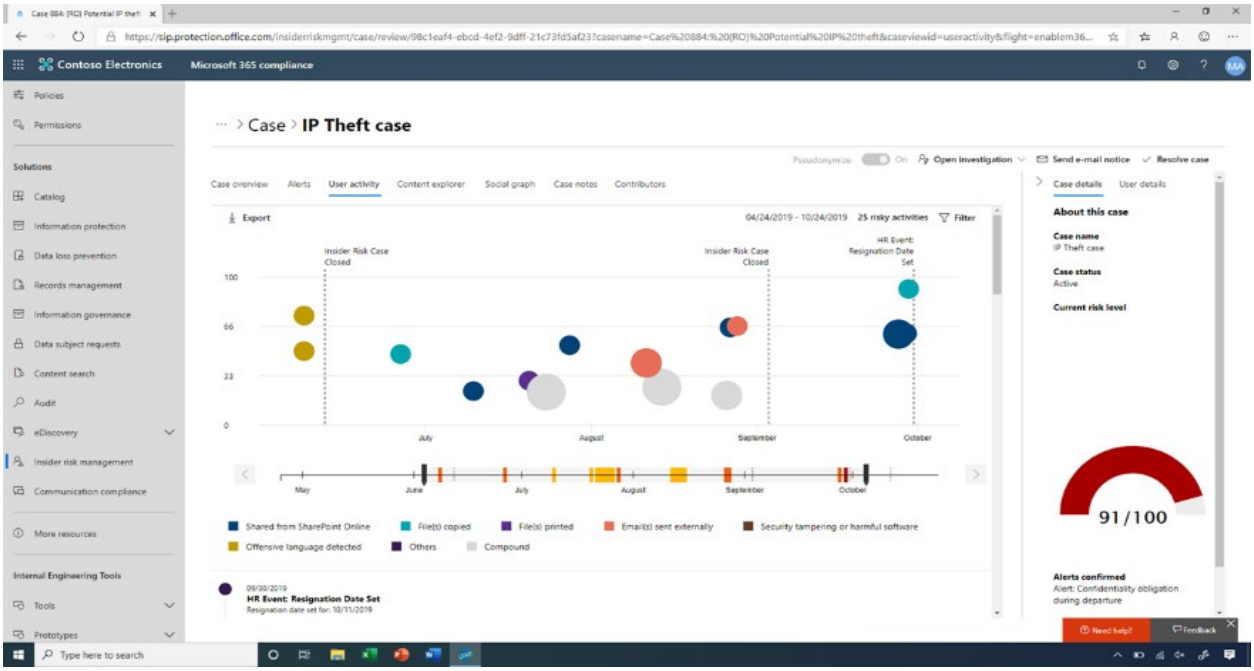
The investigator was unsure if the user's policy infractions were malicious or unintentional. As a result, the investigator used the tool to create a new data theft case for further review of the alert and the details and circumstances associated with relevant policies.



Viewing historical insider risk activities

After creating the case, the investigator used the case dashboard to uncover a history of user activity. Further analysis revealed that the user carried out-of-policy activities months before their resignation date, including use of offensive language, copying and printing files, sharing of SharePoint Online documents and sending email to external accounts. The tool also risk-ranked this alert higher, given the user's history. Based on these findings, the investigator escalated the severity of the case.

When investigating user activity, assume positive intent unless repeated policy violations occur. Use the risk score to rank the severity of the case.



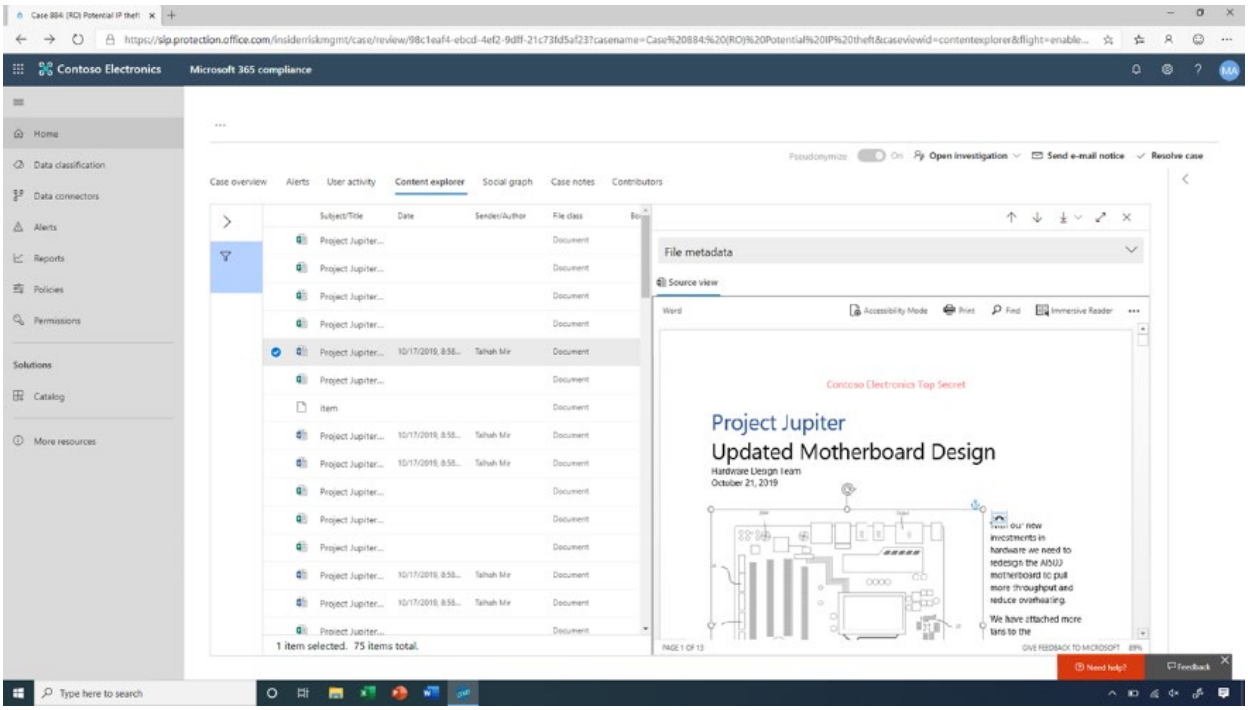
Identifying potential data loss

The investigator used content explorer to determine what files were copied to a USB drive. Content explorer displayed available data files and email messages associated with the user policy alert and allowed the investigator to filter this data by attributes including the data source, file type, tags and conversations. The investigator approved access to the tool based on user rights for additional insider risk team members to conduct triage to determine if user activity was benign or malicious. The team determined that the user copied Top Secret files that included motherboard design blueprints.

Taking further action

Insider risk management allows users to incorporate case notes and send notifications to relevant stakeholders for further action.

The potential theft of valuable intellectual property warranted case escalation. Using the case dashboard, the investigator initiated an open investigation. In this situation, the investigator categorized the case as an employee issue, including case notes and notifications to relevant stakeholders for further action.



Removing pseudo-anonymity to investigate

The investigator removed the pseudo-anonymity of the employee to determine the identity of the user – a SharePoint Administrator. Using this information, the insider risk team collaborated with key stakeholders across functions to gather additional facts that would help determine the right course of action.

The investigation helped the company quantify the risk within an appropriate timeframe and quickly take action.

It was noted that the SharePoint administrator had been flagged earlier in the year for copying data to a USB drive and for sending external emails. This evidence, combined with HR interviews and other supporting information, confirmed malicious intent. Consequently, the organization took legal action against the employee.

Feedback loop and lessons learned

After closing the case, the insider risk team drafted a follow-up report to debrief stakeholders on lessons learned from the incident

Contacts

John Boles
Principal
john.boles@pwc.com

Sloane Menkes
Principal
sloane.menkes@pwc.com

Matt Gregson
Director
gregson.d.matthew@pwc.com

Raman Kalyan
Director Product Marketing
raman.kalyan@microsoft.com

Talhah Mir
Principal Program Manager
talhahm@microsoft.com