2024

INSIDER RISK

Investigations Report

Foreign Interference:
Special Edition

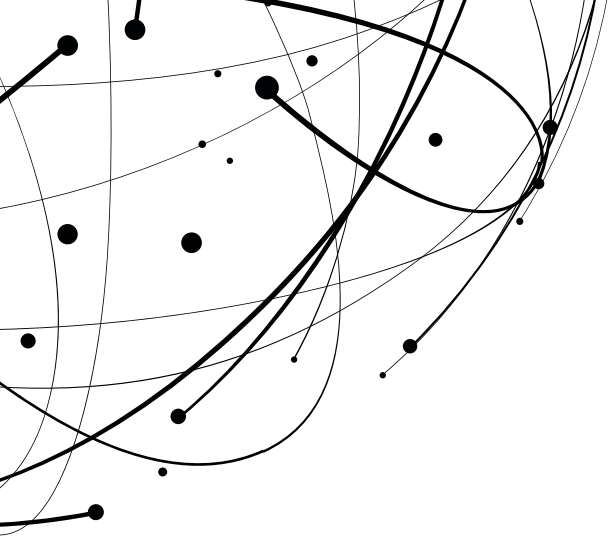


Table of contents

DTEX i³ mission

The mission of the DTEX Insider Intelligence and Investigations (i³) team is to uplift enterprise security by proactively detecting and mitigating insider risks.

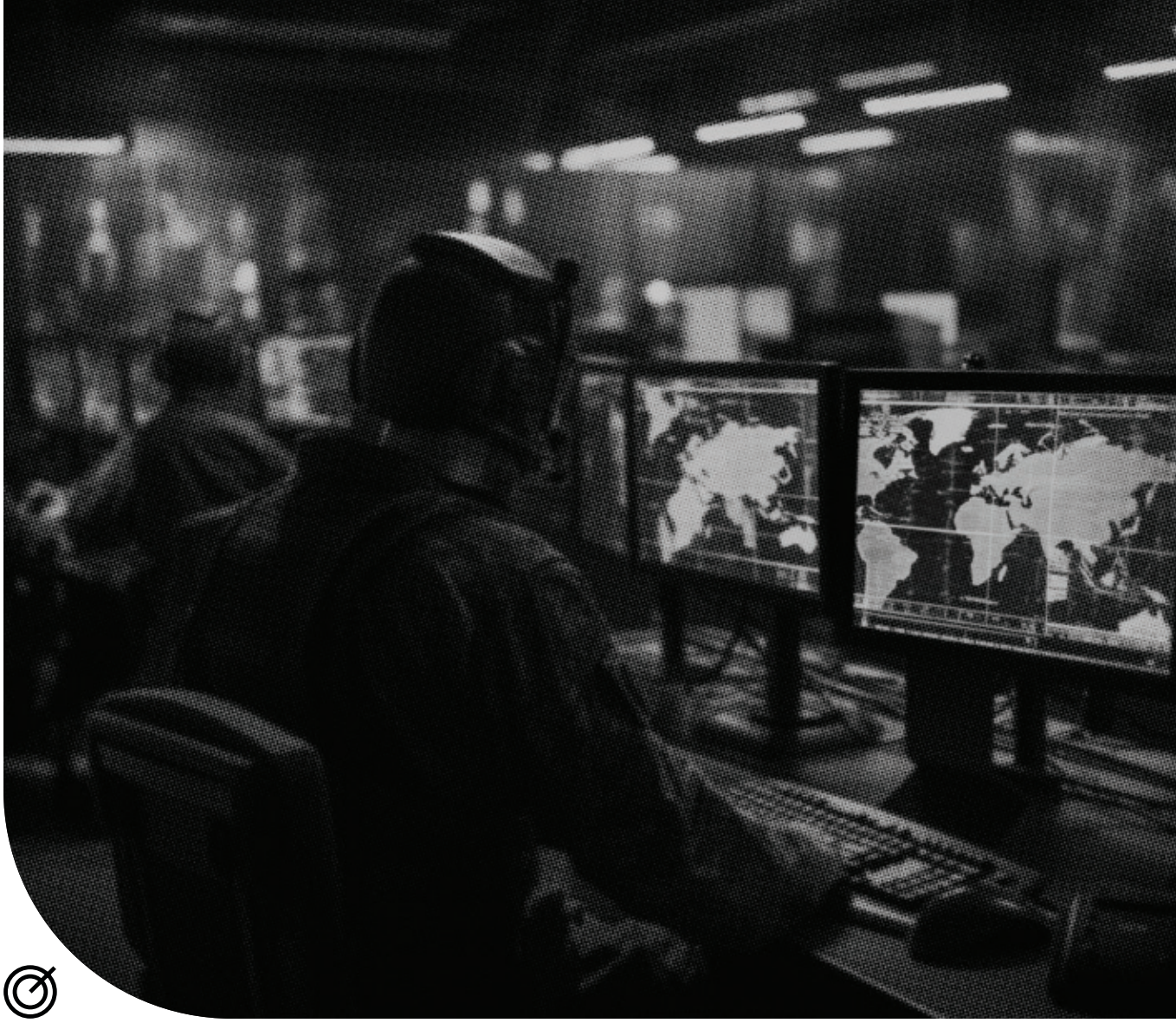
Combining over 20 years of insider risk experience with early warning insider risk indicators, the DTEX i³ team empowers organizations to stay resilient and maintain control of their public narrative and global success.

Importantly, the i³ team often discovers wider security threats that extend beyond insider risks. Such external threats are typically the outcome of an insider incident, not the intention of the insider.

In both cases, the priority is detection and deterrence, and to empower organizations to do away with reactive incident response.

DTEX i³ issues regular Threat Advisories, research, and insider risk insights. These are available online on the **DTEX i³ Insider Risk Research Hub.**

DTEX Insider Intelligence and Investigations (i³) brings together experienced behavioral researchers, consultants, and an elite team of insider threat investigators to create an intelligence-driven, investigation-ready capability.



INTRODUCTION

This report is not just a platform for understanding the insider risk landscape. It is an invitation to uplift collaboration and best-practice information sharing with trusted allies to fortify the protective security resilience of our most mission-critical agencies and entities.

Ongoing geopolitical tension against a backdrop of technological disruption has changed the security landscape as we know it, blurring the lines between cyber, physical, and psychological threats. State actors are doubling down, leveraging whole-of-government campaigns to infiltrate the critical infrastructure upon which civilians rely.

In 2024, fighting ransomware is not the number one conversation to be having. In fact, the entire notion of cyber-only now ceases to exist. Protecting trusted insiders (and the assets and systems they are entrusted with) against foreign influence is the 'how to' conversation to be having and solution to be driving for.

Now more than ever, organizations must adopt a multi-pronged approach backed by cross-cutting collaboration that extends beyond business lines to other industries and regions. Having a robust insider risk program is critical. In fact, it's non-negotiable – but it's not enough.

"Cyber threats to our critical infrastructure represent real world threats to our physical safety. It's time to keep ahead of the threat by investing in capabilities, bolstering collaboration, and building on the gains made to enable us to take action."

Christopher Wray, Director
Federal Bureau of Investigation

Industrial espionage and IP theft is at an all-time high

The following statistics are based on DTEX i³ investigations for IP theft or system sabotage throughout 2023, where user actions were found to be intentional.

70% INCREASE in customers approaching DTEX for support specific to protecting against foreign interference since 2022. The biggest uptick has been across critical infrastructure and the public sector.

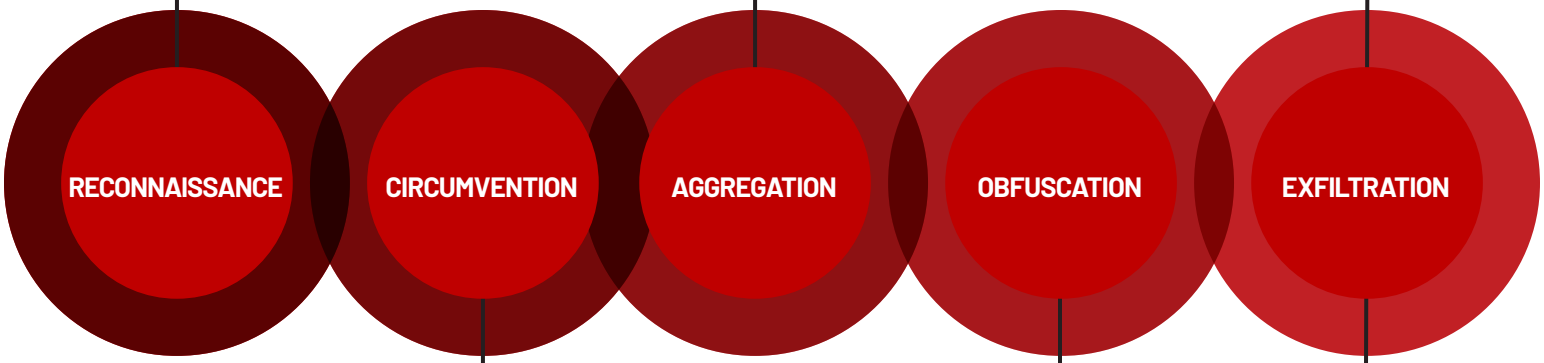
32% of malicious insider investigations included anomalous reconnaissance behavior.

- **13%** included unusual and repeated research into people and authors of 'crown jewel' topics.
- **9%** performed external and internal research on security controls.
- **5%** exercised internal security controls (e.g., sent innocuous data via an unapproved medium).

64% of malicious IP theft investigations included some form of data preparation, aggregation and/or conversion.

- **37%** of all unusual aggregation steps included the conversion of data to some form of image or PDF (e.g., screenshots).
- **22%** had some form of data compression in addition to encryption.

While the majority of incidents included data egress of some form, the techniques varied based on the controls in place.

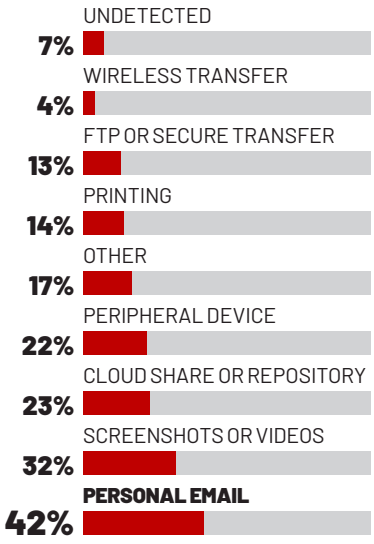


12% of super malicious insider investigations involved the active bypass of security controls.

This finding was less than expected, given 88% did not bypass anything.

77% of sophisticated malicious insiders attempted to conceal their activity to evade detection.

- **35%** attempted to conceal the source of their internet connection, including private browsers, VPN, mobile hotspots, etc.
- **95%** of super malicious insiders were able to avoid using ATT&CK techniques in a deliberate attempt to fly under the radar.
- **25%** increase in the usage of burner email and encrypted messaging accounts since 2022.



By the numbers

→ 15%

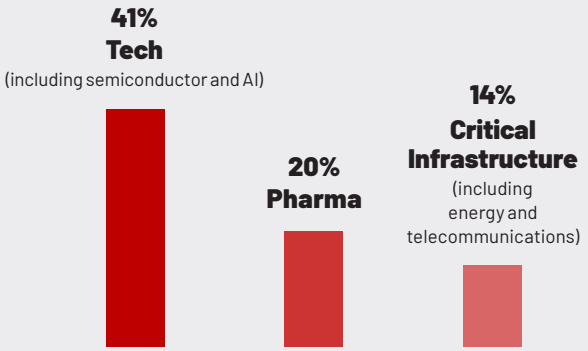
of employees take sensitive IP when they leave an organization.

76%

of departing employees take non-sensitive proprietary data.

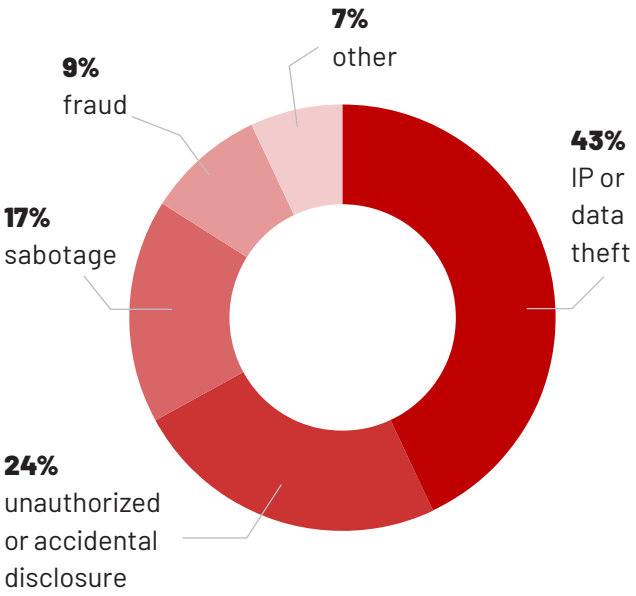
Non-sensitive data, in the wrong hands, can have as detrimental an impact as sensitive IP, especially if weaponized by malicious insiders or external attackers. The DTEX i³ team has observed the crossover between corporate data on personal devices – a notable trend of the past two years – with organizations across industries having lenient acceptable use policies. This blurring of boundaries introduces visibility gaps and operational inefficiencies (primarily due to ongoing validation) that, together, can dramatically increase the risk of unauthorized disclosure.

Industry sectors with the most IP theft incidents:



Notably, the sectors with the most IP theft incidents were highly regulated and had a lot to lose (from innovative product data, sensitive research to project information within mission-critical entities).

Breakdown of insider investigations:



→ 62%

increase in the use of unsanctioned applications – up from 55% in 2022.

Over the past year, the DTEX i³ team has found several high-risk vulnerabilities in over a dozen popular web application categories across its global customer base. Employee rewards programs and workplace monitoring applications were particularly concerning use cases where misconfiguration opened the door to unauthorized access.

There was also an increase in the use of browsers and browser extensions. Although organizations may try to lock down the use of physical applications, employees are increasingly leveraging browsers and portal applications to circumvent security controls.

New tech, new workarounds

92% of organizations identified internal use of AI tools as a key security concern.

41% have one or more employees using AI to support their job.

90% want support with employee monitoring to mitigate AI-associated risks.

→ 21%

of communication tools (such as Zoom, Slack, Cisco Webex etc.) involved the unauthorized transfer of data.

This includes transfer of documents, images, and clipboard activity, and highlights a broader trend of employees finding new ways to store their notes as they adapt to new tools and technologies.

While the ease of integration through communication and file-sharing tools affords a welcome convenience, it also creates the risk of 'data bleed', where corporate assets are visible on personal devices and vice versa. There is a significant need among organizations to ensure acceptable use policies that delineate between personal and corporate to negate any blind spots and protect corporate (and personal) assets.

→ Human-first triumphs cyber-only.

72%

of DTEX i³ investigation requests were initiated by HR.

This once again highlights the power of human sensors in the early detection and mitigation of insider risks. Having a mechanism for reporting unusual or suspicious behavior, no matter how small, is a big piece of driving a security-driven, employee-empowered culture.

68%

of insider risk events were proactively resolved with follow-up security awareness training and corporate policy changes.

This is a significant win that speaks to the power of taking a proportionate response to insider risk management. There is no one-size-fits-all approach to insider risks, and it is unreasonable to course correct a non-malicious insider the same way one would a malicious insider. Educating negligent or compromised insiders, and enforcing clear-cut security policies, provides a dramatic improvement in corporate risk posture.

Executive summary

The DTEX i³ team is pleased to present the 2024 Insider Risk Investigations Report. This year's report offers key insights into the state of play based on more than 1,300 investigations within DTEX's global customer base.

Kellie Roessler
Insider Risk Advocate and Author
i³ Content Lead
DTEX Systems

Throughout 2023, organizations across industries were still dealing with the hangover effects of employee attrition, organizational restructuring, and remote work environments – all trends reminiscent of 2022 and 2021. For many, the focus was filling the gaps around access control, monitoring and other corporate policies relating to governance, risk, and compliance.

In the headlines, we saw increasing aggression from foreign state actors – including Volt Typhoon – put more strain on security and risk teams. Meanwhile, the uptake of artificial intelligence (AI) and generative AI tools such as ChatGPT introduced a new layer of complexity, as employers sought to balance profitability with security.

The rise of AI was undeniably felt by everyone, including our own frontline investigators who saw firsthand the good, the bad, and the indifferent. Our product development team was quick to adopt the strengths of Large Language Models (LLMs), developing our own AI risk assistant (Ai³) to democratize behavioral data analysis and expedite insider investigations.

At the same time, our investigators saw how AI tools were creating new risks to organizations, having observed several instances of employees uploading sensitive data to GenAI tools.

With the technological landscape constantly changing, the concern around AI isn't going away anytime soon.

Our research found 92% of organizations identified internal use of AI tools as a key security concern. Adding to this concern is the growing threat of foreign interference and espionage, and the stealth at which foreign state actors are operating. Indeed, there has never been more opportunity for adversaries to outsmart insiders and undermine the truth in pursuit of knowledge and power.

Judging by the headlines and our own insider investigations, there is no doubt espionage, and IP theft, has reached a new all-time high. Another growing concern is that of super malicious insiders, who are increasingly flexing their tech know-how to access and obtain sensitive data without sounding alarms. Our investigations found 12% of super malicious insiders actively avoid circumventing security controls. Why? Because they want to appear as 'normal' or unsuspecting as possible so as not to set off a security alert.

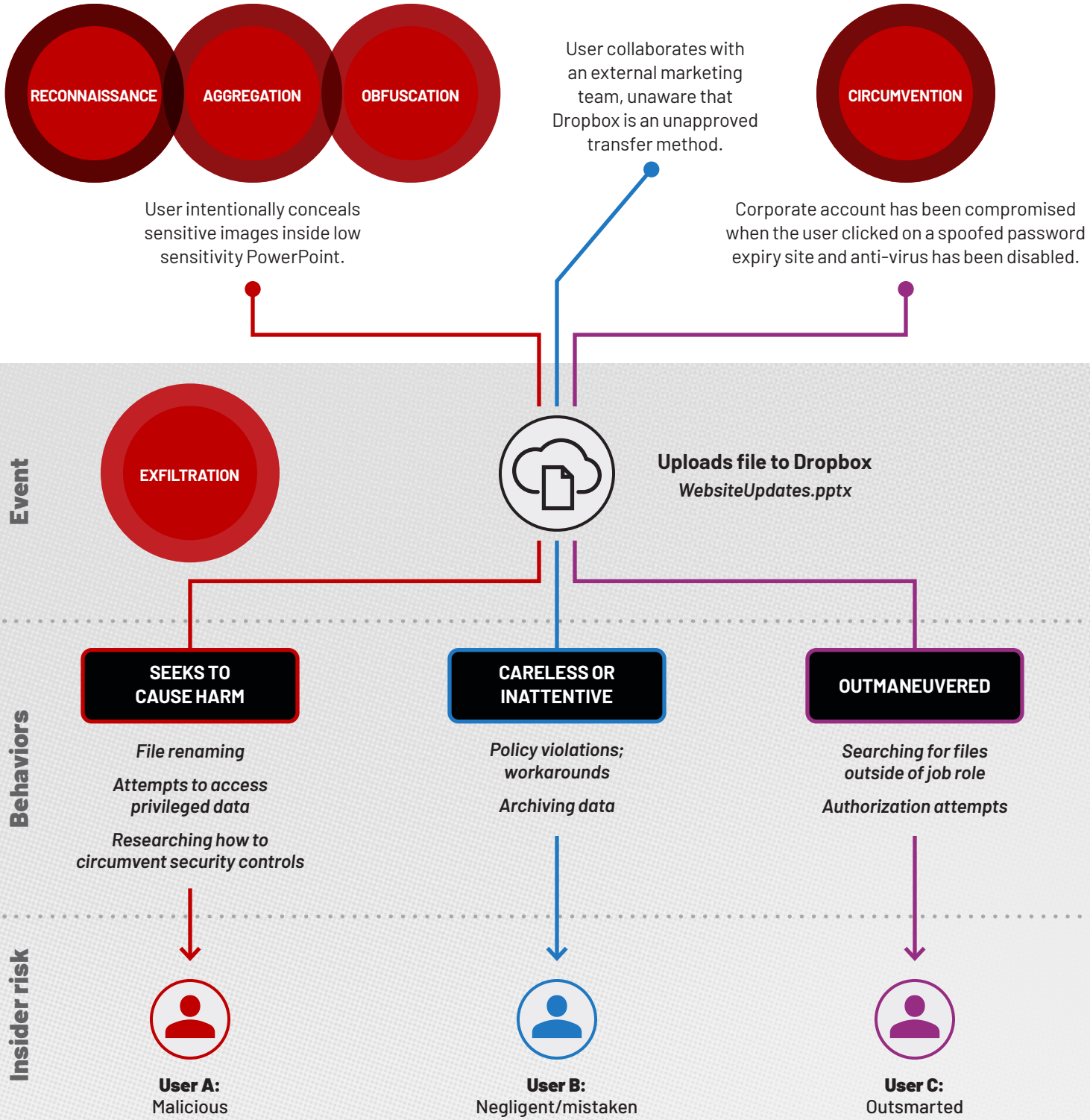
The threat landscape has never been more precarious. But despite this, there is cause for optimism and hope. The work being undertaken by several public and private entities shines light on what can be, and what is being, done to get ahead and stay resilient. The trick now lies in collaboration and a sharing of the minds under one trusted alliance. This will set the scene for security, prosperity, and success - now and for decades to come.

More findings, investigative insights, and practical content awaits inside.

In 2023, we saw a massive uptick in customers wanting our support in protecting against foreign interference (a 70% increase since 2022).

Not all risks are created equal

The behaviors leading up to a data exfiltration event are more important in differentiating the types of insider risks than the event itself.



The rise of the socially engineered insider

The past year has seen a sharp rise in the stealth and frequency of foreign interference, as state actors weaponize technology to socially engineer trusted insiders.

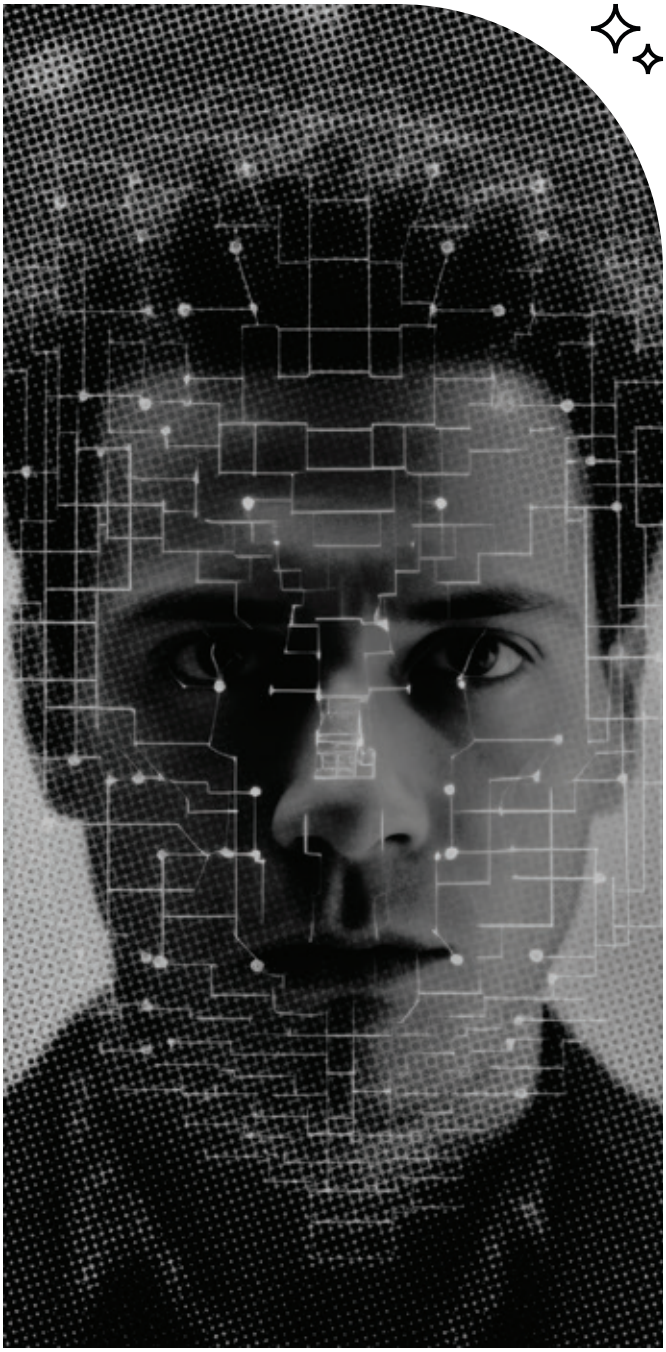
The hardest hit sectors are those with access to intelligence that can be used for economic, military, or technological advantage. Increasingly, threat actors are pursuing everything from critical research and innovation IP to classified nuclear intelligence and information on how critical infrastructure operates.

Many are exploiting social platforms – from professional networking sites, email, messaging and even dating applications – to hide behind a fake persona and lure insiders into an information exchange. This pervasive tactic often manifests with a spy posing as a credible figurehead on LinkedIn and offering an insider a 'consulting' opportunity in exchange for handsome payments. The gig might involve preparing a report that includes sensitive information relating to foreign policy, military intel, or academic projects. Recruitment of disgruntled employees via the Dark Web is another popular tactic, though this generally applies to malicious insiders (not outsmarted).

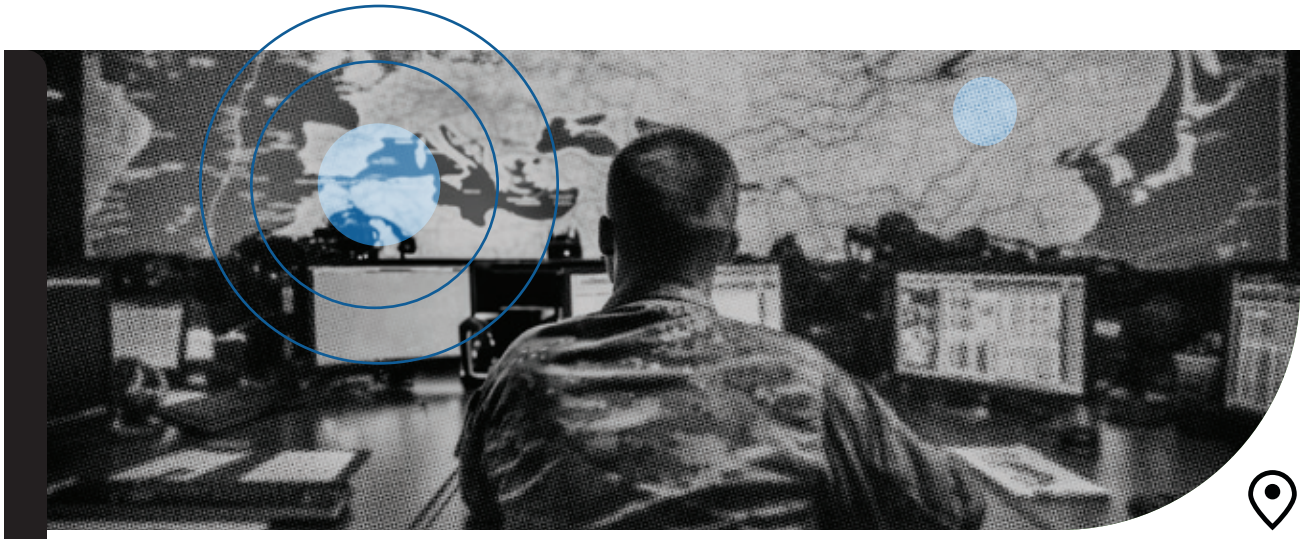
The rise of AI has made these outreach efforts an attractive tactic for threat actors, who can now target and outsmart trusted insiders at enormous

scale with minimal cost and effort. AI tools based on LLMs enable threat actors to craft clean, personable emails that appear indistinguishable from what the genuine sender would typically write. But this is just the tip of the iceberg of what are ultimately elaborate whole-of-nation campaigns.

The use of deep fakes also represents a significant threat to national security – and enterprises are just as vulnerable as governments. The ability of technology to undermine the truth is something no organization can afford to ignore. Staying on top of emerging social engineering tactics, and educating the workforce, is critical in stopping trusted insiders from falling victim to espionage attempts.



Organizations can help prevent successful espionage through employee education programs on social engineering motivations and tactics. Importantly, education shouldn't be seen as a checkbox exercise, but rather an ongoing effort to instill a security-conscious culture. Providing skills-based training to help employees recognize when they may be a target of foreign recruitment, and providing mechanisms for reporting concerns safely and with anonymity is key to protecting and uplifting a trusted workforce.



Countering foreign interference

Protecting sensitive information and national security resilience go hand in hand. Countering the threat of foreign interference to both malicious and non-malicious insiders requires a multi-pronged approach inspired by best practices from both public and private sectors. Fortunately, there are many strong examples of what 'good' looks like coming from both sides.

Continuous Vetting for a trusted and secure workforce

Implementation of Trusted Workforce 2.0 – the U.S. Federal Government's biggest reform of the personal vetting system – is currently in flight. One of the centrepieces of the initiative is the transition from periodic background checks to a Continuous Vetting (CV) model to enable detection of concerning behavior in near real time.

This includes significant life changes that might increase a cleared person's propensity to become an insider risk (whether malicious or otherwise).

Corporate entities outside the public sector have a powerful opportunity to follow in the footsteps of the U.S. government by adopting CV to mobilize

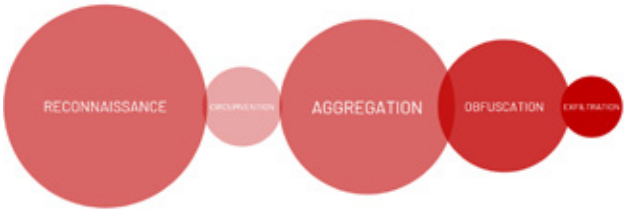
and maintain trust within their own workforces. Importantly, a continuous approach should not be seen through the lens of power and suspicion, but rather transparency and support. Depending on the scenario, this might manifest as financial counselling, psychological help, or even legal support – it all depends on the context. This supportive approach is critical for sustaining the **bidirectional loyalty** upon which trust and security thrive.

→ Continuous Vetting in practice

- A continuous approach to vetting in the enterprise should cut across people, technology, and processes, and be founded on a culture conducive to bidirectional loyalty. When employees feel loyal to their employer, they will be motivated to act in the organization's best interests.
- Employees should also know when and how to air concerns around suspicious behavior coming from their peers under a formalized reporting program that ensures anonymity. Importantly, they should feel safe and motivated to do so in the first place.
- Technology should capture meaningful data for analysts to understand an individual's risk profile at any given time. System interoperability (including with HR reporting feeds) is a key consideration for capturing the data that is needed to surface true positives.

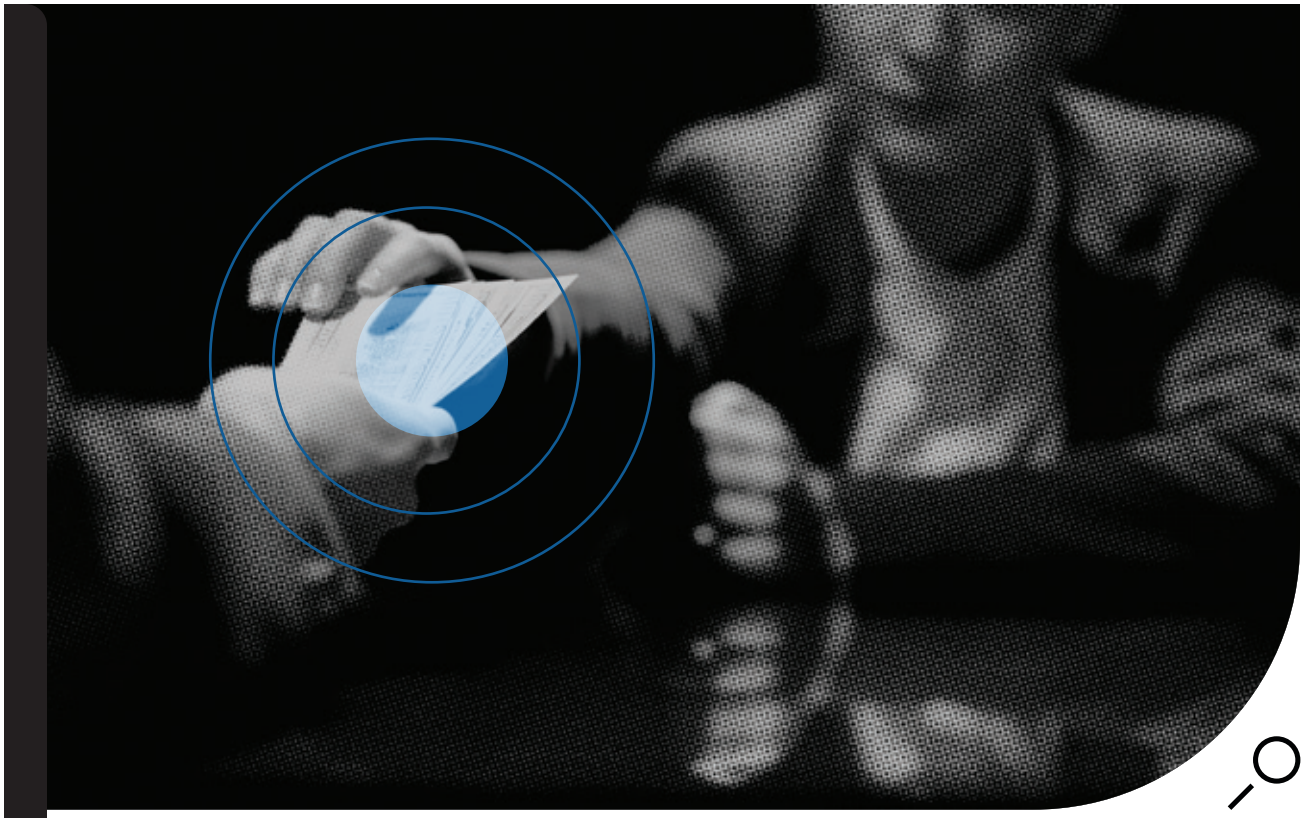
The power of the Insider Threat Kill Chain

The key stages of the Insider Threat Kill Chain – particularly reconnaissance, aggregation, and obfuscation – are all important for surfacing early warning risk indicators, especially when dealing with malicious incidents that have a foreign nexus. Our investigative findings demonstrate that preventing malicious data breaches requires contextual insights into the psychology of human behavior. This is especially essential for being able to find the needle in the haystack.



Security of Critical Infrastructure (SOCI) Act

Australia's Security of Critical Infrastructure (SOCI) Act is a strong example of how non-government agencies are evolving to combat the risk of foreign interference. The SOCI Act mandates critical infrastructure operators to establish and comply with a Critical Infrastructure Risk Management Program. The program "aims to ensure responsible entities take a holistic and proactive approach to identifying, preventing, and mitigating risks." The risks span cyber and information, personnel, physical, natural, and supply chain. As more Australian organizations comply with the mandate, there are likely to be several lessons learned, thus presenting a strong opportunity to share new insights and best practices with trusted cross-national public and private entities.



Espionage

The state of the threat landscape is such that espionage, system sabotage, and insider fraud all represent serious risks not just to vulnerable entities, but to national security.

Detecting espionage is a complex undertaking, especially when the avenues of entry are legitimized. The reality is those involved in such clandestine tradecraft know too well that to maintain ongoing access to knowledge, they need appear as normal and unsuspecting as possible.

The Thousand Talents Program is one example of foreign interference that has caught the attention of government and intelligence agencies in the U.S. and other Five Eyes nations for unethically legalizing theft of IP and other sensitive data. According to the FBI, China oversees hundreds of talent plans. All incentivize its members to steal foreign technologies needed to advance China's national, military, and economic goals.

There have been several investigations of this occurring beyond the past year, all designed to financially reward program recipients for stealing foreign technology secrets.

While the DTEX i³ team cannot comment on any specific investigations pertaining to talent plans, the team is highly cognizant of the growing threat of espionage and government recruitment due to the significant increase in investigation requests from customers. The team is actively working with customers and Five Eyes allies to bolster collaboration and best-practice information sharing to uplift cross-national security resilience.

Insider risk programs focused on foreign interference must be careful not to introduce analyst bias

While the threat of espionage is very real, it is of extreme importance to note that not all those participating in a talent plan set out to cause harm. Often, well-meaning individuals might be working under the influence of a foreign state without even knowing. Organizations have a responsibility to understand that some individuals may be more susceptible to foreign influence, and that the reasons will vary significantly. Understanding this is critical in managing insider risks fairly under a trusted workforce that is conducive to better security outcomes. Potential risk indicators in the context of the Insider Threat Kill Chain can afford organizations the ability to understand their workforce, including third-party contractors, and to manage potential risks accordingly without introducing bias.

Sectors most at risk

- Technology, scientific R&D and innovation-led companies (e.g., semiconductor and AI companies)
- Universities and academia
- Government, military and defense

Engineer arrested for allegedly stealing secret U.S. government tech

In February 2024, Chenguang Gong – a Chinese native and US citizen – was arrested for allegedly stealing trade secrets developed for use by the U.S. government to detect nuclear missile launches and track ballistic and hypersonic missiles.

According to court documents, Gong transferred more than 3,600 files from a Los Angeles-area research and development company to personal storage devices while he worked for the company in 2023.

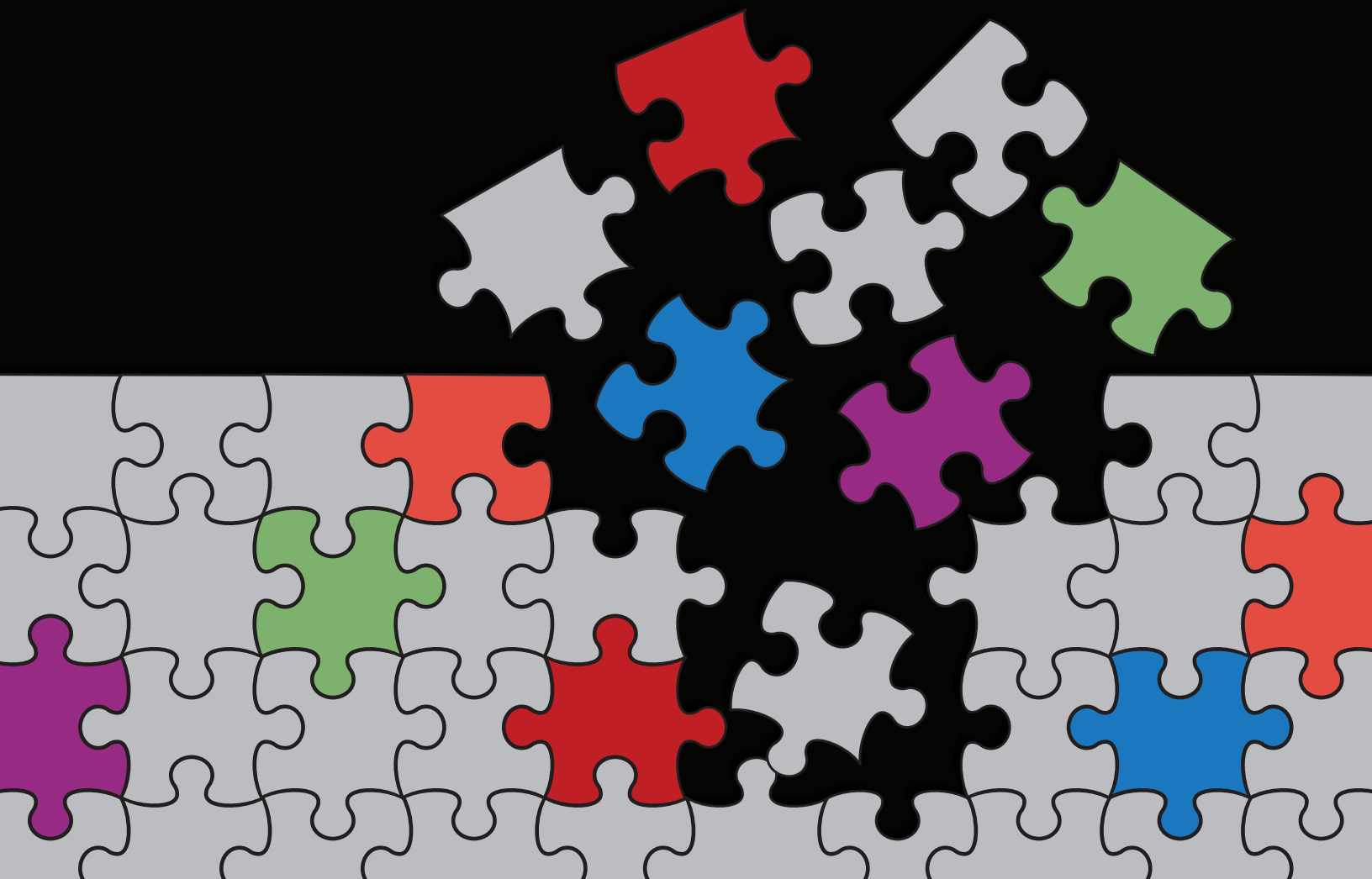
As it was investigating Gong, the Justice Department said, the FBI found he applied a number of times to "Talent Programs" run by China from 2014 to 2022, all while employed by major U.S. tech companies.

In one email translated from Mandarin, prosecutors say Gong remarked that he "took a risk" in 2019 by traveling to China because he "worked for… an American military industry company" but he took the chance because he "thought he could do something" to contribute to China's "high-end military integrated circuits."

A behavioral risk model for the early detection of insider risks

Incidents of espionage, and other insider-related events (whether malicious or not), can be mitigated through early insider risk detection. Having high-fidelity data that cuts across cyber, physical, organizational, and psycho- social sensors enables analysts to better gauge insider risks and to course correct in a way that is proportionate.

The following Behavioral Risk Model highlights how key data points, when correlated, can form potential risk indicators that can be used to build context to better understand insider risks. For clarity, signals are single data points. Observations are a collection of signals that meet a pre-defined criteria associated with insider risk. Observations can also be a single behavioral signal, if the signal meets the pre-defined criteria (for instance, if an employee reports another employee for suspicious behavior).



Behavioral Risk Model

Signals

Incoming data is processed to create observations

Access type
Email activity
Facility access logs
File downloads
File renaming
Geographical location
Internet traffic
Phone records
System access logs
Time of day
Travel records
Web access

Observations

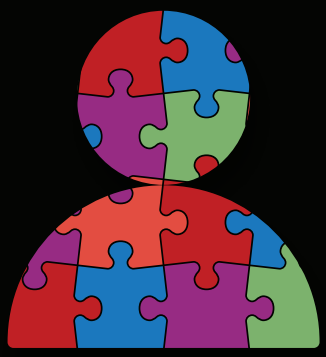
Observations processed to create indicators

Authorization attempts
File combinations
File size
Frequency of access
Frequency of communication
HR/performance information
Install scripts
Usage patterns
Websites

Indicators

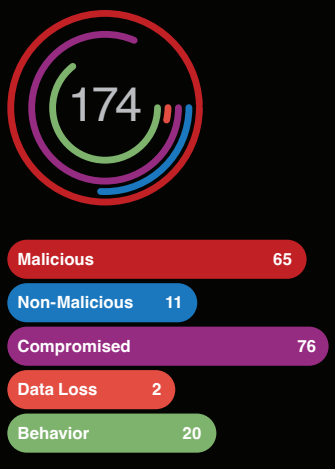
Indicators assessed to evaluate insider risks

Attempts to access privileged data
Access attempts outside of the pattern
Disgruntled employee
Harvesting data
Policy violations
Suspicious communications



Behavioral risks

Early detection of behaviors that match insider risk types



Artificial intelligence risk vs. reward

Accidental or intentional data loss

Non-malicious insiders are regularly using LLMs for productivity gains, but this poses a significant risk of accidental data leakage. Making matters worse, malicious insiders can use LLMs to exfiltrate sensitive data with a high degree of plausible deniability.

Deep fakes and AI-powered fraud

A significant danger of GenAI is the ability to create deepfakes – a type of manipulated image or video that makes it appear like someone said or did something they actually didn't. Malicious insiders or external threat actors can use deepfakes to manipulate other inside employees into revealing information and gaining access to critical systems or conducting fraud.

Nation states and social engineering

State actors are increasingly using LLMs to augment their cyberoperations. Well-meaning insiders are vulnerable to social engineering as part of the information-gathering stages that form part of larger-scale campaigns.

RISK

The adoption of AI boasts several benefits in productivity gains, but the risks of AI-based tools must be understood and managed accordingly.

→ Act now to mitigate AI risk

- Leverage advanced monitoring tools to verify the data that is being uploaded to AI tools.
- Discourage employees from uploading proprietary code into AI tools by educating them on the risks to the employee and the organization.
- Create and implement acceptable use policies for AI tools that limit its use for testing and mock scenarios.
- Review policies regularly to ensure they are fit for purpose in light of new AI feature changes or updates.

Democratizing behavioral data analysis

Using AI risk assistants, analysts can bypass complex data wrangling to gain actionable insights on demand, saving potentially hours of work. AI risk assistants can also act as a guide, prompting the right questions at the right time to surface the insights that matter most in complex investigations.

Data quality comes first

The rewards of AI cannot be realised unless the data from which AI draws is of high quality. Only by having the right high-fidelity signals and observations can analysts gain context to detect insider risks against false positives and insider threats that might otherwise slip through the cracks.

REWARD

From a risk analyst perspective, the rewards of AI cannot be understated, accelerating investigations while filling technical gaps.

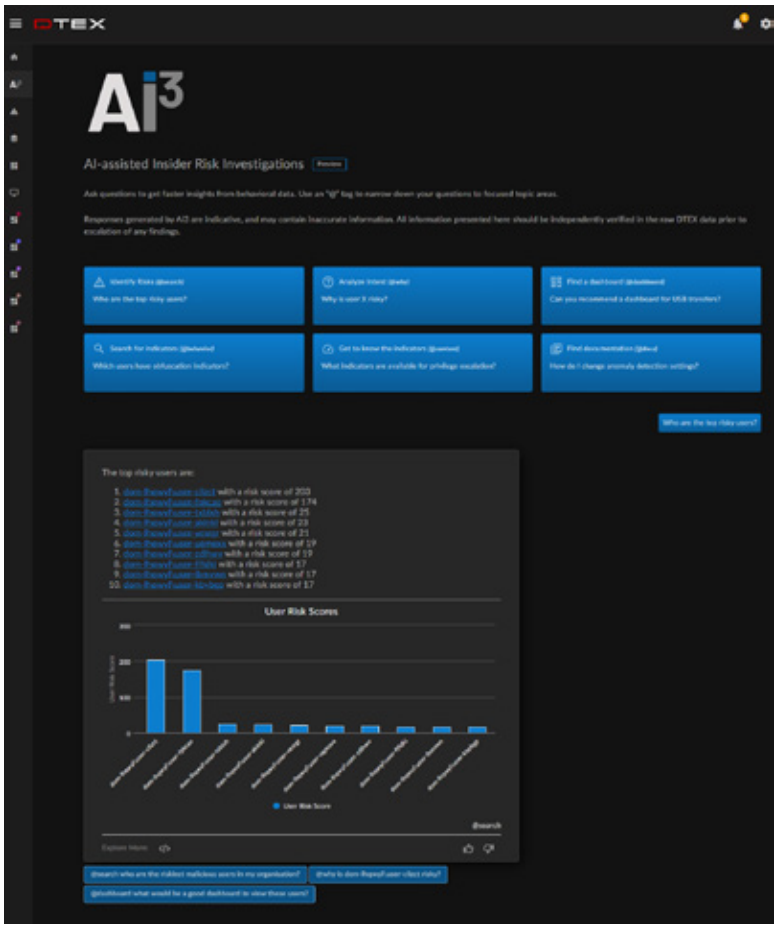


Figure 1. The DTEX Ai³ Risk Assistant processes natural language to provide quick and comprehensive insight into the complicated nature of insider risk and intent. Ai³ guides analysts to critical insights in real-time, bypassing complex data wrangling that takes away from the mission at hand.

IP and data theft

Nearly half (43%) of all DTEX i³ insider investigations in 2023 involved IP or data theft. Departing employees were at higher risk of taking data with them (15% of 'leavers' took sensitive IP, sometimes to a competitor, while 76% took non-sensitive proprietary data).

Of all sectors, tech (41%), pharma (20%) and critical infrastructure (14%) experienced the most IP theft incidents.

In almost all data theft incidents, the insider accessed personal webmail accounts on corporate devices to exfiltrate data. The use of unsanctioned applications, including browsers, was also commonly used to circumvent corporate controls.

SPOTLIGHT INVESTIGATION

In one i³ investigation, an employee triggered security alerts by accessing private emails and transferring files from a non-work-related business folder. Further investigation revealed they held a senior position at another company, identifiable through a domain name in their emails. This dual employment was confirmed by their LinkedIn profile picture, which matched the one on the secondary company's website. Despite being hired as a commercial leasing executive, they were simultaneously selling distressed businesses at the other company, leveraging confidential information from our client to pinpoint sales opportunities.

Risks and impact

- Conflict of interest: When an employee's personal interests interfere with their professional obligations, it can damage both the employer's business and the employee's reputation.
- Breach of confidentiality agreement or Non-Disclosure Agreement (NDA): Using information from one job to profit in another could be a direct violation of these agreements.
- Ethical issues: Using information from one job for personal gain in another job can be seen as dishonest and unprofessional.

Early warning insider risk indicators

- User accessing multiple webmail accounts separate from the corporate domain.
- High-volume email activity related to the secondary business with whom the user was employed.
- Business website the user was accessing contained the user's photo and similar name.
- Online social media accounts for this individual under an altered identity.
- File activity conducted for another entity on a corporate endpoint while employed and during business hours.

Read the **Threat Advisory on Detecting the Use of Multiple Identities** via the DTEX i³ Insider Risk Research Hub.

Organizations, especially those that handle high-value data, should establish and communicate acceptable use policies that set clear boundaries between personal versus business use. Monitoring for the use of personal webmail and providing targeted security awareness training to highlight the security risk is a quick win in helping to prevent data exfiltration altogether. In addition, risk practitioners should collaborate closely with HR to know about upcoming terminations or anticipated flight risks to proactively plan ahead to avoid visibility blind spots. Most importantly, organizations should foster a culture of bidirectional loyalty, where policies are communicated, and employees feel safe and valued because they feel part of the security mission. A holistic approach that encompasses continuous education, program improvement, and monitoring can significantly help in fostering a strong security culture and protecting the data most important to the organization.

Do

Unauthorized or accidental disclosure

Throughout 2023, the DTEX i³ team found several high-risk vulnerabilities pertaining to misconfiguration in over a dozen popular web application categories. The risks associated with such investigations are a prime example of how internal and external threats are becoming increasingly blurred.

Among the most concerning use cases involved applications for employee rewards programs, CCTV, and drones. Several applications belonged to companies that are blacklisted by the U.S. government due to national security concerns.

SPOTLIGHT INVESTIGATION

During a DTEX i³ investigation, three Software as a Service (SaaS) applications were identified as posing significant risks to the client. One application provided livestreaming footage of the entire worksite, offering unchecked visual access at any point and time. The second application – an online system for ordering uniforms – enabled unauthorized access, potentially allowing acquisition of company-branded attire without any verification. The third application exposed detailed shift reports for security contractors, revealing security personnel rotation schedules, incident reports, and patrol patterns.

By exploiting these application vulnerabilities, a motivated threat actor (whether internal or not) could exploit key information sources to bypass physical security controls and gain physical entry into the worksite.

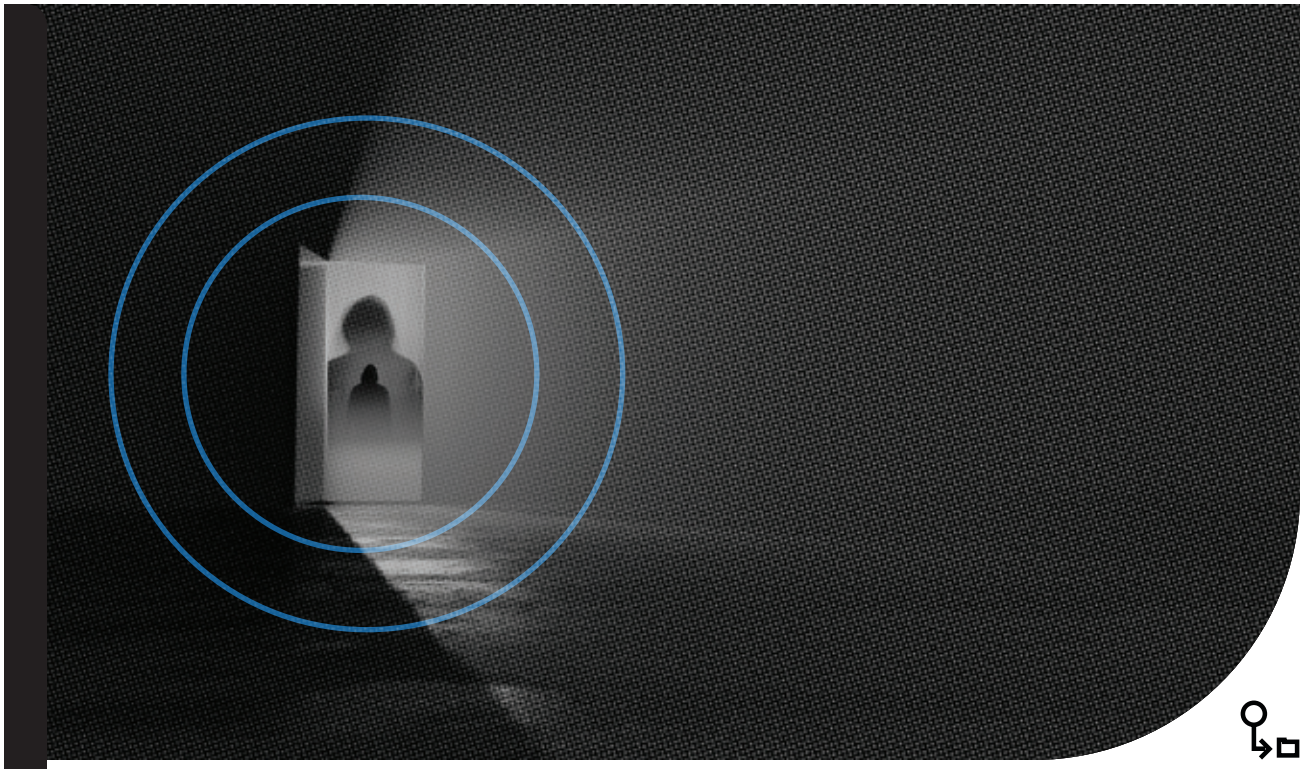
Risks and impact

- Unauthorized access: The ability to view livestream footage offers potential intruders a way to surveil the site in real time.
- Impersonation: Access to the uniform ordering system allows for the easy acquisition of company attire, enabling threat actors to impersonate staff or contractors.
- Exploitation of security gaps: With detailed knowledge of security guard shifts and patrol patterns from the shift reports, intruders can plan their movements around the site's security operations, targeting times when the site is most vulnerable.

Early warning insider risk indicators

- Session tokens did not expire, thus allowing access from anyone with the link.
- Livestream footage contained "shared" in the URL string.

Addressing security vulnerabilities in third-party web applications requires a comprehensive approach that encompasses regular security assessments and ongoing monitoring. By understanding and proactively mitigating misconfigured APIs, IDOR vulnerabilities, and authentication weaknesses, organizations can significantly enhance the resilience of their web applications against potential threats – both internal and external.



System sabotage

Throughout 2023, the DTEX i³ team investigated several incidents whereby critical vulnerabilities in clients' IT environments could literally open the door to system sabotage.

Misconfigurations in web portals, publicly accessible links, and lack of sufficient role-based access controls can create a perfect recipe for a malicious insider or outside threat actor to gain unrestricted access and control of sensitive data and control systems. Super malicious actors with comprehensive IT knowledge are constantly looking for new ways to break in and enter, and when there's no barrier to entry, the opportunities for exploitation are limitless.

In the majority of investigations, the i³ team was able to prevent system sabotage from occurring by detecting and deterring the risk of entry before anyone else could. The findings from our investigations should serve as a timely call to action to prioritize sound security hygiene and security awareness training before exploitation occurs.

SPOTLIGHT INVESTIGATION

In a case of system sabotage waiting to happen, a global critical infrastructure client was found to have an open Virtual Network Connection (VNC). If known and exploited by a malicious threat actor, the exposed VNC would provide a clear entry point to hijack the client's entire IT environment and operational output.

The open VNC provided unrestricted unauthenticated access to a computer responsible for controlling vital machinery. Through this access point, a motivated threat actor would be able to obtain highly sensitive mission-critical information, including satellite coordinates, machinery movement data, and project files integral to the client's operations.

In a worst-case scenario, a threat actor could seize control of the client's machinery and other crucial systems to inflict shutdowns and endanger human lives.

The **Florida water plant hack** is an example of an investigation that was not prevented.

Risks and impact

- Operational disruption: Malicious actors can alter process controls, leading to shutdowns, inefficiencies, or dangerous operational states.
- Safety hazards: Unauthorized changes to Human Machine Interface (HMI) settings can compromise safety mechanisms, potentially leading to hazardous conditions that endanger human life and environmental safety.
- Data breach: Access to an HMI often means access to sensitive operational data, including proprietary technology details, operational procedures, and potentially personal data.

Early warning insider risk indicator

- URL string contained session token information that appeared to be an allow listed IP address. The session token did not expire, thus allowing access from anyone with the link.

Without adequate access control policies, Virtual Network Connections (VNCs) and other remote access tools pose a significant risk to organizations, particularly those operating within critical infrastructure sectors. All it takes is one malicious threat actor to run a search on exposed VNCs to identify vulnerable organizations and wreak havoc. Organizations can proactively mitigate this risk by implementing robust access policies and firewalls, conducting ongoing security awareness training, automating patch management, and continuously monitoring systems, networks, and user behaviors.

An invitation to collaborate

As a fundamentally human challenge, insider risk management is complex. No one person, program or entity can shield against the endless possibilities for exploitation of their workforce. The way forward lies in collaboration and best-practice information sharing of potential risk indicators and other data-driven findings and research.

This report is an opportunity to learn about the incredible communities across the Five Eyes that are driving powerful initiatives to spark collaboration, partnership, knowledge transfer, and skills development. It is an invitation to get involved in the pursuit of national security resilience.

US INSIDER RISK MANAGEMENT CENTER OF EXCELLENCE

The US Insider Risk Management (US-InRM) Center of Excellence (COE) is dedicated to promoting private, public, and academic partnerships to foster knowledge sharing and resources to mitigate insider risk to U.S. and international corporations. Their vision is to raise the proverbial tide to lift all insider risk/threat practitioners by providing best practices and guidance, training, research and thought leadership, information sharing, and events.

Strategic partners:

- Applied Research Laboratory for Intelligence and Security
- Australian Insider Risk Centre of Excellence
- Canadian Insider Risk Management Centre of Excellence
- Carnegie Mellon University, Software Engineering Institute
- DTEX Systems
- National Cybersecurity Alliance
- National Counterintelligence and Security Center
- MITRE Corporation

→ **Get involved:**
usinsiderriskmanagementcoe.org

The Canadian Insider Risk Management Centre of Excellence (C-InRM CoE) is a not-for-profit entity that is evolving Canada's capabilities in insider risk management by fostering an interdisciplinary approach aimed at accelerating research, training, education, and building sustained community partnerships. The C-InRM CoE fosters an interdisciplinary approach to insider risk management towards the promotion of industry best practices and innovation within an evolving threat environment.

Strategic partners:

- The Norman Paterson School of International Affairs, Carleton University
- Canadian Cyber Threat Exchange
- Accenture
- CGI
- DTEX Systems
- VigilantCS
- Government of Canada
- Australian Insider Risk Centre of Excellence
- MITRE Corporation
- Defense Personnel and Security Research Center (PERSEREC)

→ **Get involved: canadianinsiderriskmanagementcoe.com**

The Australian Insider Risk Centre of Excellence (AIR CoE), established by the Australian Collaboration Centre, is dedicated to strengthening Australia's cyber resilience through collaborative insider risk management. AIR CoE is committed to developing a community of practice and experts in insider risk; adopting an industry-led approach to deliver programs and events; developing best-class capability-building activities (including masterclasses and workforce training); driving research and development; and addressing the evolving risk management requirements across defense, critical infrastructure, and the SMB space.

Founding partners:

- MITRE Corporation
- DTEX Systems
- McGrathNicol

→ **Get involved: cybercollaboration.org.au/aircoe**

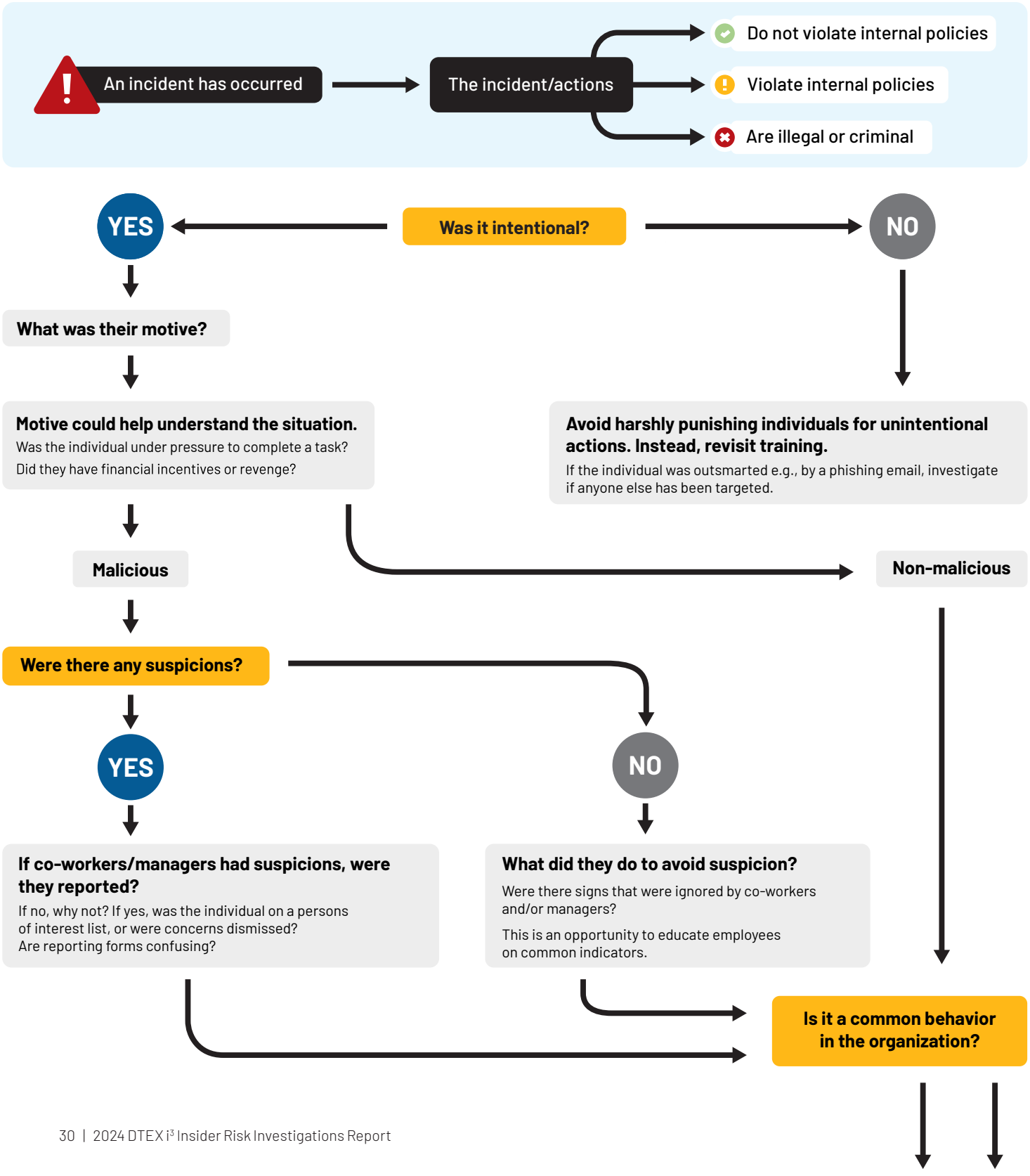
Five Eyes Insider Risk Practitioner Alliance (FIRPA)

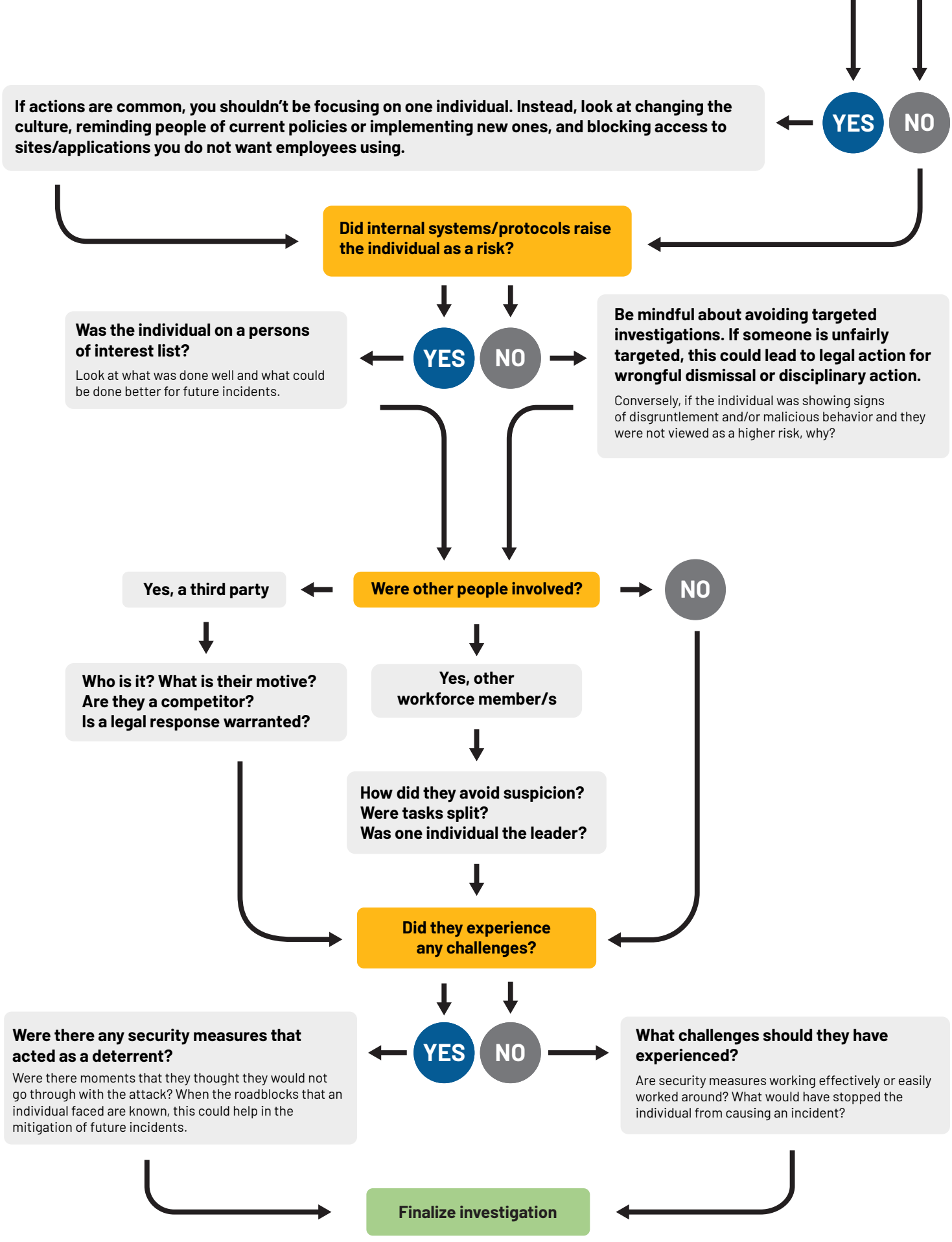
The FIRPA vision is to grow, support, and prepare a global community of skilled insider risk practitioners to accelerate capability maturity across defense and critical infrastructure in the Five Eyes. FIRPA has been developed by the Canadian Insider Risk Centre of Excellence and the Australian Insider Risk Centre of Excellence to unite communities of skilled practitioners committed to this mission, with founding members such as MITRE Corporation. FIRPA will provide ongoing opportunities for practitioners to share best practices for building and running effective insider risk programs. Importantly, FIRPA will be a trusted forum for sharing early warning indicators of malicious insider behavior.

→ **Get involved: firpa.org**

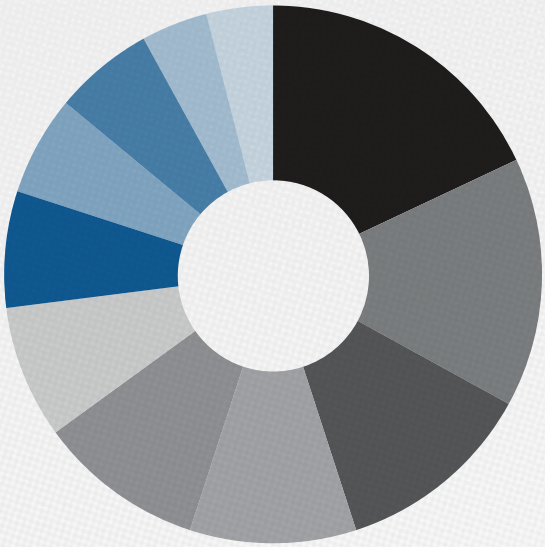
Insider risk resolution decision tree

The following framework can be used by analysts and security teams to help resolve insider risks in a way that is proportionate and fair.



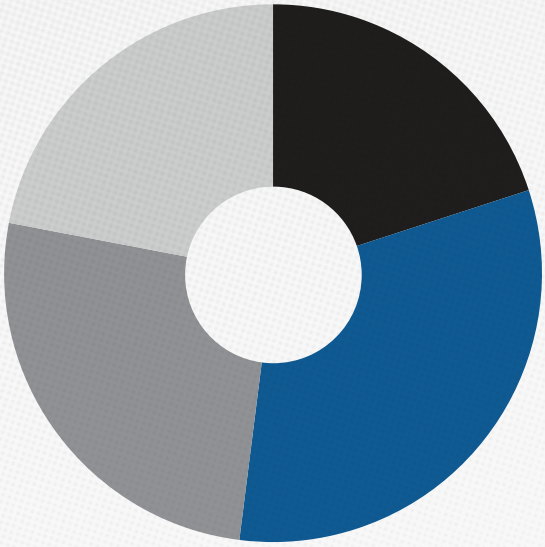

If actions are common, you shouldn't be focusing on one individual. Instead, look at changing the culture, reminding people of current policies or implementing new ones, and blocking access to sites/applications you do not want employees using.
YES
NO
Did internal systems/protocols raise the individual as a risk?
Was the individual on a persons of interest list?
Look at what was done well and what could be done better for future incidents.
YES
NO
Be mindful about avoiding targeted investigations. If someone is unfairly targeted, this could lead to legal action for wrongful dismissal or disciplinary action.
Conversely, if the individual was showing signs of disgruntlement and/or malicious behavior and they were not viewed as a higher risk, why?
Yes, a third party
Were other people involved?
NO
Who is it? What is their motive?
Are they a competitor?
Is a legal response warranted?
Yes, other workforce member/s
How did they avoid suspicion?
Were tasks split?
Was one individual the leader?
Did they experience any challenges?
Were there any security measures that acted as a deterrent?
Were there moments that they thought they would not go through with the attack? When the roadblocks that an individual faced are known, this could help in the mitigation of future incidents.
YES
NO
What challenges should they have experienced?
Are security measures working effectively or easily worked around? What would have stopped the individual from causing an incident?
Finalize investigation

About this report



DISTRIBUTION BY INDUSTRY

Financial Services	18%
Government	15%
Pharma and Life Sciences	12%
Telecommunications	10%
Information Technology	10%
Energy	8%
Manufacturing	7%
Transportation	6%
Healthcare	6%
Media	4%
Retail	4%



DISTRIBUTION BY NUMBER OF EMPLOYEES

0k - 1k	20%
1k - 10k	32%
10k - 50k	26%
50k+	22%

DISTRIBUTION BY HEADQUARTER LOCATION

Americas	56%
APAC	20%
EMEA	24%

The Global Leader for Insider Risk Management

As the global leader for insider risk management, DTEX unifies data science with AI and behavioral psychology to stop insider risks from materializing into data breaches. DTEX InTERCEPT cuts across Data Loss Prevention, User Activity Monitoring and User Behavior Analytics in one lightweight platform to enable mission-critical entities to safeguard their most sensitive assets. Combining rich telemetry across cyber, physical, and psycho-social sensors, DTEX surfaces unique early warning indicators to detect and deter true insider risks at unprecedented scale, with privacy by design.

To learn more about DTEX, please visit dtexsystems.com.