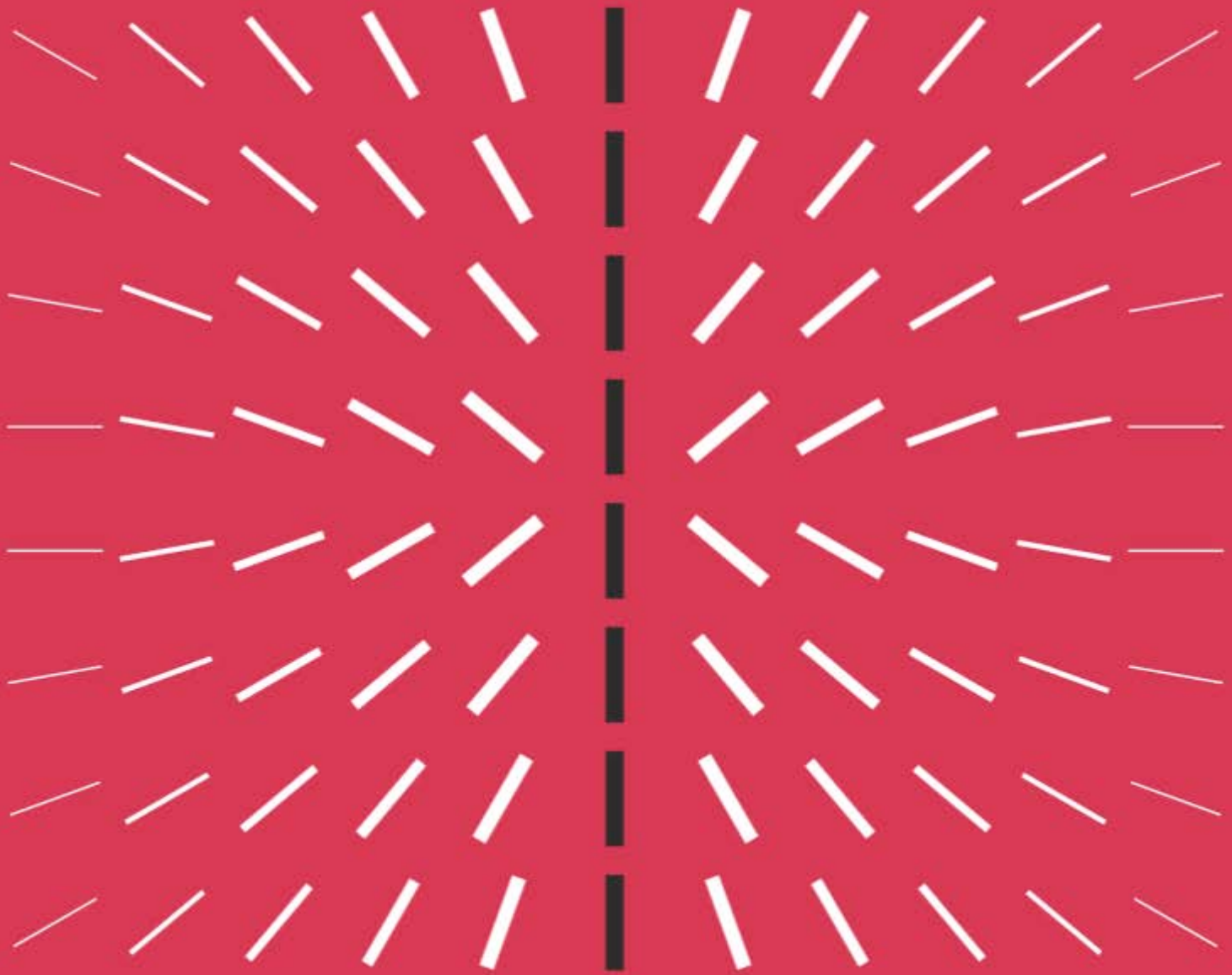
A pragmatic and threat-based approach to address cyber insider risk

PwC Cyber Security



pwc

Table of contents

Insider risk – what's happening?

Cyber security has historically prioritised securing organisations from external malicious threat actors. Less focus was spent to secure organisations from internal actors creating an inherent implicit trust relationship between organisations and their employees.

Organisations are continuing to transform business processes and IT to remain competitive and adapt to technology innovation and business continuity threats. The adoption of cloud and other third party managed services and partnerships, as well as changes in working practices and human behaviours as a result of the pandemic have contributed to a growth in the cyber insider threat attack surface by providing internal users with new means and opportunities to exceed or misuse their access and knowledge to harm an organisation. For example many organisations have introduced hybrid working by establishing new remote working capabilities and increasing the allowed usage of personal devices within a short period of time. Physical access controls and Acceptable Use Policy are less effective and careful consideration should be paid to ensuring that technical controls which were primarily designed for an office environment remain effective for remote workers – this consideration must also be extended to third party contractors and service providers, such as those providing routine engineering support to IT systems.

Insider risk events are varied and in our experience the top three cyber insider risks which we have observed through our analysis of scenarios are:

1. Loss / theft of sensitive data and intellectual property (IP) – this was observed by two incidents with vastly different intentions but similar impacts. The first incident involved an insider working for an IT provider who was able to abuse their knowledge and privileges to steal customer data from a Multinational Bank, and the second involved an insider working at a major European Bank who leaked data about their customers.
2. Fraud and financial crimes – this was observed by an insider working at a financial technology company who abused their knowledge of a cyber breach to perform insider trading activities.
3. Sabotage and service disruption – this was observed by an incident involving an insider working for a multinational automotive company who made direct changes to company source code to sabotage systems.

Business executives are becoming increasingly concerned about cyber insider risk and are asking the following questions

The purpose of this whitepaper is to help answer these questions by:

- Giving readers an understanding of the different types of cyber insider threats, and where to begin focusing on building a programme to help mitigate the risks.
- Defining the responsibilities of each function / stakeholder to provide organisations with guidance on how they approach and tie each stakeholder into the programme.
- Providing our point of view on how to understand and mitigate key cyber insider risks.
- Exploring how to use insider threat scenario modelling and an insider threat control framework (e.g.: resources provided by Mitre, UK Centre for the Protection of National Infrastructure, Carnegie Mellon) to identify the key mitigating controls for insider threat attacks.

At the end of the whitepaper, readers will have an understanding of why insider threats are important to organisations now, the main reasons insider risk programmes fail, and understand the key components to successfully mitigate cyber insider risk.

Key Insights

Our experience of helping organisations identify, prioritise and mitigate their insider risks has helped us to develop key insights. These are outlined below to help organisations that are developing their business case for investment or continue reducing their insider risk.

1. The worst case scenario of an insider threat could cause significant business and technology impacts, potentially greater than that of external threat actors. This is because insider threats have intimate knowledge of business processes and critical assets, where control deficiencies exist and how to potentially bypass controls.
2. An insider threat is typically much harder to detect, and once detected the incident response team must prove it is not a compromised user. Forensics will play a vital role in confirming if an incident is a result of a compromised-user or an insider threat and Legal should be involved to advise on the information that is required to prove an insider threat case.
3. Most organisations do not have a single accountable owner or forum focused on understanding and mitigating the risk posed by insider threats on a day-to-day basis.
4. The likelihood of an insider threat attack has increased in recent years due to the adoption of Cloud and other third party managed services and partnerships which has increased the number of people outside of the organisation's direct control with access to critical assets, as well as changes in working practices and human behaviours as a result of the pandemic.
5. Addressing insider risk requires a collaborative effort across the business who understand their processes and data better than others and can advise what an insider may look like. This will help to break down silos in risk management decisions.
6. Whilst zero-trust (which is an information security model that denies access to applications and data by default[1]) is becoming a buzzword in our industry, there are key guiding principles which if adopted can support an organisation's strategy to becoming cyber-resilient. Addressing insider risk will help organisations to implement some of the principles such as; assuming attackers are operating beyond perimeter-facing defences (assume breach), verifying trust explicitly (not implicitly trusting those who present as genuine), and implementing least-privilege and context-based access controls. This will reduce the attack surface by ensuring only permitted users on permitted devices / locations can access critical information and services. Such preventative controls can also reduce the number of users requiring enhanced monitoring and improve return on cyber security investment.
7. Identity and access management controls offer the greatest coverage of mitigating attack vectors for insider threat scenarios which are attributed to a broad set of insider threat attack categories e.g. loss / theft of sensitive data and IP, sabotage and service disruption, and insider fraud.
8. According to research from the 2022 Ponemon Institute Cost of Insider Threats Global Report[2] the most frequently occurring insider threat incidents are negligent insiders (56%) and incidents due to credential theft (18%). In our experience the key opportunities to reduce the likelihood of these threats include a focus on building a strong cyber culture, upskilling employees to handle confidential information securely without impacting business objectives and processes, and using a combination of technology and human-awareness training to identify social engineering attacks.
9. Insider risk programmes tend to deliver less benefits when technology is implemented without taking the time to identify and understand why they are being deployed i.e. the specific insider risk scenarios that exist for an organisation's users and assets. Without taking this initial step, programmes can become overwhelmed by a high noise-to-benefit ratio. This is strongly noticed when organisations implement threat detection tools and rely on out-of-the-box detection rules that eventually get turned off.
10. It is challenging to write detection rules specific to malicious insider activities without identifying insider threat scenarios for specific business assets or by obtaining business and people intelligence to indicate higher risk user groups. Without this information, organisations should focus resources to improve their threat detection and response capabilities on ensuring the incident response processes and forensic capabilities are in place to support compromise discovery and post-incident investigation activities. Ensuring users are aware of this capability throughout the organisation will also help to deter opportunistic insiders.

Introduction – Insider threats are underestimated and harmful

What is an insider threat?

Insiders are current or former members of staff of an organisation and its third parties, with authorised access to, or knowledge of, an organisation's assets, facilities, information, or people. Insiders become a threat when they willingly, knowingly or accidentally exceed or misuse that access to harm the organisation.

Did you know?

Many organisations focus mainly on the risks posed by external threats, however **recent events have increased the likelihood of an insider threat attack** such as; extending access to your business environment to include unmanaged third parties and suppliers, and supporting new hybrid and remote-working practices following Covid-19. **Many organisations are lacking a single accountable owner for managing insider risk** on a day-to-day basis.

Why is insider threat a concern?

The **worst case scenario of an insider threat has significant impact**, potentially more than threats caused by external actors **due to the insider's intimate knowledge** of the business, location of critical assets, **and understanding of how controls work and how to potentially circumvent them.**

Be aware!

Insider threat types can vary between malicious and accidental insiders, and can extend to third parties and contractors. Insiders can also be used as a nexus by external threat actors to gain access to your network.

Insider threat activities are much harder to detect and prove, and are likely already occurring more than organisations are aware.

PwC's approach to help you understand and mitigate insider risk involves building a strategy, organising your teams, measuring and prioritising risk, and uplifting your controls. The benefits of this approach are:

- Removes silos in risk management which will provide efficiencies
- PwC UK agrees that zero-trust is becoming a buzzword in our industry, however some of the guiding principles will help organisations move from cyber-secure to cyber-resilient. Our Insider Risk mitigation approach will support your zero-trust strategy by implementing key guiding principles such as; assuming attackers are operating beyond perimeter-facing defences (assume breach), verifying trust explicitly, implementing least-privilege and context-based access controls.

In our experience insider threats can be broadly split into three types:

Malicious Insider Threat

- Will take actions to harm an organisation for personal gain or act on a grievance.
- Can be motivated by internal influences (e.g. to "get even") or external influences (e.g. to pay off debts).
- Impact can vary based on whether the insider has privileged access or non-privileged access.
- The research from the 2022 Ponemon Institute Cost of Insider Threats Global Report[2] estimates malicious insiders accounted for 26% of insider incidents.

Accidental Insider Threat

- Impacts the organisation through mistake (e.g. sending sensitive data to incorrect recipient, opening a URL or attachment from a phishing email) or carelessness (e.g. allowing someone to tailgate behind them, or ignoring security update/patch messages).
- The research from the 2022 Ponemon Institute Cost of Insider Threats Global Report[2] estimates negligent insiders accounted for 56% of insider threat incidents, and 18% of insider threat incidents involved credential theft.

Third Party Insider Threat

- Typically contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work. For example; service providers carrying out engineering support.

According to Microsoft Market Research, 93% of organisations are concerned about insider risks and 25% of all data breaches are due to insider activity[3].

According to the 2022 Ponemon Institute Cost of Insider Threats Global Report[2] which analysed the results of 6,803 insider incidents across 278 organisations:

- Credential thefts have almost doubled since 2020 and accounted for 18% (up from 14% in the previous 2020 report) of insider incidents with an average cost of $804,997 per incident. This is largely through phishing attacks but can also occur through insider implants who sell their credentials and multi-factor authentication access. This may be attributed to an increase in the sophistication of phishing attacks following the pandemic.

  Our security researchers have observed high profile ransomware groups such as LockBit attempting to recruit malicious insiders that are motivated by finance or revenge on the dark web for a return on ransomware payouts. Our analysis suggests this is because threat actors require significantly less effort to gain privileged access, locate critical assets and execute malicious payloads with the help of an insider, which removes the need to operate with initial access brokers acting on opportunistic zero-days and other vulnerabilities.

- Negligent insiders accounted for 56% of insider incidents (down from 62% in the previous 2020 report) with an average cost of $484,931 per incident. Increased awareness of this type of insider threat and details collected through granular incident root cause analysis shows that this is a result of activities such as; forgetting to patch or upgrade devices, and not working in compliance with company policy requirements.

  Our Global Threat Intelligence team has also observed nation state threat actors using social engineering tactics through LinkedIn and fake recruitment websites to target accidental insiders with malicious payloads in the form of job descriptions, application forms and interview guides, which was presented at BlackHat USA 2022 and can be found here.

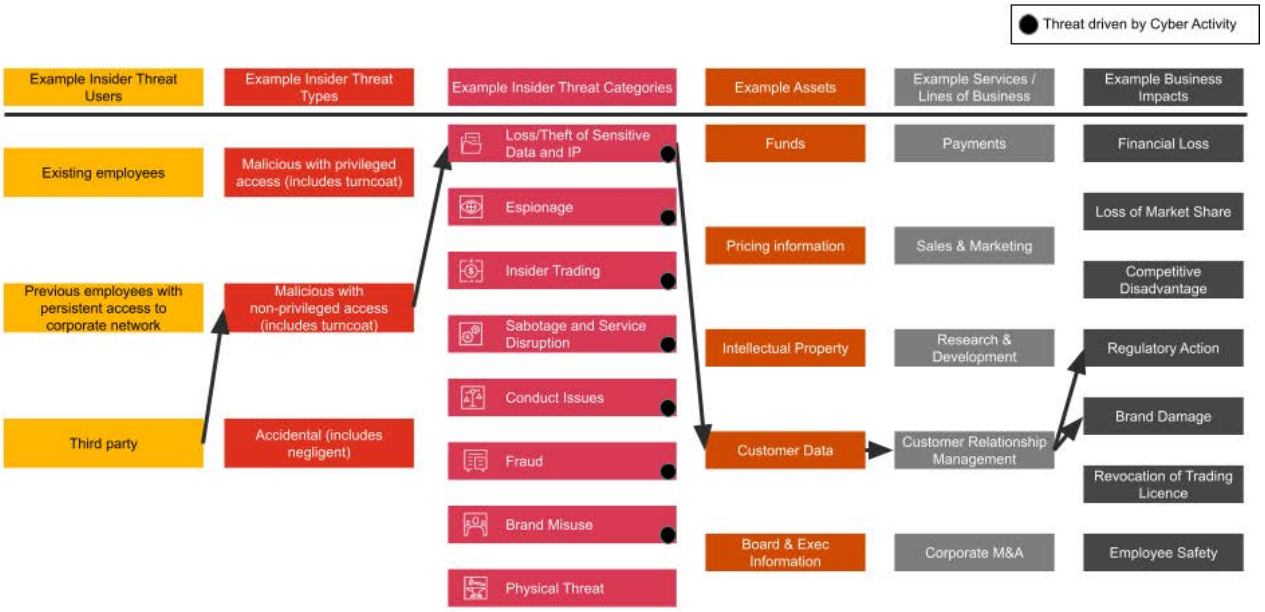
- Criminal / malicious insiders accounted for 26% of insider incidents (up from 23% in the previous 2020 report) with an average cost of $648,062 per incident. This may be attributed to the changes in a user's means, opportunities and intentions following a shift to remote working and changes in human behaviours during and after the pandemic.

Establishing the foundations for a successful cyber insider risk program

A successful cyber insider risk programme is underpinned by a strategy which defines the programme scope and goals and is driven by a cross-functional team. The strategy should consider the organisation's business strategy, industry, culture and geographies – for example if the business strategy is focused on acquiring smaller fintech and startups then greater focus should be placed on protecting against theft of Corporate mergers and acquisitions assets, or if the business strategy is focused on driving innovation then greater focus should be placed on research and development, and protecting against the theft of intellectual property assets. Organisations should begin by prioritising their strategy to focus on the highest risk cyber insider threat categories based on the business and technical impacts caused if a critical asset is compromised or taken offline. Over time the strategy should be revisited and iteratively evolved to cover broader cyber insider threat categories, assets and divisions which were not originally prioritised. A complete strategy and programme should account for insider threats involving user groups that are malicious, accidental and belonging to a third party.

Mapping insider threat types and categories to business impact

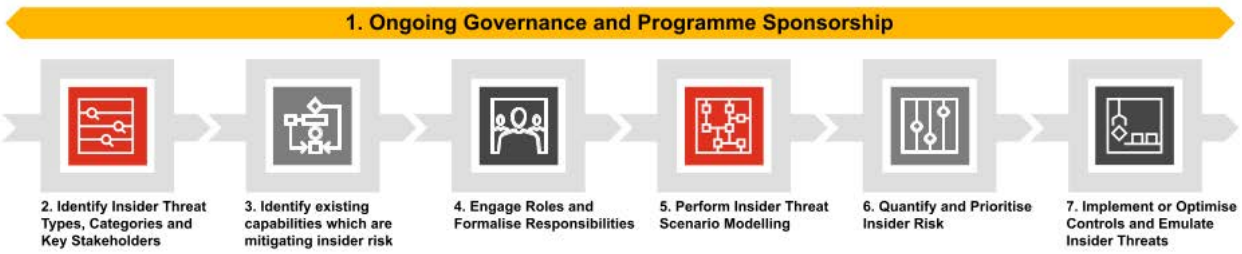
Organisations should understand how the various insider threat types and categories can exploit assets to impact the business. This information can be used to inform the development of tactical and strategic priorities which will be developed further in threat modelling.



The cyber insider risk management programme must be built on a foundation of governance and risk management fundamentals to set guidelines and enable consistent understanding, implementation and use of the programme across the organisation. For more information on building an effective insider risk management programme and the governance fundamentals required see our joint report with Microsoft here.

A successful cyber insider risk programme should be pragmatic and threat-based

The main components of successful cyber insider risk programmes are shown below which help an organisation to build an insider risk strategy, organise their teams and prioritise key mitigating controls identified through threat scenario modelling. Each step of the approach is described below and has been designed to overcome the four main reasons that PwC has observed that cause insider risk programmes to fail.



PwC has observed four main reasons causing cyber insider risk programs to fail

- Limited engagement outside of Cyber Security and IT
- Insider risk programmes are too broad leading to delivery fatigue
- Roles and responsibilities are not defined in advance of achieving stakeholder buy-in
- Insider risk programmes are impacted by an employee council / union

1. Ongoing governance and programme sponsorship

What happens at this stage: Establish the fundamentals for governance to enable a strong foundation and consistent understanding, implementation and use of the programme, and identify a programme owner with executive sponsorship who can influence other function stakeholders to contribute to mitigating insider risk.

Example outputs: Identified a programme owner, formalised their responsibilities and established key governance fundamentals such as; documented programme charter, insider risk policies, processes, playbooks and procedures.

2. Identify insider threat types, categories, and key stakeholders

What happens at this stage: Identify the insider threat types and categories which can be driven by cyber security activities, and align this understanding to the types of critical assets and services that can be exploited resulting in various types of business impact.

Example outputs: High level mapping of priority insider threat types and categories mapped to business impacts, which will be used to prioritise the strategy and first iteration of the programme. Identified stakeholders that are required to input to the insider risk programme.

3. Identify existing capabilities which are mitigating insider risk

What happens at this stage: Identify the capabilities used across the organisation that are mitigating insider risk. Organisations should understand that there is an overlap between control activities which are already mitigating external threats and control activities which mitigate internal threats. See an example control framework below which provides examples of capabilities derived from good practice guidelines from the UK Centre for the Protection of National Infrastructure, Carnegie Mellon, and our industry insights.

Example outputs: Identified capabilities and owners for controls that are implemented and mitigating insider risk, and identified where gaps exist against good-practice. PwC's control framework and reference architecture can be used to support the gap analysis.

Governance and Leadership
Inform business leaders to make informed decisions on insider risk capabilities.

Identity and access management
Grant access only to trusted digital identities reducing the likelihood of related insider risks whilst maintaining a seamless and frictionless user experience.

Threat detection and response
Timely ability to detect, respond and contain insider scenarios.

Human resources, people change and culture
Appropriate and proportionate processes that identify insider indicators for response.

Data security and protection
Protect critical data, reducing related insider risks whilst maintaining a seamless and frictionless user experience.

Risk and compliance
Insider related risks operating in appetite and compliance of relevant legal and regulatory requirements.

Physical security
Appropriate physical layers of defense reducing the likelihood of associated insider scenarios.

4. Engage roles and formalise responsibilities

What happens at this stage: Understand how various types of stakeholders across the organisation contribute to the cyber insider risk programme and control activities, and agree roles and responsibilities as part of a programme. See below for further details on who to involve and why.

Example outputs: Documented RACI for control activities which shows the stakeholders involved and what they are expected to contribute.

Example of roles and responsibilities for managing insider risk

Considerations for working with employee representation councils / unions:

PwC UK acknowledges that every union and council is unique for each organisation and where we have seen insider risk programmes delayed or impacted at these forums it is typically for people-based analytical controls which require monitoring of digital identities and sending personally identifiable information outside of the regulated country, rather than the overall programme being impacted. This leaves a broad set of insider risk mitigation control activities which can be applied in highly regulated countries such as identity and access management (e.g. just in time access, just enough access and context-based access), building security into change management processes and data classification and prevention. Security teams should work closely with internal legal, compliance and data protection teams to anticipate where engagements with employee councils and unions are required, which is likely to occur when employees are impacted by solutions. By engaging with councils and unions early, organisations can ensure their requirements, including objectives and principles, are clearly agreed and built into the consideration of solutions. The monitoring approaches which had a higher potential of success included combining:

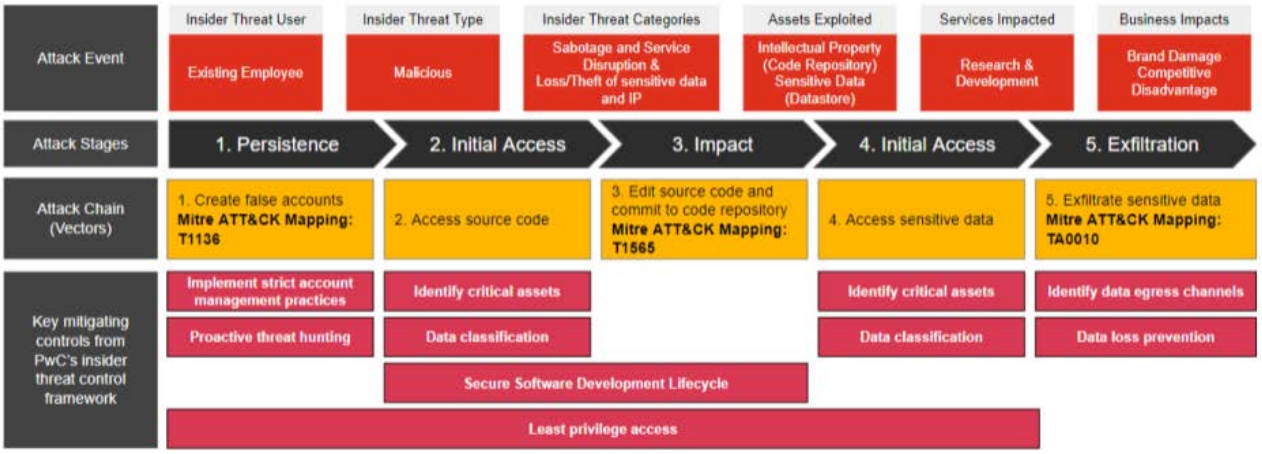
- User baseline monitoring for all users globally rather than a restricted group deemed higher risk, which removed bias.
- Implementing a pseudonymisation approach to hide user identities and provide the union / council with one part of the decryption key. This means the union / council must see evidence of a potential insider threat based on indicators and behaviour analytics before the user's identity can be revealed. This reduces the potential for data misuse.
- Working with your Legal and Compliance teams and your Data Protection Officer to create solutions based on their requirements before engaging your employee councils / unions to collect further requirements.

5. Perform insider threat scenario modelling

What happens at this stage: Use a threat-based approach to model cyber insider threats and identify the key mitigating controls that will address the priority insider threat types and categories identified at stage 2 (Identify insider threat types, categories and key stakeholders). See below for an example approach and note that key mitigating controls can also be identified from Mitre Engage and Mitre D3FEND to support identification of the right capabilities.

Example outputs: Documented threat scenario models mapped to Mitre ATT&CK for the priority insider threat types and categories picked earlier. Identified controls and control gaps required to mitigate the attack vectors for each threat scenario.

Readers should note that insider threats will already have initial access to an organisation and therefore modelling insider threat attacks may not require reconnaissance or initial access as the first stage. Also cyber attacks may repeat attack stages and not follow a unidirectional chain. For example there may be multiple techniques within initial access and other attack stages used throughout the attack.



Research performed by Mitre Engenuity suggests that techniques relating to data collection and exfiltration occur most frequently for insider threat incidents[4]. From our analysis of real world insider threat attacks the key capabilities which organisations should prioritise in their insider risk strategy are mentioned below. The importance of a capability in our analysis is based on its frequency of appearance and the attack stage it mitigates, which assumes that mitigating an attack at earlier attack stages will provide greater returns on investment. However consideration should also be given to maturity, effort and resources required to make changes which will vary by organisation:

1. Identity and access management.
2. Threat detection and response.
3. Security in the change management process.
4. Data security and protection.

Organisations should keep in mind that the priority control capabilities may vary depending on the insider threat categories considered most important in their cyber insider risk strategy. For example:

- Controls within Data Security and Protection are likely to be a higher priority if the organisation considers ‘Loss / theft of sensitive data and IP’ to be their most critical insider threat category.
- Security in the change management process is likely to be a higher priority if the organisation considers ‘Sabotage and Service Disruption’ to be their most critical insider threat category.
- Controls within Human Resources, People Change and Culture are likely to be higher priority if the organisation prioritises mitigating insider threat incidents from accidental and negligent insiders.

6. Quantify and prioritise insider risk

What happens at this stage: Leverage cyber risk reporting mechanisms to articulate and quantify your position of insider risk based on each threat scenario modelled in the previous stage, and use this information to prioritise the key mitigating controls to focus on which are delivering risk reduction for insider risk and other risk categories.

Example outputs: Quantified inherent and residual risk scores for each priority insider threat type and category based on the assets and services modelled so far. Investment strategy based on controls which will provide the largest return on investment for insider risk – if other risk types have been quantified then this can provide an investment strategy based on controls providing the largest return on investment across all measured risk types.

Read more here to find out how PwC can help organisations to improve their cyber risk reporting capability with integrated risk frameworks and learn about our proven Cyber Risk Reporting Platform.

7. Implement or optimise controls and emulate insider threats

What happens at this stage: Implement or optimise control activity gaps by leveraging assets and security services from internal Cyber services and technology service providers. Perform insider threat emulation exercises using a red or purple teaming approach to demonstrate the effectiveness of controls working together and identify how they can be improved.

Example outputs: Identified where control gaps can be covered by implementing new controls and existing controls are optimised based on the results of threat scenario modelling and insider threat emulation exercises.

Organisations should work with their technology service providers to investigate collaborative ways to identify and mitigate existing insider threats

Insider threats include current or former members of staff of an organisation and its third parties, with authorised access to, or knowledge of, an organisation's assets, facilities, information, or people. In the context of third parties this can include business partners, suppliers, technology service providers (which includes services hosted by the third party and products licensed to the organisation), and other providers of developers, consultants and contractors. Supply chains are an integral part of how businesses operate, and by providing third parties with direct access to critical assets, organisations are increasing the number of employees who can pose an insider threat in environments which they may have less control and monitoring over.

Organisations should identify the third parties that have the potential to present a major threat based on the access they have to critical assets, which may occur due to malicious or negligent insider threats. These third parties should be added to the inventory of critical third parties (CTPs). Organisations should be aware that The Bank of England (the Bank), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) (collectively the 'supervisory authorities') have set out potential measures to oversee and strengthen the resilience of services provided by critical third parties to the UK financial sector. This could allow the supervisory authorities to use their proposed powers to include:

- A framework for identifying potential CTPs, which would inform the supervisory authorities' recommendations for formal designation by HM Treasury.
- Minimum resilience standards, which would apply to the services that designated CTPs provide to firms and Financial Market Infrastructures (FMIs).
- A framework for testing the resilience of material services that CTPs provide to firms and FMIs using a range of tools, including but not limited to scenario testing, participation in sector-wide exercises, cyber resilience testing, and skilled persons reviews of CTPs.

Organisations should identify their providers of technology and security tools and work with them to investigate how their tools can be leveraged to identify and mitigate existing insider threats. Examples of key workshops to start with include:

- Identify and secure digital identities – Work with technology service providers to identify the applications being used by the organisation (including unsanctioned / shadow IT), increase visibility into who has access to what (including non-human users such as service accounts) and develop an action plan to ensure digital identities are operating with least-privilege.
- Discovery of sensitive data and data protection – Work with technology service providers to perform a data discovery exercise looking for sensitive information and intellectual property, stale data, and privacy or regulatory risks in Email, data stores and collaboration services.
- Threat detection and response – Work with technology service providers to understand how threats are being detected based on suspicious user activity tied to digital identities. Work with internal incident response, third party retainer and Legal teams to understand if the right information is being collected to understand what users are doing to support post-detection investigation.

How can PwC and Microsoft help you?

PwC UK brings broad expertise and capabilities to support organisations with understanding and mitigating their cyber insider risks. With access to PwC's extensive global network, cross-industry experts and our Gold Partnership with Microsoft, organisations should be confident they are able to call on the required skills and experience to support their challenges. By combining the breadth of PwC's network of capabilities across global geographies with Microsoft's security services, organisations can mitigate Insider risk across all of the control domains identified in our control library. Examples of where we support clients around insider risk include:

- Design a data security strategy based on various data risks and egress channels, implement Microsoft security solutions to reduce the identified data risks and detect attempted data breaches from malicious insider threats, and design intellectual property protection rights with our Data Protection and Legal advisory teams.
- Implement Defender for Identity, perform access reviews, derive a set of higher risk users, and define a strategy to remediate user access to least-privilege principles. This will help to prioritise a user base for SOC detection rules, and reduce the number of users with the means and opportunities to execute insider attacks.
- Implement Defender for O365 to filter out inbound identifiable malicious and phishing emails, which will reduce the likelihood of users being able to accidentally or negligently open up security issues by interacting with such emails. Working with PwC UK they can implement proactive threat hunting to identify targeted and more advanced malicious and phishing emails which may bypass security technologies.
- Implement Defender for Endpoint and apply our Cyber Culture and Human Resources Transformation services to produce behavioural indicators of intent. Information obtained from these sources can be fused in the SIEM to detect insider threat techniques and user groups who are likely to become malicious insiders (turncoats).
- Work with our Forensics Advisory team to proactively ensure they have the required data retained to support investigations when they are required. Organisations can also subscribe to PwC's Incident response retainer services to ensure they have the response and investigation support available on-demand, and leverage PwC's incident readiness advisory services which will include designing and testing insider threat investigation playbooks.

PwC has partnered with Microsoft to run their 'Mitigate Compliance and Privacy Risks' workshop for organisations who want to identify their insider and privacy risks using Microsoft's dedicated Insider Risk Management and Compliance Management services. Through this workshop we work with organisations to:

- Document your objectives and strategy around insider and privacy risks.
- Show you how to detect, investigate and take action on insider and privacy risks using Microsoft security solutions.
- Demonstrate ways to accelerate your compliance journey with the latest Microsoft security solutions and PwC services.
- Provide actionable next steps based on your needs and objectives.

Contact Us

Our experienced team has worked with organisations to develop a pragmatic and threat-based approach to understand the cyber insider threats most relevant to their environment, and identify the tactical and strategic mitigating controls which will maximise return on investment, demonstrate value and minimise friction. Contact us to learn more about how we can help you to understand your vulnerability to insider threats, develop a strategy and build cyber security capabilities to deliver sustainable risk reduction.

Matt Burns, Director
+44 (0) 7711 562536
matt.burns@pwc.com

Jay Vinda, Manager
+44 (0) 7718 978408
jay.vinda@pwc.com

References

[1] https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/
[2] https://www.proofpoint.com/uk/resources/threat-reports/cost-of-insider-threats#:~:text=Independently%20conducted%20by%20Ponemon%20Institute&text=Malicious%2C%20negligent%2C%20and%20compromised%20users,a%20third%20to%20%2415.38%20million
[3] https://www.microsoft.com/en-us/security/business/risk-management/microsoft-purview-insider-risk-management#coreui-contentrichblock-zfh3o49
[4] https://medium.com/mitre-engenuity/launching-a-community-driven-insider-threat-knowledge-base-20a249acb2f