

# Evaluating Red Flags and Insider Threat Mitigation Measures

## Debriefing

**Mathias Reveraert**

**Lisa De Laet**

March 5<sup>th</sup> – March 6<sup>th</sup>, 2024

# Roundtable



What is your key take-away from today's exercise?

# Background of the exercise



- List of potential red flags/ mitigation practices based on Delphi study
  - Multidisciplinary & international panel of experts
  - Three rounds of online questionnaires: Brainstorm – Rating - Refinement
- Goal of today's exercise
  - Do players of the TTX come to same conclusions as Delphi panel?

	<u>Delphi categorization</u>	<u>Expected categorization TTX</u>	
Mitigation practices	High-rated practices	Essential	
	Medium-rated practices	Preferred	
	Low-rated practices	Additional	Not recommended
Potential red flags	High-rated red flags	High	
	Medium-rated red flags	Medium	
	Low-rated red flags	Low	

# Example results\*



\*Example of results from another exercise.

The results of this exercise will later be shared on the Whova app.

Good Practices Observation (ENG)	Group A	Group B	Group C	Group D	Group E
Physical protection and technical measures (decent camera systems, ...)	Essential	Preferred	Essential	Essential	Essential
Declaration by the organization of assets and interests	Essential	Preferred	Preferred	Essential	?
Ensure insider threat awareness on Board, CEO and management levels	Preferred	Essential	Essential	Essential	Essential
Have various means to report red flags	Essential	Preferred	Essential	Essential	Preferred
Use and audit a system to monitor the use of badges/access rights (electronic access control)	Essential	Essential	Additional	Essential	Essential
Prevent an employee from accessing data/facilities he/she does not need for his/her work (role-based access)	Essential	Additional	Essential	Essential	Essential
Internal audit	Preferred	Preferred	Essential	Additional	?
Put responsibility for monitoring behavior with all members of staff, not just the security team (vigilant managers & staff)	Essential	Essential	Essential	Essential	Not Recommended
Do not punish employees that make a wrong call when reporting red flags in good faith	Essential	Essential	Additional	Essential	Preferred
Development of a formal threat assessment	Preferred	Essential	Essential	Preferred	Preferred
External audit	Essential	Additional	Essential	Additional	Essential
Invest in a culture of open feedback and trust	Preferred	Essential	Essential	Essential	Not Recommended
Put in place alarms on access systems	Essential	Preferred	Additional	Preferred	Essential
Data loss prevention (DPL) tools	Preferred	Essential	Additional	Preferred	Essential
Ensure an active role of line manager/supervisor following-up if someone appears unhappy or different from usual	Preferred	Preferred	Additional	Essential	Essential
Secure endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices (endpoint security tools)	Essential	Not Recommended	Additional	Essential	Essential
Create a supportive culture	Preferred	Essential	Additional	Additional	Essential
Let security report directly to the CEO	Additional	Preferred	Preferred	Preferred	Essential
Require management sign-off for potentially disruptive actions	Preferred	Not Recommended	Additional	Additional	Essential
Installation of a point of contact to report red flags	Additional	Essential	Additional	Additional	Additional
Scrutiny of internet use and social media activity	Essential	Not Recommended	Additional	Additional	Preferred
Put in place a hotline to report red flags	Additional	Preferred	Additional	Additional	Additional
Conduct red team tests	Additional	Preferred	Preferred	Additional	Not Recommended
Separation of key roles/duties	Additional	Not Recommended	Additional	Preferred	Preferred
Insist on a regular use of vacation and holiday time off from work	Not Recommended	Not Recommended	Additional	Additional	Essential
Encourage isolated or withdrawn employees to participate in informal gatherings	Preferred	Additional	Not Recommended	Additional	Additional
Periodic and variable workplace climate surveys	Not Recommended	Not Recommended	Preferred	Preferred	Additional
Periodic and variable psychological assessment (fitness for duty screening)	Additional	Not Recommended	Additional	Preferred	Additional
Conduct random tests	Additional	Not Recommended	Preferred	Additional	Additional
Four-eyes principle/two-person rule	Not Recommended	Additional	Additional	Additional	Preferred
Use artificial intelligence/machine learning to find warning signals (UEBA, Anomaly Detection, Sentiment Analysis, Keyword Matching, ...)	Additional	Additional	Additional	Additional	Not Recommended
Reward employees that report red flags	Additional	Not Recommended	Additional	Not Recommended	Not Recommended
Job rotation	Not Recommended	Not Recommended	Not Recommended	Not Recommended	Additional
Formally inform employees that use of time during work hours can be checked by private investigators	Additional	Not Recommended	Not Recommended	Not Recommended	Not Recommended
Promote self-reporting	Not Recommended	Not Recommended	Not Recommended	Additional	Not Recommended
Risk analysis based on access and impact	Preferred	Preferred	Additional	Preferred	Essential
Structure coordination and communication along the organization (avoid information silos)	Preferred	Preferred	Preferred	Essential	Additional
Tailor-made training for managers and staff to detect and report red flags in their context	Additional	Essential	Preferred	Preferred	Preferred
Conduct desktop simulations	Additional	Additional	Preferred	Additional	?
Implement an anonymous whistleblower system (compliant with relevant legislation and not only ticking the box)	Essential	Essential	Additional	Additional	Additional
Stage manipulation by a hostile third party (social engineering)	Additional	Additional	Preferred	Additional	?
Create a culture of reporting where employees know they are actually helping co-workers by disclosing concerns	Preferred	Essential	Additional	Preferred	Not Recommended
Repeat screening when employee moves to a more vulnerable position	Additional	Additional	Additional	Additional	?
Let employees work in teams	Not Recommended	Preferred	Preferred	Preferred	Preferred
Use a formal assessment process supported by regular catch-up sessions	Not Recommended	Additional	Additional	Preferred	Essential

## Conclusion of the exercise

- Some recommendations from the expert panel are endorsed by the players of the TTX
- Other recommendations from the expert panel are contradicted by the players of the TTX
  - Some red flags/ mitigation practices score better than expected
  - Some red flags/ mitigation practices score worse than expected

# My key take-aways of the exercise

- No 'one-size-fits-all' solution to mitigate insider threat
  - Recommendations from Delphi expert panel are indicative rather than conclusive
  - Tailor-made approach needed that is contextualized to your organizational context
- TTX/Delphi study as input for tailor-made mitigation policy
  - Insights on potential red flags you should be vigilant of to increase early identification of possible impending incidents
  - Inventory state-of-the-art insider threat mitigation measures you can implement



# More information?

- PhD Thesis
  - Exploring Insider Threat Awareness and Mitigation: More than the Devil in Disguise
- Contact details
  - [Mathias.reveraert@infrabel.be](mailto:Mathias.reveraert@infrabel.be)
  - [LinkedIn](#)

