

# PDM

---

## Insider Threat Program Development Manual



Co-financed by  
the Internal Security Fund  
of the European Union

Edition 2019, 2



**Publisher:** Catherine Piana, Director General of CoESS

**Disclaimer:**

Our Liability - to the fullest extent possible at law we (and all of our sister, parent, subsidiary and member companies and organisations) exclude all liability for any loss or damage (including direct, indirect, economic or consequential loss or damage) suffered by you as a result of using the contents of this manual.





# Table of Contents

Acknowledgements	7	
Acronyms	8	
Introduction	11	
<b>1</b>	<b>What is an Insider Threat?</b>	<b>13</b>
1.1	The Insider Threat	16
1.2	Increase in Insider Threat Cases	23
1.3	Who is an Insider in Aviation	24
1.4	Abbreviated Insider Threat Case Studies	26
1.5	Insider Threat Ecosystem	34
1.6	Threat Actions	37
1.7	Threat Data	40
1.8	Threat Landscape & Cybersecurity & Emerging Threats	41
<b>2</b>	<b>Mitigating the Insider Threat and Developing an Insider Threat Program (InTP)</b>	<b>46</b>
2.1	Insider Threat Indicators	48
2.2	Unintentional Insiders	51
2.3	Radicalisation - Basics & Indicators	52
2.4	Addressing the Insider Threat	54
2.5	Insider Threat Mitigation	55
2.6	Methodology	59
2.7	Insider Threat Program Functions	60
2.8	Insider Threat Program Building	63
2.8.1	Program Building Key Steps	65
2.8.2	Getting Started	67
2.8.3	Reporting	68
2.8.4	Identification of Stakeholders	68
2.8.5	Communication with Stakeholders	69
2.8.6	Workforce Consent	71
2.8.7	ICT Usage Information	72
2.9	Communications Strategy	73
2.10	Insider Threat	75
2.10.1	Insider Threat Awareness Training	75
2.10.2	Insider Threat program Building Training	78
<b>3</b>	<b>Best Practices</b>	<b>80</b>
3.1	Obstacles	82
3.2	What Others Have Done	84
3.3	Some Legal Considerations	86
3.4	Top 10 Question List to Check (Basic Due Diligence)	87
3.5	Safe Hiring & Pre-Employment Screening/Vetting (Onboarding)	88
3.6	Temporary Workers, Interim Staff, (Sub)-Contractors & Interns	98
3.7	During Employment	99
3.8	Offboarding - Exit Procedures	101
3.9	Risk Assessment	104
3.10	Infinity/Continuous Screening	107
3.11	Managing Trust & Suspicion	108
3.12	Reporting Suspicious Behaviours & Issues	109
3.13	Post Reporting	111
<b>4</b>	<b>Protective Measures</b>	<b>113</b>



# Acknowledgements

The AITRAP project team would like to express its appreciation to the many people who worked on, and contributed to, the project. The project team continued to develop the AITRAP deliverables, the 2 Computer Based Training (CBT) modules, awareness building and program building, providing many iterations and additional material. In 2018, the team developed this handbook and, to do so, solicited input from various industry stakeholders.

This handbook would not have been possible without the assistance of our major contributors which included EU's DG HOME represented by Mrs. Eva-Maria Engdahl, Mr. Radoslaw Olszewski, the US Federal Bureau of Investigations represented by Mr. Dwayne Sharp, CoESS (Confederation of European Security Services) represented by Mrs. Catherine Piana, Securitas Transportation Aviation Security, represented by Mr. Cliff Lodewijckx, Securitas NV, Securitas Transportation Aviation Services represented by Mr Bohdan Paszukow, and DHL Express, represented by Mr. Hans Streumer and Palmyra Aviation Advisors, represented by Mr. Hugo Lücke.

We also would like to thank those partners who supported us with the logistical side of the AITRAP project, the Polish Border Guards, Transportföretagen and Kötter Services GmbH.

This handbook, and the associated CBT eLearning Modules, are based on a wide range of knowledge and information from staff throughout the project.



[twitter.com/Help2Protect](https://twitter.com/Help2Protect)



[linkedin.com/groups/12203116](https://linkedin.com/groups/12203116)

# Acronyms

ACFE	Association of Certified Fraud Examiners (US)
AIRPOL	EU Airport Law Enforcement Network
aka	Also Known As
APP	Application (Computer/Mobile Program)
ASG	Abbu-Sayyaf Group (Terror Organisation)
ATC	Air Traffic Control
BYOD	Bring Your Own Device
CAA	(National) Civil Aviation Authority
CAD	Computer-Aided Design
CBT	Computer Based Training
CCTV	Closed Circuit Television (Video Surveillance)
CD	Compact Disc
CERT	Computer Emergency Readiness Team (USA)
CEO	Chief Executive Officer
CIA	Central Intelligence Agency (USA)
CIPD	Chartered Institute of Personnel and Development (UK)
CoESS	Confederation of European Security Services
CPNI	Centre for the Protection of National Infrastructure (UK)
CV	Curriculum Vitae
CWB	Counter-Productive Work Behaviour
DG HOME	Directorate-General for Migration and Home Affairs (EU Commission)
DHS	Department of Homeland Security (US)
DNA	Molecule that contains the instructions an organism needs to develop, live and reproduce
DPO	Data Protection Officer
DVD	Digital Versatile Disc
EAP	Employee Assistance Program(s)
EMS	Emergency Medical Services
EMT	Emergency Medical Technician
ERP	Emergency Response Plan
EU	European Union
FANC	Federal Agency for Nuclear Control (Belgium)
FBI	Federal Bureau of Investigations (USA)
FBO	Fixed Base Operator (Business Aviation Handling Agent)
FIDS	Flight Information Display System
FIE	Foreign Intelligence Entities
FSB	Russian Intelligence Service
GDPR	General Data Protection Regulations (EU Law)
HR	Human Resources
HRIS	Human Resource Information System
HRM	Human Resources Management

HRMS	Human Resources Management System
HVAC	Heating Ventilation Air-Conditioning
ICT	Information & Communications Technology
ID	Identity
IED	Improvised Explosive Device
InTP	Insider Threat Program
IP	Intellectual Property
IS	Islamic State (Terror Organisation) aka ISIL, ISIS, DAESH
ICT	Information Technology
MEP	Member of the EU Parliament
MP3	Audio coding format for digital audio
NCCIC	National Cybersecurity and Communications Integration Center (USA)
NSA	National Security Agency (USA)
OCAD	Organisation for the Coordination and Threat Analysis (Belgium)
OCR	Optical Character Recognition
PC	Personal Computer
PED	Personal Electronic Device
PII	Pre-Incident Indicator(s)
R&D	Research & Development
RPS	Risques Psychosociaux
SAAIA	Somali Air Accident Investigation Authority
SME	Small & Medium Sized Enterprises
TSA	Transportation Security Administration (USA)
USB	Universal Serial Bus
VPN	Virtual Private Network
WIFI	Technology for radio wireless local area networking of devices
ZIP	Data compression and archival file format



# Introduction

This project has been developed as a result of the European Commission's DG HOME action plan which implements EU policy initiatives, in particular the 2014 Commission Communication on Strengthening Preparedness against CBRN-E Threats.

Therefore, as part of the DG HOME policy work program and assistance to Member States security authorities and operators, on 24-25 March 2015 DG HOME organised an EU Workshop on Insider Threats to Critical Infrastructures. Tragically, during the opening hour of the conference on 24 March 2015, an Insider (GermanWings suicidal pilot) took another 149 lives on this fatal flight.

The following workshops during 2015 and 2016 sponsored by DG HOME allowed the industry and authorities to stake out the key priorities and shaped the needs for immediate near-term actions. International cooperation in this important area has been visible from the beginning, as DG HOME invited the US authorities (FBI, DHS) to participate in this work and exchange lessons learned on the other side of the Atlantic. The support of DG HOME as well as the US authorities (FBI Insider Threat Division) resulted in an excellent dialogue with the industry and contributed to important input into this project and its output. The input of the FBI has been very valuable and whilst the EU has a distinctly different legal landscape and hosts many national rulemaking entities, the US lessons can nonetheless offer value in

developing different tools. The EU actions steered by DG-HOME led to a public call on how to support development of Insider Threat tools, which resulted in the AITRAP project.

The terrorist attacks in Paris 2015 and Brussels 2016, continued to highlight the threat by Insiders and the EU Action Plan on Protection of Public Space and Critical Infrastructures of October 2017 led by DG HOME further emphasized the importance of addressing the issue of Insiders at both national and EU level, since we operate in a borderless environment.

This handbook aims to provide direction to all aviation & transportation and critical infrastructure stakeholders wishing to implement basic building blocks of an Insider Threat program (InTP). It should be used alongside the CBT program on building an InTP. This handbook contains different sections, which provides useful material and references to build programs from scratch. The sections in this handbook are arranged based on the logical flows of program design and activity.

This handbook also attempts to answer common questions posed by those building the InTP program. The material and InTP guidance contained within this handbook are the result of the workshops and discussions held by the AITRAP team and the experience of the many experts who were involved in its creation.



# 01.

---

## What is an Insider Threat?

## Definition of an Insider Threat

An Insider Threat<sup>1</sup> is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organisation's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organisation's information or information systems. Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware they are aiding a threat actor (i.e. the unintentional Insider Threat).

**Insider Threats:  
"It's not about the 98%  
you catch, it's about the  
2% you miss"**

## Definition of an Insider

A current or former employee, contractor, business partner or anyone who has or had authorized access to the organisation's network, systems, or data. Insider Threats present a unique challenge to transportation and critical infrastructure<sup>2</sup> security. Since Insiders touch everything in the organisation, everything is part of the Insider Threat landscape.

<sup>1</sup> US-CERT: Definition of Insider Threat.

<sup>2</sup> Critical Infrastructure normally covers following industries: telecommunications, energy, finance, government/public services, water, health, emergency/law enforcement services, transport and food. This may differ from country to country.

EU definition of critical infrastructure: critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

- They have the ability to regularly observe security (procedures) to determine systemic vulnerabilities.
- They are generally considered "trusted persons" and their actions often do not receive the same level of scrutiny as other external individuals.
- They are often granted access credentials or security knowledge, as part of their duties, which equip them to bypass security measures.
- The Insider may look and act just like everyone else – "finding a needle in a stack of needles".
- Employees know the organisation's security measures and how to work around them.
- Insider Threat can be overwhelming to consider – companies should not become paralyzed by the problem; there are solutions.

It is important to note that even the smallest issue could cover or hide a more serious one. Innocent behaviour can hide radical motives, and everyone should, over time and with training, develop a natural awareness and understanding of discrete changes while also developing an eye for detail which might provide clues to potential Insider Threats.

Every single employee within every transportation and critical infrastructure company should at least have been given the opportunity to follow the EU Insider Threat awareness CBT, which was created by the EU-funded AITRAP working group. It will eliminate questions like “why should I care, or, what’s in it for me?”.

This is about the protection of self, colleagues, the company, its assets and customers. It is about preventing them from being harmed by detecting insiders before they could strike.

It is this motivation that spurred the EU to provide the means necessary to create awareness and program building aids like this.



YOUR EMPLOYER NEEDS

**YOU**

---

# 1.1

## The Insider Threat

### Betraying the trust

- Insider(s) must overcome every human being's natural tendency to remain loyal to the organisation.
- Societal norms, personal beliefs, moral and ethical codes are normally a good insurance against betrayal.
- Overcoming fears of discipline, embarrassment, loss of employment, arrest and the possibility of death is (very) hard for most employees.
- Some will never betray the organisation regardless of circumstances.
- Most people find betrayal to be (very) difficult to carry out.
- Most will remain generally loyal but may "cheat" or "cut corners" if actions will not result in criminal charges or in being fired.
- Some will commit serious acts of betrayal under duress - work or home stressors or life events, grow to the point where the Insider can no longer handle the stress.
- Highest risks are people who have little or no capacity to remain loyal to the organisation.

Every betrayal  
begins with  
**trust**

Potential Insiders often demonstrate a liability or tendency to suffer from a particular condition, hold a particular attitude, or act in a particular way. Some of the possible dispositions are listed below:

## Predispositions

Any capacity for disloyalty is a predisposition to becoming an Insider Threat. Predispositions will not predict who will be an Insider Threat but do indicate who may be more apt to become a threat.

- **Divided loyalties:**  
put employees at risk of choosing the competing loyalty:
  - Host country/nationality versus employee's native country;
  - Work travel versus family obligations.
- **Life experiences:**
  - Cultural and moral upbringing regarding loyalty to family, country, ideals and religious beliefs;
  - Marriage, war, conflict and economic downturn can influence loyalty.
- **Personality:**
  - Certain personality traits make individual less likely to display loyalty to an organisation;
  - Some people have a sense of "moral flexibility";
  - A few people have no sense of moral "right and wrong" (psychopaths understand right or wrong as a concept, but don't care).
- **Relationships with others and society:**  
some have difficulty relating to, or bonding, with others. As such, they may not care about others and are less likely to consider how their actions may affect the organisation or their co-workers:
  - Lacks moral values or personal integrity;
  - Disregards social norms, rules & etiquette;
  - Feels above the rules, or, "rules only apply to others".
- **Questioning self:**  
some have difficulty understanding themselves. They are so preoccupied with trying to understand identity that they disregard others or the organisation. Such people are less likely to consider how their actions may affect the organisation or their co-workers. They often show/seem:
  - Low self-esteem;
  - Identity disturbance;
  - Lack of maturity;
  - Superficiality.
- **Unstable self:**  
some have difficulty controlling moods or handling emotional situations. Such people are likely to lash out or make irrational and emotionally charged decisions without consideration for impact on others. They could be:
  - Emotionally unstable;
  - Anger management issues;
  - Fantasizing;
  - Restless and impulsive;
  - Self-Absorbed.

Research has shown that three personality disorders combined present a much higher risk for security concerns than other mental disorder.

Trusted Insiders can unknowingly or intentionally assist external (third) parties in conducting activities against the organisation or they can commit malicious acts for a wide variety of reasons. It should be clear that there is not a single type of trusted Insider. However, there are broadly 3 categories of trusted Insiders who could pose a threat:

- The **unintentional Insider**: the employee does not understand actions are harmful. The employee has no intention to cause harm and may demonstrate very few indicators of risk.
- The **negligent Insider**: the employee knows that his/her actions are a security violation but “takes a chance” to “cut corners.” The employee may demonstrate some indicators of risk.
- The **malicious Insider**: the employee takes action specifically for the purpose of damaging the organisation. The employee may take steps to hide indicators of risk.

There are two types of malicious Insiders:

**Self-motivated Insiders**: they are individuals whose actions are undertaken of their own volition, and not initiated as the result of any connection to, or direction by, a third party.

**Recruited Insiders**: they are individuals co-opted by a third party to specifically exploit their potential, current or former privileged access. This includes cultivated and recruited foreign intelligence, or their entities with malicious intent.

All malicious Insiders intentionally use their access to resources for financial gain, or to cause harm, loss or damage. Almost all physical and electronic attacks need to be assisted or conducted by an Insider. Some attacks can only be committed by Insiders, such as the unauthorised release of proprietary information or the sabotage of assets that only employees can access.

Most self-motivated Insiders are a result of an individual seeing an opportunity to exploit their access while already employed, rather than having sought employment with the intention of committing an Insider act.

Information obtained from an unintentional Insider is often the result of a lack of security awareness and a failure to follow security protocols. Often, an unintentional Insider acts in breach of their duty to their employer. Additionally, a trusted Insider who inadvertently assists an external party may not be aware that they are allowing access to assets or passing on information, or that the resources they are providing are valuable and wanted by someone else.

Studies indicate that most Insider cases involve a self-motivated Insider. It is not only government employees who are targets of exploitation and recruitment as an Insider; businesses, large and small, may also be targeted.

### Characteristics of Employees at Risk

- Not impulsive.
- Multiple Motives.
- Ineffective crisis management in the past.
- Pattern of frustration, disappointment, and a sense of inadequacy.
- Seeks validation.
- Aggrandized view of their abilities and achievements.
- Outspoken sense of entitlement.
- Rules not applicable to self.
- Actions seek immediate gratification, validation and satisfaction.

### If the Employee's needs are not met, the Employee becomes....

- Rebellious.
- Passive aggressive.
- Destructive.
- Complacent.
- Self perceived value exceeds performance.
- Intolerant of criticism.
- Unable to assume responsibility for their (own) actions.
- Blaming others, lack of self-criticism.
- Minimizing of their (own) mistakes or faults.

**The greatest vulnerability to asset loss may not be from an outsider, but the end result of a pattern of behaviours and actions taken wittingly by an "Insider".**

## Motivation

The FBI's researched CRIME model shows following motivation traits:

- **Compromise** - Outsider coerces employee to conduct an attack.
- **Revenge** - Employee feels wronged by the organisation and conducts the attack to "get even."
- **Ideology** - Employee supports ideals which are contrary to the ideals supported by the organisation and conducts an attack to "set the record straight."
- **Money** - Employee conducts the attack for financial gain.
- **Ego** - Employee likes the excitement of "being a spy" or thinks he is better than the organisation's management or security department.

## Insider Threat Drivers

Research shows most employees do not join an organisation with the intent to become an Insider Threat.

After being hired, the employee experiences some type of significant life change. The employee then takes a series of actions, which leads to a threat. This phenomenon suggests there is a pathway the employee takes to become a threat.

**There are distinct and preventable drivers of Insider Threats which are influenced by an organisations' established policies, procedures, and values.**

### Malice

**An act that is malicious and intentional in nature to cause damage.**

- Current or former employees that are triggered by a specific work-related or non-work-related incident such as a poor performance review and large amounts of debt.
- Insiders typically develop a plan in advance of the act that someone within the organization may detect.
- Examples: Information and asset exploitation such as espionage, fraud, corruption, and IT system exploitation.

### Negligence

**Lax approach to policies, procedures, and potential security risks.**

- Over time employees may become more lax about security policies.
- Violators often assume that their specific behaviour does not have a noticeable impact or that no one is monitoring their behavior.
- Examples: Removal of proprietary or classified information or material from secure areas; forwarding information to home email addresses to work on a task after hours; inappropriately placing information in an open and unsecure area.

### Accidental

**Lack of awareness of policies and procedures creates security risk.**

- Employee ignorance is a challenge to organisations attempting to manage and maintain a secure organization.
- Lack of understanding of security protocols, and the potential impact if not followed, further exacerbates the impact of unknowing exposure of critical information.
- Examples: Disclosure or dissemination of information determined to be proprietary or classified to persons without clearance or purpose to have the information; irresponsible handling of classified or proprietary information; irresponsible use of information systems.

### Underlying Themes

- Process of idea to action.
- Discernible patterns of behaviour.
- Personality styles.
- Accumulation of problems.
- Crisis as a trigger.
- Exploitation deemed to be a solution.

## Insider Threat Pathway

Since progression along the pathway is a deliberate action, human factors such as motivation and intent are critical to understand. As the employee makes individual decisions to move along the pathway, he or she will often display a number of observable behaviours. By matching an employee's observable behaviours with phases along the pathway, investigators can start gaining a sense of how far down the pathway to an attack the employee may be.

Motivations, and the observable behaviours associated with them, will vary by person and by the employee's individual situation.

### Causes

- Private or work-related crisis (financial, personal, relational, health, life events, etc.).
- Feelings of frustration, disappointment or disgruntlement.
- Over-inflated sense of abilities and achievements.
- Strong sense of entitlement and egoistic view of what the organisation is, or is not, doing to/for them.
- Need to demonstrate value to others to be recognised.

### Effects

- Revenge.
- Retaliation.
- Rebellion.
- Seek ways to achieve immediate gratification, satisfaction.
- Resolve a conflict or perceived injustice.
- Act passive aggressive or destructive towards others. Especially if Insiders think that they are neglecting them, or not recognising their potential.

### Actions

- Disclose proprietary, sensitive, restricted or classified information.
- Sell document(s) and/or information.
- Sabotage facilities, material or systems.
- Enables access to facilities to others.
- Hurt others.
- Commit suicide.



## Insider Threat Models

Researchers in Insider Threats have developed a number of models. A good number of these models describe a pathway to becoming a threat.

As of yet, there is no one model which fully explains every Insider Threat. Models will not predict Insider Threats but can be used to assess employees for risk. Understanding each of the models can assist investigators (post holders) in better understanding how to identify an Insider Threat.

The 5 main Insider Threat models are:

- Fraud Triangle<sup>3</sup>:
  - Pressure, such as a financial need, is the “motive” for committing the fraud;
  - Employee identifies an internal control weakness and commits fraud;
  - Employee rationalizes the fraud making it easier to continue the fraudulent activity.
- Pathway to Intended Violence<sup>4</sup>;
- Critical Path Model<sup>5</sup>;

- Stressor Emotion for CWB (Counter-Productive Work Behaviour)<sup>6</sup>:
  - The Stressor-Emotion model of counterproductive work behaviour (CWB) is based on prevalent approaches to emotions, the stress process in general and job stress in particular.
  - The sense of control is key to the appraised coping capacity. A combination of perceived stressors and insufficient control is likely to trigger negative emotions, which in turn increase the likelihood the employee will engage in CWB, which is viewed as a special case of behavioural strain.
  - Radicalisation & Mobilization Framework<sup>7</sup>.

We strongly encourage to consult the resources provided in the footnotes to gain a better understanding of Insider Threat models and drivers.

Please note that these resources are valid at the time of writing, but the authors cannot guarantee that they will remain so.

<sup>3</sup> Developed by sociologist Donald Cressey.

<sup>4</sup> F.S. Calhoun & S. Weston - *Contemporary threat management: A practical guide for identifying, assessing and managing individuals of violent intent*. © 2003 F.S. Calhoun & S. Weston.

<sup>5</sup> Eric Shaw and Laura Sellers - *Application of the Critical-Path Method to Evaluate Insider Risks*.

<sup>6</sup> Paul E. Spector & Suzy Fox - *The Many Roles of Control in a Stressor-Emotion Theory of Counterproductive Work Behaviour*.

<sup>7</sup> See: [http://gangerforcement.com/uploads/2/9/4/1/29411337/radicalization\\_process.pdf](http://gangerforcement.com/uploads/2/9/4/1/29411337/radicalization_process.pdf)

# 1.2

## Increase in Insider Threat Cases

### Why is there a marked increase in Insider Threat cases?

- Before the commonly accepted definition of Insider Threat, many criminals were listed as common “criminals” in the statistics and little differentiation took place.
- Employees suffer(ed) financial hardships during recent economic downturns.
- Linked to these economic downturns, or increased competition, employer affordability initiatives like reduction of benefits and pension plans, lay-offs, etc. create further employee hardships and (potential) resentment.
- The global economic crisis leading foreign nations (state actors) to become more eager to illegally acquire new technologies and R&D results, or, the overall increase in mergers, acquisitions, divestitures, joint ventures creates a climate where information exchange becomes easier.
- The extreme ease of stealing anything stored electronically/digitally.
- Increasing exposure to foreign intelligence entities (FIE) presented by the reality of global business, joint ventures, and the growing international footprint of multinational companies.

# 1.3

---

## Who is an Insider in Transportation

While the examples we provide in this section are based on the aviation ecosystem, they can be transposed to other transportation modes or critical infrastructure. The aviation examples were chosen due to the heavy media interest in recent times and the resulting familiarity of it towards the public.

The aviation ecosystem is rather unique; it is a micro-society with theoretically and technically educated employees mixing daily.

The industry should also gradually accept the idea that also lower-income employees are security partners and should be motivated/activated to form part of the security chain. (e.g.: cleaning staff are the eyes and ears of every airport/station and are present in every nook and cranny of airport terminals, train stations and buildings. They should be considered the first security layer partner).

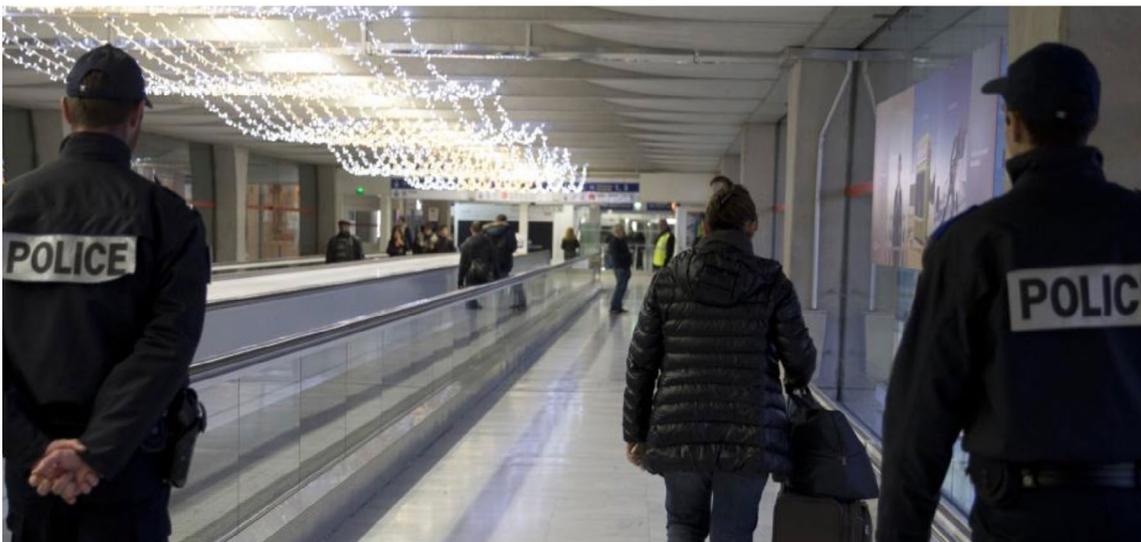
Every aviation ecosystem stakeholder operates in its own niche with unique threat possibilities. InTP awareness must be adapted at each local environment.

Potential Insider Threats within the aviation industry include a wide variety of individuals involved with aircraft and passengers, including, but not limited to, the following categories:

- airline employees;
- retail concessions and food & beverage outlets employees;
- cleaning and catering crews;
- fuelling, ground handling and FBO employees;
- construction and maintenance crews;
- freight warehouse and road transport operator staff;
- law enforcement, military, fire brigade, EMT and/or security personnel;
- taxi cab, metro/train, shuttle bus and/or other transportation specialists;
- current and/or former national CAA employees;
- current and/or former (contract) government employees;
- airport management;
- air traffic controllers;
- etc ...

## Aéroports de Paris : près de 70 badges retirés à des agents, notamment pour radicalisation<sup>8</sup>

"Près de 70 badges" d'agents sur les 85 000 qui travaillent dans les zones les plus sécurisées de Roissy et Orly avaient été retirés à leurs porteurs depuis les attentats du 13 novembre.



<sup>8</sup> Airports in Paris (France); nearly 70 Airport ID Badges removed from agents, in particular for radicalisation.

*After the November 13 attacks (2015), Paris airports, Roissy (Charles-De-Gaulle) and Orly, which employ some 85000 employees, revoked nearly 70 Airport ID Badges from staff working in security restricted areas.*

# 1.4

## Abbreviated Insider Threat Case Studies

### Case Study 01: Maritime Terrorist Attack

Two terrorist cells (monitored by EU intelligence agencies) demonstrated a high interest in monitoring maritime traffic. Intercepted internet sites included “Marine Traffic<sup>9</sup>”, which shows live the traffic of any maritime vessel.

(Note: this is very similar to aircraft tracking, possible through popular tracking APPs/websites like FlightRadar24, FlightAware, PlaneSpotter, etc.).

The initial suspicion highlighted the possibility that the terrorist groups were participating in smuggling activities, as a number of monitored targets included container ships. Since the US authorities have intercepted on one or more occasions maritime containers configured for living/smuggling, the activities with screening of sea containers have increased (from approx. 3-4% to perhaps 5-6%).

However, it seems that the evaluation has showed that the monitoring of the sea traffic was focused on 2 chemical tankers and 2 -3 smaller general freight vessels. The 2 chemical tankers were owned by an Asian shipping company with a European commercial branch.

Review of the vessels crew logs showed that one of the Chemical vessels deck crew was provided by an agency, which was suspected of aiding pirates in Somali waters (it's an agency that could not operate without some form of cooperation with criminal groups). It appears that the individuals provided to the targeted vessels were part Somali/ part Pakistani origin but claimed to be Filipino and were holding forged Seafarers certificates.

<sup>9</sup> <http://www.marinetraffic.com/ais/>

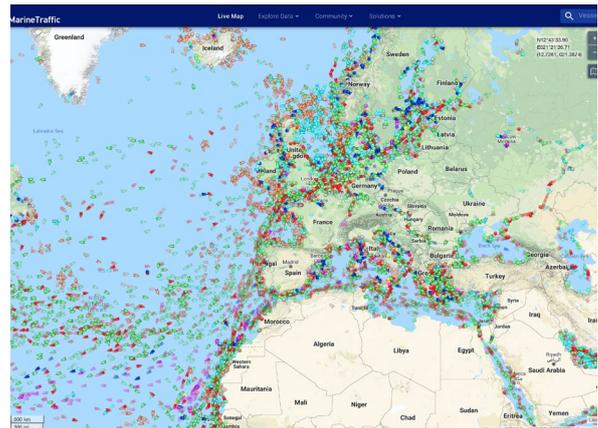
Those who were arrested have made many calls to the countries of interest.

The chemical tanker was carrying chlorine gas on several of the reported journeys. The crew had access to the areas that manage loading/unloading of the chemicals and the act of sabotage was considered real. One of the arrested operatives was during short time living in the same house in Somalia as one of the arrested ship crew members. One of the laptops from the arrest location showed detailed instructions taken from a technical industry website<sup>10</sup>.

### Possible plot situations:

1. Discharge of the chlorine gas in the port area (after mooring) to cause massive damage to local public, facilities and psychological damage.
2. Sabotaging the ship and setting it on fire inside the port areas (or approach shipping lanes) for the purpose of shutting down an important commercial shipping infrastructure (similar to the February 2004 “Abbu Sayyaf Group” (ASG) IED attack on “SuperFerry 14” which killed some 116 people).
3. Creating a shipborne improvised explosive device (IED) and detonating it adjacent to a high density passenger ship (e.g. cruise ship). This idea was highlighted by evidence of monitoring cruise ship traffic into specific EU ports.

Several EU ports were visited but it seems that the next port of call was supposed to be a major EU maritime port in central Europe.



<sup>10</sup> <http://www.chemicaltankerguide.com/preparation-for-unloading.html>

## Case Study 02: Insider Threat Critical Infrastructure (Nuclear)

In 2014 the Doel 4 nuclear reactor, near the Belgian city of Antwerp, was shut down following an oil spill. It soon became clear that the leak was most likely the result of sabotage. Was it an act of terrorism, by a disgruntled employee? To date, the investigation has not revealed definite results.

On 5 August 2014, around 11:06am, a safety valve was opened in the non-nuclear part of the Doel 4 nuclear reactor. In no time at all, 65,000 litres of lubricating oil drained from a storage tank to an underground reservoir. The Doel 4 power turbine was overheating and had to be shut down urgently.

The damage to the turbine was so extensive that Doel 4 could not be restarted until some 6 months later, in December 2014. The costs for the repairs amounted to more than 138 million euros. A large part of Belgium's electricity production capability was unavailable all along.

The opened valve is protected and is only intended for use in the event of a fire. It is therefore very unlikely to have been opened accidentally. From the very beginning, the nuclear power plant owner, Engie Electrabel, assumed that there was sabotage in the game.

Fortunately, there was no immediate threat to safety, but the fact that a nuclear reactor was shut down as a result of an act of sabotage was unseen in Belgium's nuclear industry safety records.

An investigation was launched under the direction of the Federal Public Prosecutor's Office and is being conducted with the utmost discretion coupled with the investigation by the FANC, the Belgian Federal Agency for Nuclear Control.

In December 2014, OCAD<sup>11</sup> stated that the investigation had shown that the crime was very well-prepared. Also according to OCAD, the investigation followed the path of terrorism. "If the Federal Public Prosecutor's Office were to deal with this case, it would mean moving in this direction," said one OCAD top executive.

The investigation focused on the employees who were present in the turbine hall on 5 August. The most logical scenario is that one of them, an Insider, was responsible for the sabotage. This involved some 60 people: Engie Electrabel employees themselves and subcontractors. Everyone was questioned, and following this, the group of potential suspects was then shortened. The aim was to test the last suspects with a lie detector in May 2015. Eight employees refused this test on the recommendation of their lawyers and trade unions.

It can be said with some certainty that one of these eight might be the actual perpetrator of the act of sabotage. The tests with the lie detector were finally carried out in May and June 2015. But since then, this part of the investigation has come to a standstill. The judicial investigation concluded in December 2016 only states 'that no perpetrator could be found'.

<sup>11</sup> OCAD: Organisation for the Coordination and Threat Analysis, Belgian law enforcement and intelligence services coordination unit: <http://www.comiteri.be/index.php/en/39-pages-gb/306-what-is-the-coordination-unit-for-threat-assessment>

## Stricter safety procedures

There were also concerns that there were no CCTV images of the crane being opened and no fingerprints or DNA material.

In order to prevent similar incidents in the future, the FANC imposed a series of additional safety measures on all Belgian nuclear power plants immediately after the incident.

Both in Doel and Tihange (the other Belgian Nuclear Reactor facility), 150 extra CCTV cameras will be installed. Even more doors were equipped with magnetic cards so that they can register when and by whom the doors are opened.

The screening of employees has become even stricter. The so-called “four eyes principle”<sup>12</sup> has been extended, which makes sure that certain areas cannot be accessed if the workers are on their own.

These are just a few concrete examples of measures that are part of an extensive security regime, which cannot be further explained because of its confidential nature. These measures have been added to the security measures already in place as a response to the incidents.

## Investigation continues

At the end of 2016, Engie Electrabel asked the examining magistrate for an additional investigation. “We have submitted a request to the investigating judge for additional investigative measures so that they go as far as possible in the investigation”, says their spokeswoman. “We hope to see results as soon as possible. But that result has not been achieved for the time being. “The investigation is still under way”, is the only thing the Federal Public Prosecutor wants to divulge.

In March 2018 a case update was published: “In the investigation into sabotage at the Doel 4 nuclear reactor, no perpetrator has yet been found”, that is what the Belgian Federal Minister of Justice, said in response to a question from a MEP of the “Green” party in parliament.

<sup>12</sup> The “four eyes principle” is a requirement that two individuals approve some action before it can be taken. The four eyes principle is sometimes called the two-man rule or the two-person rule.

### **Case Study 03: Espionage or Malicious Insider.**

The case of Edward Snowden brought Insider Threat to the forefront of the public and corporate minds. He provides a case study for the intelligent Insider Threat, a trusted (and vetted) employee who acts in violation of his organisation's policies and discloses massive amounts of restricted information to the public (or a competitor). Snowden's tale should serve as a warning call to government and industry leaders.

In June 2013, computer expert Edward Snowden, a former Central Intelligence Agency (CIA) system administrator and National Security Agency contractor, illegally removed up to 1.5 million classified documents from the US NSA and released these to the world press. The secrets were stolen from "NSANet", the agency's internal computer network, and from an intelligence community-wide system called the Joint Warfighter Information Computer System. The 1.5 million documents, if printed out, would form a pile more than 5 kilometres high. As a computer systems administrator, Snowden used download tools called scraping software, specifically a program called "wget" and "DownThemAll!" that allowed large numbers of files to be downloaded over slow networks. He also accessed a small number of documents by asking unsuspecting colleagues for their usernames and passwords.

It is estimated that Snowden shared between 50,000 and 200,000 classified documents with reporters, of which only a very small percentage have been made public so far.

His actions violated the US Espionage Act of 1917, which defines the leak of state secrets as an act of treason. Yet despite the fact that he clearly broke the law, Edward Snowden argued that he had a moral obligation to act. He gave a justification for his "whistleblowing" by stating that he had a higher duty "to inform the public as to that which is done in their name and that which is done against them." Again, according to Snowden, the government's violation of privacy had to be exposed regardless of legality.

There were a number of warning signs to suggest Snowden could become a trusted Insider, including inconsistencies on his CV. He also promoted his ideological views using social media.

Further reports suggest that the company which completed Snowden's security clearance, had been accused of signing off on thousands of incomplete security checks.

The disclosures of NSA documents to date represent the "tip of the iceberg" of more damaging disclosures, the estimated cost of mitigating the damage could reach a roughly estimated €1 billion.

## Case Study 04: Malicious Insider Aviation Terror Plot.

Daallo Airlines Aircraft Bomb aka “The Successful Failure”.

On 2 February 2016, an explosion occurred on board Daallo Airlines Flight 159, an Airbus A321, shortly after take-off from Mogadishu (Somalia), which tore a hole in the fuselage. The aircraft involved was a 19-year-old Airbus A321, owned by Hermes Airlines, and operated by Daallo Airlines at the time of the incident. The aircraft was operating a sub-service for Turkish Airlines, the only airline with regular scheduled flights to Mogadishu airport at that time.

The explosion occurred on board the aircraft, blasting a hole in the fuselage behind the R2 door. It was reported that day that the explosion was most likely close to seats 15/16F, abeam the anterior wing root and fuel tanks. At the time of the incident, there were 74 passengers and 7 crew members on board.

The pilots warned Mogadishu’s tower and reported a pressure problem but did not declare an emergency. The aircraft returned to Mogadishu Aden Adde International Airport and made an emergency landing. Two injuries were reported, and the burnt body of the suicide bomber fell out of the airplane, landing in the town of Dhiiqaaley near Balad, Somalia; where it was found by nearby residents.

The flight had been delayed before departure, as a result of which the aircraft was not yet at cruising altitude at the time of the explosion and the cabin was not yet fully pressurised. It was thought that a laptop was equipped with a timer device to detonate the bomb middle flight.



## Investigation

The Somali Air Accident Investigation Authority (SAAIA) stated on 3 February 2016 that one person was missing on the aircraft when it returned to Mogadishu and later confirmed that the body of the missing person had been found near Balad. The bombing was investigated by the National Intelligence and Security Service in cooperation with the airport authorities and the local police. Daallo Airlines stated that a technical team of Hermes Airlines, the owner of the aircraft, as well as the manufacturer of the aircraft, Airbus, were playing a role in the active investigation. The US FBI were also contributing to the investigation.

Initial tests of damage to flight 159 confirmed traces of explosive residue. It was thought that a bomb, possibly hidden in a laptop, had been brought onto the plane by a wheelchair user. Two passengers on the aircraft, one of them sitting on the next seat, were arrested on suspicion of complicity. On 6 February, Transport Minister Ali Ahmed Jama confirmed that the explosion had been caused by a bomb “intended to kill all people on board”.

The Somali authorities identified the deceased passenger as Abdullahi Abdisalam Borleh, a 55-year-old male from Hargeisa, the capital of the Somali island region of Somalia, but did not confirm that he was suspected of being a suicide bomber. Borleh was a teacher at an Islamic school and has indicated that he was going abroad for health reasons, according to Sheikh Mohamed Abdullahi, a mosque imam in Hargeisa.

A Somali federal official stated that Borleh had been checked by security officers ‘but we had never considered him dangerous’.

A CCTV camera recording<sup>13</sup> from the airport shows two men, seemingly airport workers, giving a laptop to Borleh. U.S. officials said that the researchers believed the bomber had some connection with airline or airport staff.

At least 20 people, including government officials and the two airline employees, were arrested on suspicion of links with the attack. The Serbian pilot, Vlatko Vodopivec, criticised the lack of security around the aircraft at the airport and described the facility as “chaotic”. In an interview with the Associated Press, Vodopivec explained “Security is zero. When we park there, about 20 to 30 people come to the asphalt. No one has a badge or those yellow vests. They go in and out of the plane, and no one knows who is who. They can put everything in when the passengers leave the plane”.

On 13 February, eleven days after the incident, the Islamic militant group al-Shabaab claimed responsibility for the attack in an e-mail statement, stating that it was “a retaliation for the crimes committed against the Muslims of Somalia by the coalition of Western Crusaders and their intelligence services”. Al-Shabaab also said that it focused on Turkish Airlines, because Turkey is a NATO Member State supporting Western operations in Somalia, and that it focused on Western intelligence officers and Turkish NATO soldiers on board.

<sup>13</sup> <https://www.youtube.com/watch?v=6RKyd09T3nM>

## **Brief Case Study 05: Malicious Insider Train Terror Attack Plot.**

In October 2015, a Russian citizen who worked as an engine-driver's mate<sup>14</sup> was said to have confessed to preparing an explosion on a suburban train.

The Russian intelligence service, FSB, arrested A. K. Ferzaliyev, who on "VKontakte"<sup>15</sup> administered a terror-focused group." The man had been planning to flee Russia after having carried out the attack, to join the ranks of Islamic State terror group fighters in Syria.

The man had published materials defending the actions of banned terrorist groups and had attempted to recruit new members for the Islamic State on his "VKontakte" page.

He had also contacted an Islamic State member in Syria and had asked for instructions on how to build an improvised explosive device (IED).

Mr. Ferzaliyev confessed his plans and is currently under arrest pending further investigation.

## **Other Cases**

Unfortunately, there have been many more cases in history involving Insiders as perpetrators in the aviation industry. We would like to mention also the following which can be looked up on-line as they are also quite well documented:

- Auburn Calloway (FedEx 705) (April 1994) (Disgruntled ex-FedEx employee tried to kill crew and crash the aircraft);
- Andreas Lubitz (Germanwings 9525) (March 2015) (Suicide and deliberate crash);
- Rajib Karim (British Airways ICT Expert) (February 2011) (Planned ICT crash & Explosives on-board BA aircraft);
- 100 Staff Members of the Malaysia Airport Immigration Department (2016) (Passport fraud);
- Eugene Harvey (Delta Airlines Baggage Handler, Atlanta Airport) (2014) (Gun Smuggling).

<sup>14</sup> A driver's mate travels with the driver helping the driver with all logistic aspects.

<sup>15</sup> Vkontakte ("VK") is a Russian online social media and social networking service with some 500 million accounts. VK allows users to message each other publicly or privately, to create groups, public pages and events, share and tag images, audio and video, and to play browser-based games.

# 1.5

---

## Insider Threat Ecosystem

The most effective protection against Insider Threats does not depend on a single measure, but rather on taking a holistic approach, which:

- Takes a risk-based approach;
- Focuses on assets and those who protect them;
- Sees risk posed by people as a corporate risk;
- Evolves, based on current and emerging threats;
- Appoints one senior owner of human risk which reports directly to the CEO;
- Decides on, and develops, a clear organisational security culture (an InTP does not replace a comprehensive security program);
- Seeks input from across the entire organisation to address human risk(s) (e.g. legal, HRM, ITC, operations);
- Implements transparent and ethical (security) policies.



**Organisations must define what constitutes an Insider, threats to mitigate, risk tolerance, key stakeholders, and critical assets to protect.**

### Types of Insider Threat Incidents

### Insider Threat Drivers

#### Who is an Insider Threat?

A person who has the potential to harm an organisation for which they have inside knowledge or access.

An insider threat can have a negative impact on any aspect of an organisation, including employee and/or public safety, reputation, operations, finances, national security, and mission continuity.

#### **Information Theft**

Use of Insider access to steal or exploit information.

#### **Workplace Violence**

Use of violence or threats of violence to influence others and impact the health and safety of the organisation's workforce.

#### **Security Compromise**

Use of access to facilitate and override security countermeasures (e.g. drug and contraband smuggling).

#### **Espionage**

Use of access to obtain sensitive info for exploitation that impacts national or corporate security and public safety.

#### **Terrorism**

Use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes.

#### **Physical Property Theft**

Use of Insider access to steal material items (e.g., goods, equipment, badges).

#### **Sabotage**

Intentional destruction of equipment or IT to direct specific harm (e.g., inserting malicious computer code).

#### **Other**

Captures the evolving threat landscape including emerging threats not covered in the previous examples.

#### **Malicious**

Employees who intentionally abuse their privileged access to inflict damage on their organisation or co-workers.

#### **Negligent**

Employees whose careless approach to policies, procedures, and information security exposes the organisation to external risks.

#### **Accidental**

Employees whose lack of awareness of (the) organisations security policy, procedures, and protocols exposes the organisation to external risks.

# 1.6

## Threat Actions

Organisations must define what constitutes an Insider (Threat), threats to mitigate, risk tolerance, key stakeholders, and critical assets to protect. Insider activities can range from passive betrayal to active, unwitting or unwilling involvement in causing harm, or:

- Theft: such as espionage, data loss, property theft or media leaks.
- Sabotage: such as the destroying or disrupting of organisational equipment, compromise of operations, corruption of information or disruption of decision-making ability.
- Workplace Violence: such as intimidating co-workers, physical violence, shootings.
- Terrorism Support: such as recruiting co-workers, using organisational assets to provide material support to terrorist organisation, attempting to influence organisational policy or operations.

## Vulnerabilities - Examples

Below are listed some of the means that a malicious Insider could use to easily steal and remove the company's confidential data, which therefore highlight these companies' vulnerabilities:

- Using a smartphone's hot spot capability to connect a WIFI enabled laptop or desktop computer to the internet, then upload the information to webmail, a data "cloud" or any other source.
- - **Step 1** Downloading all the information from a network shared drive, to a local hard drive;  
- **Step 2** Then disconnecting the computer from the network;  
- **Step 3** Installing external hard drive;  
- **Step 4** Booting from CD and cloning to 1st hard drive;  
- **Step 5** Leaving the company premises, unchallenged, with the external hard drive with confidential data.
- Using remote access software installed on an internet connected computer that contains sensitive information and accessing network shares ("teamviewer", Apple remote desktop connection, etc.).
- Using screen sharing software on an internet connected computer that contains sensitive information and access to network shared drives.
- Using USB storage devices or removable, writeable media (USB sticks, smart phones, mp3 players, DVD-R, ZIP-disks, etc.).
- Using fax machines and multi-function devices (without authentication) or computer webcams.
- Storing stenography software on the cloud (iCloud, DropBox, OneDrive).
- Using a PC/laptop/smartphone microphone to dictate protected information to a sound file, then e-mailing the sound file to the Insiders' personal e-mail account, or placing it on removable media.
- Scanning/OCR-ing sensitive or classified documents to an Internet-connected scanner with e-mail capabilities and e-mailing to the individual's personal e-mail account or another individual, or placing it on removable media.
- Using company e-mail or web based personal e-mail and exporting the Insiders e-mails and/or folders to a compressed email container file, and then e-mailing to the individual's personal e-mail account or another individual, or placing it on removable media.
- Posting information not for public disclosure on social networking websites.
- Disclosing information not for public disclosure in public areas, to the news media, other sources, by any means (Whistleblowing).
- Using a work phone (verbally releasing information to competitors, outside sources, etc.).

- Using a smartphone (PED/BYOD) or portable hand-held document scanner or mouse scanner (verbally, pictures, recording, scanning).
- Using any electronic devices (to include covert spy gadgets<sup>16</sup>) that the Insider has brought into the company with or without approval.
- Simply walking out the front door with stolen documents or data (no security guard inspections).

The examples listed above only deal with data theft and show that threat possibilities are infinite. They highlight the need to hold mitigation exercises on a regular basis to define counter actions which, in turn, result in creating/ updating policies and procedures.

<sup>16</sup> Like these European operated web-shops specialised in selling surveillance/recording/monitoring electronics/solutions: <https://www.spywebshop.nl>, <https://www.camaras-espias.com>, <http://www.spy3k.be> or <https://www.flexispy.com>

# 1.7

---

## Threat Data

### **Insider Threat - frequency vs damage/cost. (Based on US data)**

**Insider Threat is not the most numerous type of threat:**

- 1900+ reported incidents in the last 10 years;
- Approximately 9% of incidents involve malicious Insider Threat actors.

**Insider Threats are generally the most costly and most damaging ones:**

- Average cost approximately 360.000 € per incident;
- Average victim loss: approximately 13 million € per year;
- Multiple incidents exceed 1 Billion €.

# 1.8

## Threat Landscape & Cybersecurity & Emerging Threats

**A threat is determined by assessing the INTENT to commit an act and the CAPABILITY to carry it out successfully. Both intent and capability have to exist for the threat to be considered genuine.**

The transportation industry and critical infrastructure are always at risk of security threats, criminal activity or terror attacks. With respect to the emerging Insider Threat trends in transportation, we expect to see a lot more cybercrime and the misuse of privileges, which therefore constitute the future weaknesses to monitor. The case of the Horizon Air “hijack<sup>17</sup>” by a Horizon Air ground service agent with no piloting experience shows what havoc can be created by an Insider with access privileges (and a suspected mental disorder).

Another important threat is that of hacking the control systems of a(n) aircraft/ship/train/vehicle. Transportation operators should therefore implement a layered approach to cybersecurity, which use several defence mechanisms such as access restrictions, 2-factor authentication, strong encryption, pro-active threat hunting, Insider Threat monitoring, and managed detection and response. Anonymisation of transport assets, linked to on-line platforms, should also be considered, where practical.

The best defence against those threats is advanced technology, which can be used to detect criminals/terrorists planning to orchestrate attacks.

Transportation ecosystems unfortunately have a tendency to focus their security efforts on compliance with existing regulations. As a result, they fail to detect, and prepare, for new vulnerabilities and evolving threats.

## Criminals

### Impact

Costly regulatory inquiries and penalties, consumer and shareholder lawsuits, loss of consumer confidence.

### Motivation

Financial gain.

### 2019 Outlook

Cyber-extortion will continue to rise.

## Insiders

### Impact

Competitive advantage, trade secret disclosure, operational disruption, brand and reputation.

### Motivation

Personal advantage, monetary gain, professional revenge, patriotism.

### 2019 Outlook

More organisations will implement Insider Threat mitigation programs, processes and training (Help2Protect Awareness CBTs are a good start).

## Hackers

### Impact

Disruption of business activities, brand and reputation, loss of consumer confidence.

### Motivation

Negatively impact reputation, drive attention to a cause, pressure for change.

### 2019 Outlook

Expected to escalate attack methods with high-profile data breaches.

## Nation States

### Impact

Loss of competitive advantage, disruption to critical infrastructure.

### Motivation

Economic, political, and/or military advantage.

### 2019 Outlook

Will continue to strengthen their defensive and offensive cyber (war) skills.

It is therefore strongly recommended that regular updates of security regulations and procedures be performed with due risk analysis. Each transportation company management team and their respective security department should always be “in-the-know” on emerging threats. Clearly, protection of transportation hubs and critical infrastructure must never be compromised.

## Cybercrime

The ever-emerging and growing threat is the “cyber battlefield”. Most companies are out-matched in their ability to combat cyber-attacks from Nation States, global criminals and malicious Insiders.

It is important to remember that in no other crime arena private organisations are expected to “do battle” with the likes of:

- Izz ad-Din al-Qassam Cyber Fighters;
- Anonymous;
- #RSAC;
- The Syrian Electronic Army;
- North Korea’s Bureau 121;
- Russia’s Sandstorm Crew;
- China’s 13638 group;
- Sandworm Team;
- Lizard Squad;
- Comment Crew;
- AnonGhost.

Cybercrime is global, unstoppable, ruthless, and requires special skillsets and protection measures. The saying “information is power” is certainly true when it comes to cybercrime. Access to your company’s and personal information is what gives hackers and “cyberfighters” the power to tap into your accounts and steal money or identities.

However, the right information can also empower companies and individuals to protect themselves from being caught up in this thriving criminal industry. With that in mind, here is a list of useful steps which can be taken to avoid becoming a cybercrime victim. Remember: good knowledge on cybercrime by the entire workforce will diminish the likelihood of generating cases of unintentional Insiders causing (great) harm to the company!



Logo of the Syrian Electronic Army

**Education:** hackers are not the only parties who can gain power from information. Companies should continue to educate the workforce about the types of scams that exist on the Internet and, when everyone knows to avert them, you can remain one step ahead of the cybercriminals. Educating the workforce is a first good step.

**Phishing:** this technique is prevalent; companies need to keep the workforce updated on how to recognize phishing attempts and learn from peers, case studies or ICT specialists. Phishing is when cybercriminals attempt to lure persons into revealing personal information by pretending to be a legitimate organisation or person. They are extremely convincing and use social engineering to convince recipients that they're dealing with legitimate persons.

**Firewalls:** this solution monitors traffic between your computer or network and the Internet. They generally serve as a great first line of defence when it comes to keeping unwanted intruders out.

**Hyperlinks:** every employee should be careful not to click on any links in messages from people that they don't know. Every harmless-looking link could direct to a fake website that asks for private information, such as user names and passwords, or it could download malware/ransomware onto a computer (or a complete network). Even if the message is from a known sender, people should be taught to remain cautious. Some viruses replicate and spread through email, so users need to look for information that indicates that the message is legitimate. (Educate users on the ways to verify email addresses on the company host mail program used)

**Safe surfing / website blocking:**

When navigating the web, employees need to take precautions to avoid phony websites that ask for personal information and pages that contain malware/ransomware. Search engines will help navigating to the correct web address, since it will correct misspellings. This will prevent employees winding up on a fake page at a commonly misspelled address. (A fake website at an address similar to the real site is called "typo-squatting," and is unfortunately a fairly common scam, especially for online payment providers and legitimate banks.)

**Payment pages:** employees with purchasing duties and privileges should be warned about on-line payment scams. On payment pages, employees should look for lock symbols in browsers, indicating that the site uses encryption to keep your information safe. Click on the icon to make sure that the security certificate pertains to the site you are on. (Staff should check the address bar to see if the site starts with "https://" instead of "http://" because this is another way to see if the site uses encryption.)

**Comprehensive security software systems:** should be used and kept updated. Cybercriminals will use a wide array and variety of ways to access company systems and information, hence the need for comprehensive security software that can protect you from all angles.

**Wireless network(s) protection:** cybercriminals can intercept and access data while it's in transit on a(n) (un)secured wireless network. Keep cybercriminals from doing this requires enabled firewalls and changing the WiFi password regularly (See also: Passwords strength).

**Passwords strength:** passwords are the most common form of authentication. In order to be effective, their use and implementation need to follow basic guidelines. ENISA, the “EU Agency for Network and Information Security” recommends following best practices:

### **Password Security for users**

- Passwords are secrets. Keep them so.
- Mix the kind of characters in your passwords.
- Use long passwords. Any windows password up to 9 characters can be cracked in seconds using public-domain tools. The longer the password, the longer it will take for an attacker to crack it. Every added character increases the cracking time by orders of magnitude. Any password that is not a common word, and is longer than 14 characters, cannot be cracked with normal current computing means.
- Use different passwords for different purposes or web sites. That way, even if someone manages to learn or crack one of your passwords, it does not give them immediate access to your other services.
- Use a password manager to create and remember random passwords.
- If a random password is impractical, use a pass phrase instead.

### **Password Security for systems administrators**

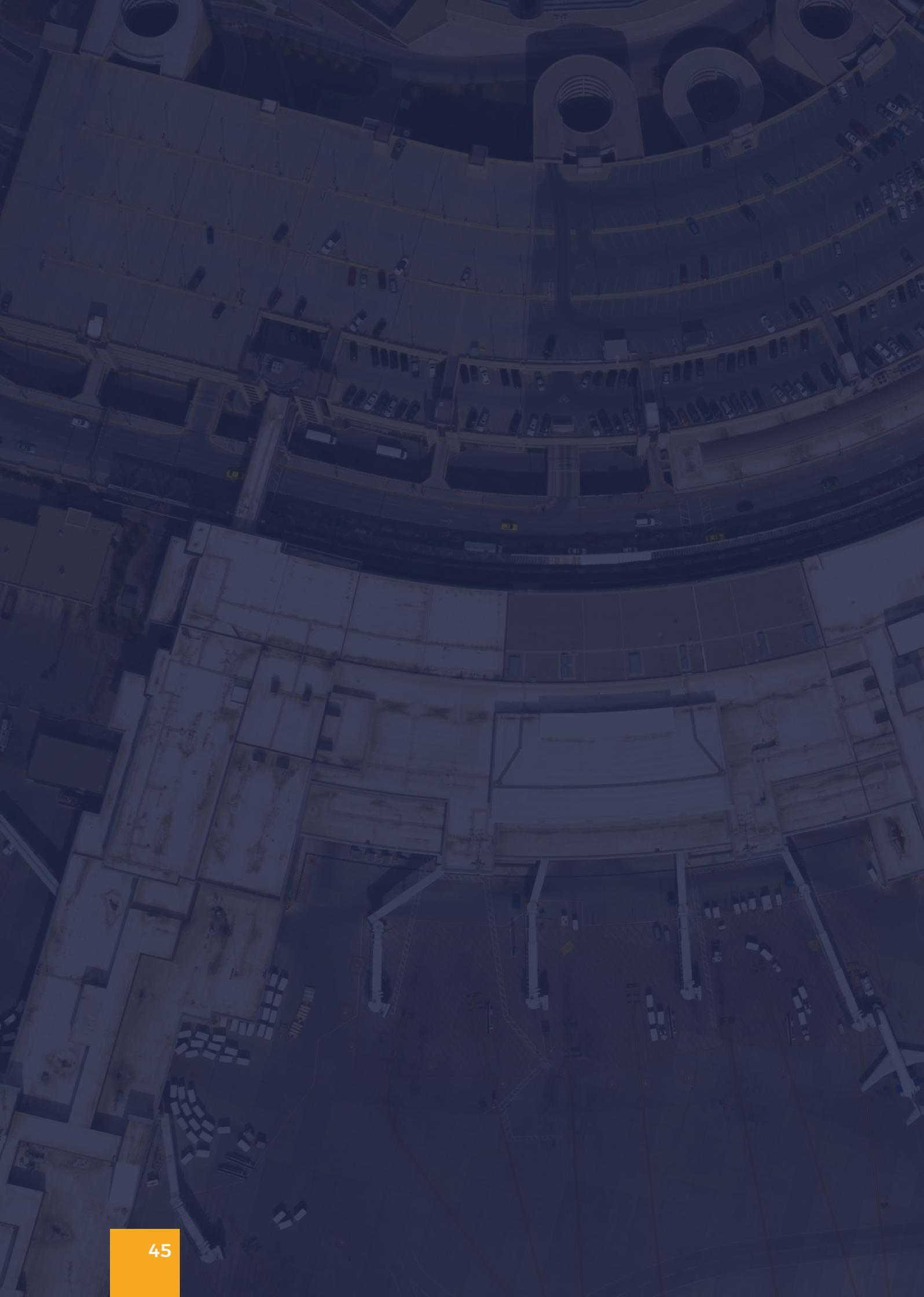
- Password managers should be provided to the users.
- Enforce long passwords through systems configuration.

- Do not force users to mix and match. A recent study shows that mandatory capitals or numbers encourage the users to use a predictable structure to their passwords. Instead, encourage users to use long and random passwords.

**Common sense:** despite the many warnings and detailed articles in the world’s press, cybercrime is increasing, fuelled by common mistakes people make, such as responding to spam and downloading attachments from people they don’t know. So, use common sense whenever you’re on the Internet. Never post personal information online or share sensitive information, such as your social security number and credit card number. Exercise caution when clicking on any links or downloading any programs.

**Being suspicious is the new normal:** even if company management and employees consider themselves cyber savvy, everyone should still need to keep their guard up for any new tricks and always be proactive about ICT-safety. Data backups should take place regularly (read: daily) in case anything goes wrong, and the finance department should monitor company accounts and credit reports to make sure that a(n) (Insider) criminal has not stolen company information or identity(ies).

Note: Even an unsuccessful criminal or terrorist attack has the potential to interrupt business continuity and damage customer confidence.



# 02.

---

## **Mitigating the Insider Threat and developing an Insider Threat Program (InTP)**

A question often heard by SME's and other stakeholders in the transportation industry and critical infrastructure is: "Why start/install an InTP - Insider Threat Program?"

**It can be neatly summed up in these few answers:**

- It is about protecting your assets, employees and customers;
- Companies really do not want to be a headline in "the news" because an Insider attack occurred;
- Be better prepared because at some point in time, it will become mandatory (in certain industries);
- Insurance companies, sponsors, customers will require this. Already now or in the (very) near future;
- Companies could reduce insurance premiums by having a robust InTP as part of their security program (ROI);
- Basically, it should just become part of your standard security procedures and this will also enhance your brand image.

# 2.1

---

## Insider Threat Indicators

Threat indicators are observable behaviours or conditions which indicate a specific threat is present. They can be general in nature (predisposition) or specific in nature (planning an attack).

Some behaviours are more indicative of certain types of attacks and may indicate progression along the pathway. The challenge is to correctly identify the appropriate mixture of observable behaviours, which may point to a risk of an Insider Threat.

By doing so, organisations may be able to determine where the employee is along the pathway, and possible risk mitigation strategies. The ultimate goal is to derail an attack before it happens. It is important to note again that even the smallest issue could cover or hide a more serious one. Innocent behaviour can hide radical motives and everyone should, over time and with training, develop a natural awareness and understanding of discrete changes and develop an eye for detail, which might provide clues to potential Insider Threats.

## **Pre-Incident Indicators (PII) (Red Flags)**

There is no “unique profile” of a terrorist, nor do terrorist incidents occur spontaneously.

In general, an (Insider) terrorist act requires certain dedicated preparation, like any other “logistics” act. It is planned, developed and carried out by individuals acting alone or as part of a group. However, the level of such preparation can differ.

A terrorist attack can be prepared in detail, taking a longer period of time, like the WTC attack in New York on 11 September 2001 (9/11), or it can be prepared within a shorter timeframe (Brussels Airport attack on 22 March 2016), with much less attention to detail.

To prepare an attack, terrorists have to undertake activities, such as intelligence collection, surveillance, training and movement of individuals, money and weaponry. Those employed within the transportation, critical infrastructure and security system industries can detect these activities.

Investigators should consider all observables over time to determine movement along the pathway, but:

- The employee(s) may not demonstrate any indicators;
- The presence of indicators does not necessarily mean the person is a threat;

- The list of Insider Threat indicators in this handbook is not complete, and probably never can be;
- Also note that employee(s) employee may demonstrate other behaviours not listed here.

The pre-incident indicators (PII) can help detect the preparation of a terrorist attack. They are divided in 6 groups as shown hereunder:

### ● **Workplace**

- Unusual visitors;
- Office used as suspicious meeting area;
- Unusual activities on strange hours;
- Unusual garbage disposal;
- Unauthorised data access: too many users with access privileges & increasing number of devices with access to sensitive data (BYOD & disable data access);
- Suspicious activity(ies) (user activity monitoring & server logs & odd working hours);
- Sloppy & careless behaviour (accidental information sharing & making (security) mistakes);
- Disgruntled behaviour (motivation);
- External cyber-attacks in all forms (enabled from within?);
- People repeatedly violating policies.

### ● **Transport**

- Misuse of company cars;
- Cars/vans used as observation vehicle;
- Overdue parked cars in parking lots.

### ● **Finances**

- Unusual excessive (unaffordable lifestyle);
- Committing cash-related crimes (smuggling, etc.).

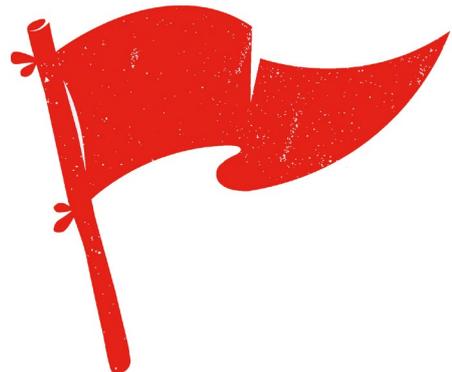
- **Forged Documents**
  - Fake identity and social security documents;
  - Fake credit cards.
- **Objects**
  - Use of photos, maps, schematics and blueprints;
  - Use of navigation & observation tools;
  - Appropriation of unauthorised uniforms.
- **Preparation**
  - Suspicious behaviour (near transportation and critical infrastructure);
  - Radicalised behaviour;
  - Documenting infrastructure;
  - Asking questions with no need to know.

Note: there is a (recent) shift from terrorist attacks from hard targets (protected people, institutions or services) to soft targets and public spaces (unprotected targets). A soft target can be defined as “person or object that is relatively unprotected or vulnerable, especially to military or terrorist attacks”.

Soft targets and public spaces are easily accessible (e.g. the truck attacks in Nice, London and Barcelona) hence posing a minimal risk for the (lone) terrorist, and can result in many victims (e.g. bomb attacks in Paris/Bataclan, Madrid/Metro, Boston/Marathon, Brussels Airport & Metro).

Companies should also provide guidance on how to understand and contextualise “red flags<sup>18</sup>”.

- Everyone in the organisation must understand that security within the company is not the responsibility of the Security Department alone, but that every single employee and department plays a pivotal role in securing the business. The company's security policy should clearly state this.
- Employees should know how to report suspicious issues that they see. Examples of “Red Flags” (Suspicious Behaviour) should be given, related to the respective ecosystem in which the company operates.



<sup>18</sup> “Red Flag” a warning sign for something that attracts usually irritated attention.

# 2.2

## Unintentional Insiders

A good example of the unintentional Insider is a person who does not adequately protect passwords, as shown below:

- **Shoulder Surfing:** When a person looks over another person's shoulder and watches keystrokes or watches data as it appears on the screen in order to uncover information in an unauthorized manner.
- **Dumpster Diving:** When a password is very hard to remember, the user might write it down, sometimes on a piece of paper, which will be discarded in garbage. The intruder would have to gain physical access to the premises, but the area where the garbage is kept is usually not highly guarded.

Remember: "Two out of three ICT breaches exploit weak or stolen passwords".

Other security violations creating unintentional Insiders are for example:

- Lending of credentials, like ID cards, key codes, physical keys, passwords, data carriers with confidential information, etc.;
- Opening doors/providing physical access and letting someone in a secured area without credentials;
- Ignoring suspicious activities (in secure areas), e.g. not challenging persons without visible credentials.

# 2.3

## Radicalisation - Basics & Indicators

Violent radicalisation can be defined as the phenomenon of people embracing opinions, views and ideas, which can lead to acts of (Insider Threat) terrorism. This can be motivated by (anti-) political, socio-economic, (anti-) religious or environmental/ecological reasons.

There are different sets of indicators, for both the process of radicalisation and the process of preparing a terrorist attack (by Insiders). The European Union's "AIRPOL COPRA on Airport" team has developed a separate set of indicators.

Whilst it should be clear that these 2 different processes are unmistakably linked with one another, the European Union "AIRPOL COPRA on Airport" team decided to develop a separate set of indicators, due to the specific nature of each process.

A key factor in preventing (Insider) terrorism in general is to avoid or stop the process of radicalisation. Indicators for recognising the radicalisation process fall within 3 general categories:

- Identity;
- Ideology;
- Behaviour.

The general indicators listed below can be attributed to one or more of these categories. They do not add up to a specific profile, but are signs that have been observed in individuals who have later radicalised. The simple fact that someone displays one of these indicators does not immediately indicate that someone is radicalising, let alone that (s)he should be called or labelled a "terrorist".

The overall picture of the observable changes should be looked at, and these indicators are only visible to those

who know how someone has behaved before and what changes have since taken place.

The process of radicalisation differs from one person to another and, for this reason, the possible signs must always be evaluated in their full context. To assess the indicators correctly, it is crucial to have solid additional background knowledge. If the indicators are assessed wrongly, actions by the company may instead drive the radicalisation process forward. Hence, companies need to address the issue with outside help, as thorough training and expertise will most likely not be available in-house.

Caution is required: none of the listed indicators can serve as evidence that an actual process of radicalisation is taking place!

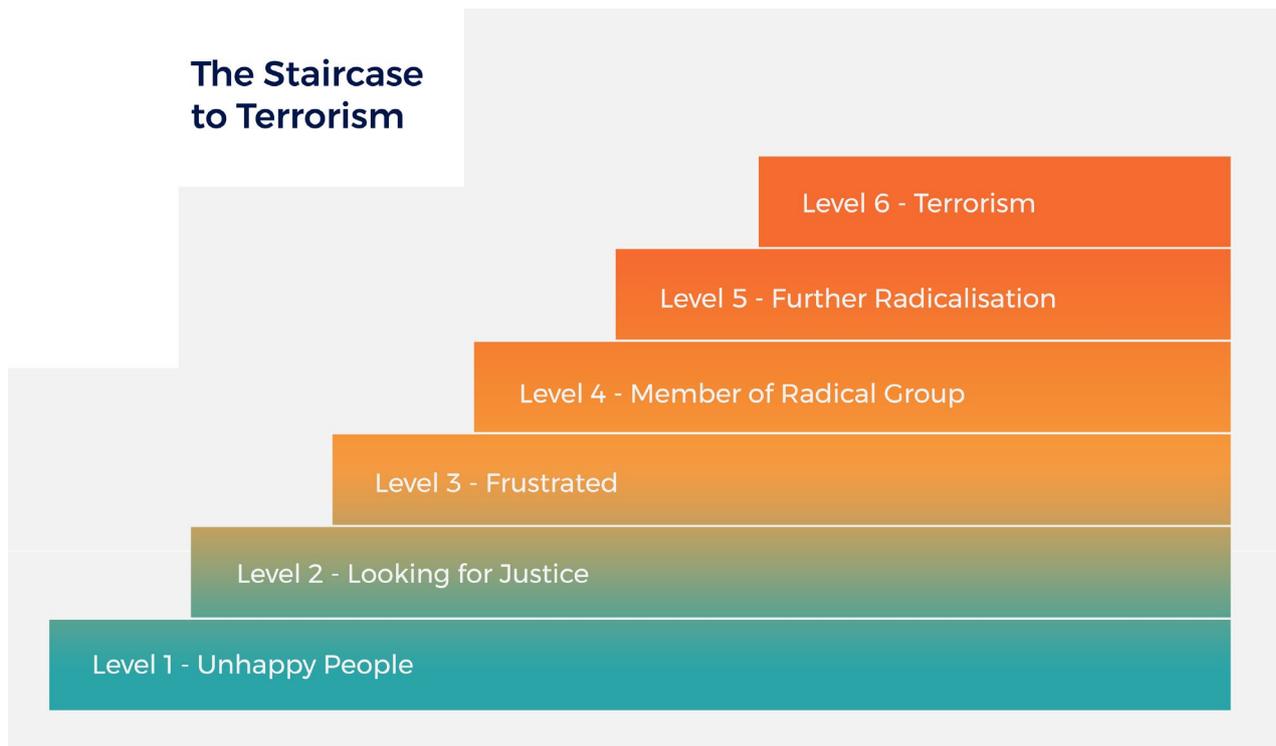
The presence of listed indicators with an employee may lead to caution and further monitoring. The following list is not an exhaustive one of possible indicators.

Employees who are in the process of radicalisation may stand out because of subtle or massive changes to their personality/identity:

- Change of name, aliases;
- Clothing style changes;
- Change in physical appearance (beards, facial hair, no hair, ... );
- Wearing or adding certain (hidden) tattoos, badges, (religious, "gang", extremist or political) symbols;
- Possession, download, of propaganda material;
- Participation in closed (religious, extremist or political) meetings;
- Glorification of violence, martyrdom or other extremist behaviour;
- Travel or stays in war/conflict zones;
- Participation in radical or extremist demonstrations;
- Use of radical, specific or other extremist terminology;
- Social isolation or change of peers.

When a company is in doubt about a potential radicalisation case, they should contact law enforcement immediately.

## The Staircase to Terrorism



# 2.4

## Addressing the Insider Threat

Addressing the Insider Threat requires a strong security culture:

- Establish and enforce security policies;
- Identify critical assets and assess their vulnerabilities;
- Establish reporting procedures;
- Develop response and investigation plans;
- Implement access controls;
- Document employee acknowledgement of “Rules of Behaviour”;
- Establish alerts for abnormal activity;
- Train the workforce;
- Focus on high risk employees;
- Develop adequate termination procedures.

Below are some of the additional of the additional security actions, which are strongly recommended to be implemented:

- Travel briefings and debriefings;
- Financial disclosure program<sup>19</sup>;
- Background investigation during the pre-employment check with periodic re-investigations. (“Infinity screening”);
- Non-disclosure agreements;
- Non-compete agreements;
- Conduct network and user activity monitoring;
- Collect and analyse employee data.

Note that Insiders will always try to use privacy protections (laws) to their advantage.

<sup>19</sup> EU/local laws need to be carefully checked whether this can be performed in the country of application.

# 2.5

## Insider Threat Mitigation

In order to have an effective Insider Threat mitigation program, companies need to address employees' behaviour.

Insider Threat case(s) may look more like a social work case than a criminal investigation. Typical mitigation actions to address behaviour:

- Disciplinary action;
- Law Enforcement action;
- Human Resources action (reprimand, suspension, performance rating, firing);
- Employee Assistance Program (EAP) referral.

Insider Threat mitigation is one of the most complex challenges facing the transportation industry and operators of critical infrastructure, given the diverse set of stakeholders and large number of areas in need of protection.

For example: airports represent a complex ecosystem of public and private stakeholders, each of which impacts an airport's ability to mitigate Insider Threats. There is a number of areas to consider, when assessing the risk posed by Insiders to an airport as shown in the table on page 56.

There is a large number of Airport cybersecurity threat vectors, and the list shown focuses on airport systems, but these are equally valid for many other transport modes and critical infrastructure buildings:

- Access Control;
- Perimeter Intrusion Systems;
- Credentialing Systems;
- Document Management;
- CAD, Blueprints;
- Radar Systems;
- Ground Radar;
- Airport Business Systems FIDS (Flight Information Display System);
- Network enabled Baggage Systems;
- Wired & wireless network systems;
- HVAC (Heating, Ventilation & Air Conditioning);
- Facility Management;
- Utilities;
- SCADA (Supervisory Control and Data Acquisition - industrial control systems);
- e-Enabled Aircraft systems supported by airport network services.

Some of the best practices of Insider Threat mitigation can be listed as follows:

- Consider threats from Insiders and business partners in enterprise-wide risk assessments;

### Example within the aviation ecosystem

Airport Ecosystem & Target Environment - Insider Threat Mitigation

Insider Threat mitigation is one of the most complex challenges facing the aviation industry, given the diverse set of stakeholders and large number of areas in need of protection.



#### Airport Employees

Individuals employed with organisations at an airport who have authorised access to secure areas.



#### Airport Operators

Commercial and Governmental organisations responsible for operating and managing airports.



#### Cargo Airlines

Airlines operating full freighter/cargo aircraft and related facilities.



#### GHA/GSP Ground Handling/Service & FBO Fixed Base Operators

Companies that have access to airport facilities including secure areas and aircraft.



#### Freight Forwarders

Logistics companies responsible for facilitating and overseeing movement of goods by air.



#### Passenger Airlines

Airline companies operating passenger aircraft and related activities.



#### Security providers

Organisations performing and maintaining security services for airports, airlines, aircraft, passengers, cargo and aviation suppliers.

- Clearly document and consistently enforce policies and controls;
- Incorporate Insider Threat awareness into periodic security training for all employees;
- Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour;
- Anticipate and manage negative issues in the work environment;
- Know your assets;
- Implement strict password and account management policies and practices;
- Enforce separation of duties and least privilege;
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities;
- Institute stringent access controls and monitoring policies on privileged users;
- Institutionalize system change controls;
- Use a log correlation engine or Security Information and Event Management (SIEM) system to log, monitor, and audit employee actions;
- Monitor and control remote access from all end points, including mobile devices;

### Insider Threat Considerations for Airport and Airline Stakeholders

Airport Ecosystem & Target Environment - Insider Threat Mitigation

Insider Threat mitigation is one of the most complex challenges facing the aviation industry, given the diverse set of stakeholders and large number of areas in need of protection.

### Identifying the Risk of Insiders

#### Types of Employees and Access

- Vendors in the terminal (e.g. restaurants, bars).
- Vendors in the sterile area (e.g. duty-free gift stores).
- Airline employees (e.g. check-in, baggage, ramp and gate agents).
- Security personnel, cleaning staff.
- Ground Handlers & GSP, Caterers and FBOs.

#### Risk Posed by Target

- Business Aviation & General Aviation.
- Sterile area(s) & ramp(s) (SRA CPSRA).
- Commercial airlines. (Regional, Medium&Long-Haul)
- Full cargo operators.
- Cargo facility(ies).
- On-airport GSP facilities (e.g. caterers, fuel farm).

### Risk Posed by Targets

#### Airport Badging and Access

- Number and location of perimeter access points.
- Access points controlled by GSP & FBO.
- Accountability of GSP & FBO for badges and customers.
- Escort policies (e.g. for construction, ITC workers).
- Badge audit processes and policies.

#### Employee Monitoring

- CCTV in secure and employee areas.
- Lighting in secure and employee areas.
- Badging data.
- Timesheets.
- Inspection/screening of employees.
- Airport security/law enforcement/military patrols.

- Develop a comprehensive employee termination procedure;
- Implement secure backup and recovery processes;
- Develop a formalized Insider Threat program;
- Establish a baseline of normal network device behaviour;
- Be especially vigilant regarding social media;
- Close the doors to unauthorized data exfiltration.

### Insider Threat Challenges at Airports

Airports face a number of unique challenges that can complicate efforts to establish an industry leading Insider Threat mitigation capability.

#### Issues

- Airport Restricted Area badge holders are often employed by many companies beyond just the airport.
- There is an extremely large and diverse number of businesses operating within the airport ecosystem, typically the larger the airport, the more the number of actors in its theatre.
- Large number of doors, gates, and other access points.
- Many Ground Service Suppliers (GSP), Ground Handling Agencies (GHA) and Fixed Base Operators (FBO) pay widely differing attention to security.
- Some EU FBO's are responsible for their own keys, access cards, etc.
- Many airports are constantly undertaking numerous construction activities.

#### Challenges

##### Data Collection and Correlation:

Since no one entity "owns" the data on its employees, it requires extensive coordination between employers in order to collect comprehensive data sets on employees to include in analytics engine.

##### Policy Compliance:

While airports can set policies, the large number of independent businesses can make it difficult to ensure compliance.

##### Access Control:

Difficult to control access given the large number of doors, gates, etc., many of which are managed by third-parties (e.g. GHA's, GSP's, FBOs).

##### Background Checks:

In many instances, contractors and construction workers gain access via escort rather than undergoing background checks.

##### Pre-Employment Checks:

Hardly enforced, despite guidance material available (e.g. the United Kingdom's CPNI - Centre for the Protection of National Infrastructure).

# 2.6

## Methodology

### How do you start an Insider Threat program?

Perform your initial Insider Threat subject research:

- There are ample free-of-charge resources available. However, note that most are from the USA and need to be evaluated for use/adaptation in the European Union;
- There have been quite a lot of good books<sup>20</sup> on the subject published these last few years;
- Some EU national/regional governments are quite pro-active and publish “how-to” guides and/or “best practices” guides on either aspects of the Insider Threat, or others take a holistic view and provide comprehensive guidance;
- Insurers, ICT service providers, finance consultants, chambers of commerce, trade associations, law enforcement entities and management consultancy firms regularly publish “white papers” on the subject for consultation, or offer other means of advice. Many also organise conferences, workshops, training sessions on the subject, which can help gain deeper insight and provide solutions or help companies on the way;
- Larger companies could also consult with their board for current/past experience at other companies or connect with industry peers for more information and/or help;
- Some trade unions also provide guidance and advice.

*20 Most on-line booksellers carry a selection of English books on the “Insider Threat” subject.*

# 2.7

---

## Insider Threat Program Functions

Building an InTP requires a methodology which is divided in three distinct phases:

- Initiation;
- Development;
- Implementation.

Each phase is agnostic and designed to be applied to the creation of any of the eco-system components, individually or collectively. Each step should be organised around five key concepts:

- Goal: the desired objective of the step;
- Participants: who should be responsible for completing the objective;
- Timeframe: the time allotted for each step;
- Justification: explains why the step is necessary;
- How to accomplish: describes the essential actions to complete the step.



Virtual Indicators	Non-Virtual Indicators	Contextual Indicators
<p><b>Network &amp; User Activity/Behaviour Monitoring</b></p> <ul style="list-style-type: none"> <li>• Data Exfiltration Monitoring</li> <li>• Company Network Activity Monitoring</li> </ul>	<p><b>Staff behaviour monitoring displayed outside ICT environment</b></p> <ul style="list-style-type: none"> <li>• Staff Access Rights, Attributes and Behaviours</li> </ul> <p><b>Staff Access Rights, Attributes and Behaviours</b></p> <ul style="list-style-type: none"> <li>• Access levels (regularities)</li> <li>• Security clearance(s) (refused, expired)</li> <li>• Privilege user rights.</li> </ul>	<p><b>Setting &amp; monitoring the level of access and individual roles within the company.</b></p> <ul style="list-style-type: none"> <li>• Compliance Cases Management</li> <li>• Time &amp; Expenses Management &amp; Audit</li> <li>• Human Resource Management (HRM)</li> <li>• External Data Handling</li> <li>• Physical Security Measures</li> </ul> <p><b>Compliance Cases Management</b></p> <ul style="list-style-type: none"> <li>• Audit remediation progress.</li> <li>• Not complying with company training requirements.</li> <li>• Company policy/procedure violations (e.g. avoiding background checks, incomplete credentials, etc.).</li> </ul> <p><b>Time &amp; Expenses Management &amp; Audit</b></p> <ul style="list-style-type: none"> <li>• Financial irregularities (e.g. expense violations)</li> <li>• Time entry violations (unusual hours activity).</li> </ul> <p><b>Human Resource Management (HRM)</b></p> <ul style="list-style-type: none"> <li>• Declining performance scores (assessment linked).</li> <li>• Notice of resignation or termination.</li> <li>• Disciplinary measures: verbal/written warnings, demotion, etc.</li> </ul> <p><b>External Data Handling</b></p> <ul style="list-style-type: none"> <li>• Social media issues/violations (questionable, inappropriate, illegal).</li> <li>• Financial issues (excessive lifestyle, unexplained behaviour).</li> <li>• Incomplete pre-employment checks, lack of documentation, falsifications. Unexplained gaps in CV.</li> <li>• Foreign contacts/travel (conflict zones).</li> </ul> <p><b>Physical Security Measures</b></p> <ul style="list-style-type: none"> <li>• Physical access request denials.</li> <li>• Physical access anomalies.</li> <li>• Bypassing controls.</li> </ul>
<p style="text-align: center;"><b>Potential Risk Indicators</b></p> <p style="text-align: center;">Correlating PRIs drives real-time threat detection and the identification of emerging Insider Threats.</p>		

# 2.8

## Insider Threat Program Functions

The graph on page 64 displays the standard 10 key steps in building an effective InTP Insider Threat program.

Before starting with the InTP 10 key steps, consider first a set of quick wins that can be achieved easily:

- Obtain buy-in from the following critical organisation elements:
  - Senior Company Leadership;
  - Legal Counsel;
  - Human Resources & HR Business Partners;
  - Facility & Physical & Operational Security Management;
  - Privacy Officer (DPO as per EU GDPR);
  - Cyber- & ICT-Security.
- Identify and prioritize the organisational assets that need protection, with the understanding that not everything can be protected/defended with equal effect. (Apply Pareto's "80/20 rule"<sup>21</sup>);

<sup>21</sup> The 80/20 rule suggests focusing on the few, larger items that will generate the most significant results.

- Follow the, previously shown, 10 steps process for creating and managing a formal Insider Threat Program (InTP);
- Ensure that Legal Counsel reviews and approves the appropriate legal and regulatory frameworks of the program;
- Create an oversight program, assign responsibilities, disseminate information about reporting processes and ensure that the InTP program is implemented equitably and in compliance with all local national laws and regulations.



## 2.8.1 Program Building Key Steps

It is important to gain senior leadership/ board endorsement followed by developing policies that have absolute buy-in from key stakeholders whilst taking into account the local organisational culture.

Develop repeatable processes to achieve consistency in how Insider Threats are monitored and mitigated. Insider Threat programs are not only about cyber-crime/terrorism.

Think about all your critical assets, especially about those that, if compromised, would impact the business the most. Use analytics to strengthen the program backbone but remember implementing an analytical platform does not create an Insider Threat detection program in and of itself.



Coordinate early and often with legal counsel and company workers representation (trade unions) to address privacy, data, employee protection and cross-border data transfer concerns. Perform regular screening of employees (own and temp-agency), contractors and vendors, especially employees who hold high-risk positions and/or have access to critical assets.

Implement clearly defined consequence management processes so that all incidents are handled following consistent standards, involving the right stakeholders.

Create training curricula to generate awareness about Insider Threats and their related risks.

Leverage information security and corporate security programs, coupled with information governance, to identify and understand critical assets.

## 2.8.2 Getting Started

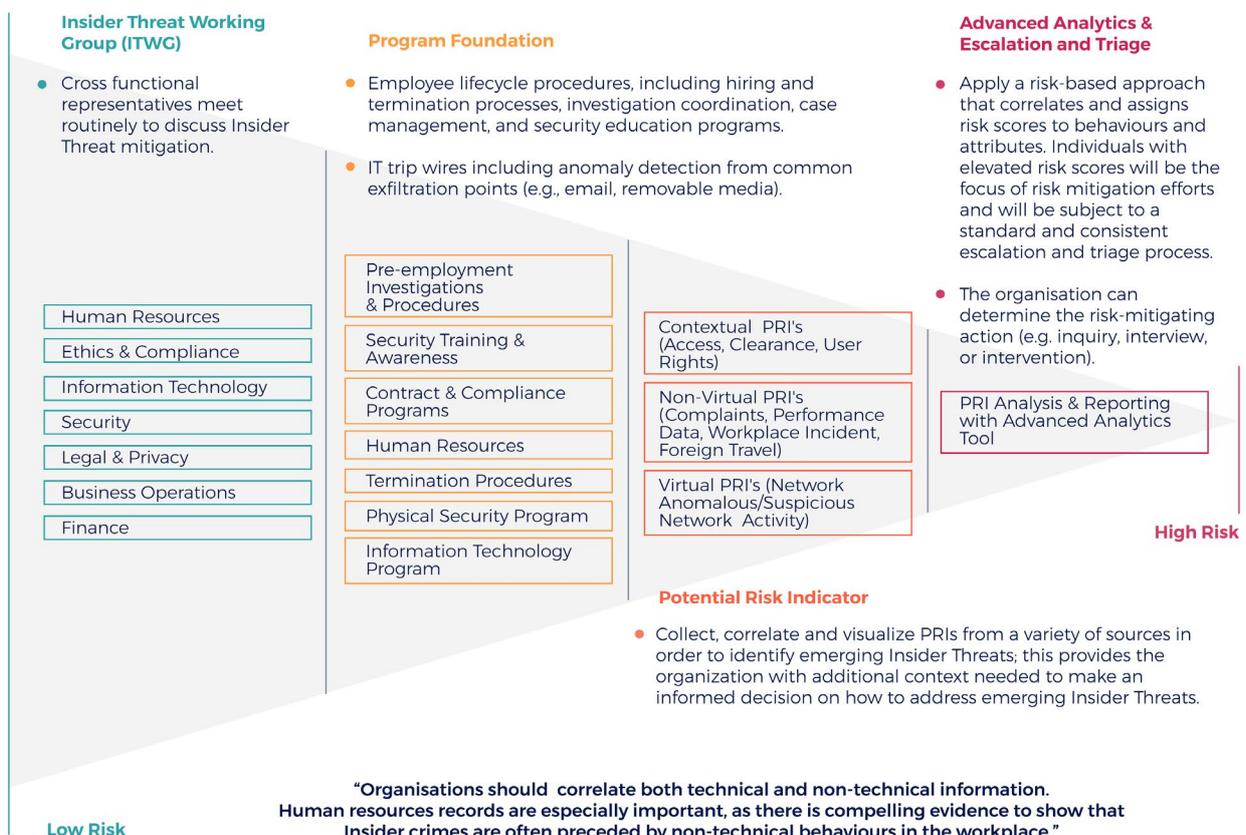
Identify the company InTP team members, who understand and can contribute to the building of the InTP program. Define who will be responsible for:

- Reporting to internal sponsors (and Government Agency/ies if applicable);
- Scheduled meetings;
- Drafting the InTP plan and program;
- Budget approvals.

Conduct risk assessments per department. Use the “Top 10 Questions<sup>22</sup>” listed earlier and revisit current procedures, like:

- Termination procedures;
- Data handling, data access and user rights;
- Violation policies;
- Acceptable use policies (e.g.: BYOD policy, etc.).

Review current security training and make provisions for Insider Threat Awareness Training. Document and disseminate the Insider Threat program expectations to all employees and ensure staff understand Insider Threat reporting whilst making it easy for staff to report confidentially.



22 Chapter 3.4: “Top 10 Question List to Check Basic Due Diligence” (page 87)

## 2.8.3

# Reporting

The importance of reporting should be stressed, and therefore employees should be encouraged to report. Only when reporting takes place will you know that a problem might exist.

- Provide robust confidential (anonymous) means of reporting;
- Employees holding security clearance are required to report adverse information, including potential threats;
- Have employees trust their instincts: if they see something, they should say/report something!
- It should be policy that it is better to report something that turns out to be nothing, than to not report something, which later turns out to be a serious security issue;
- Make sure that all employees know and understand the threat indicators. Conduct regular awareness training and update the course regularly;
- Ensure that every manager/supervisor knows their staff and therefore will recognize concerning behaviours as potential indicators;
- Pay close attention at termination(s);
- Monitor all facility ingress and egress points. (Both for ICT systems and physical security!);

- Baseline normal activity and keep a sharp lookout for any anomalies;
- Work together across the organisation;
- Educate employees regarding potential recruitment.

## 2.8.4

# Identification of Stakeholders

Many companies often don't identify the right stakeholders.

Many of the components needed for an effective Insider Threat Program are already available within an organisation:

- Senior & Middle Management;
- Legal/General Counsel;
- Human Resources;
- Personnel, Corporate, Facilities Security;
- Information & Communication Technology (ICT);
- Incident Response (ERP);
- Contracting;
- Finance & Purchasing.

## 2.8.5

# Communication with Stakeholders

During the course of the InTP program creation and start-up, it is paramount that timely and precise communication with all stakeholders is performed.

### **Internal Stakeholders:**

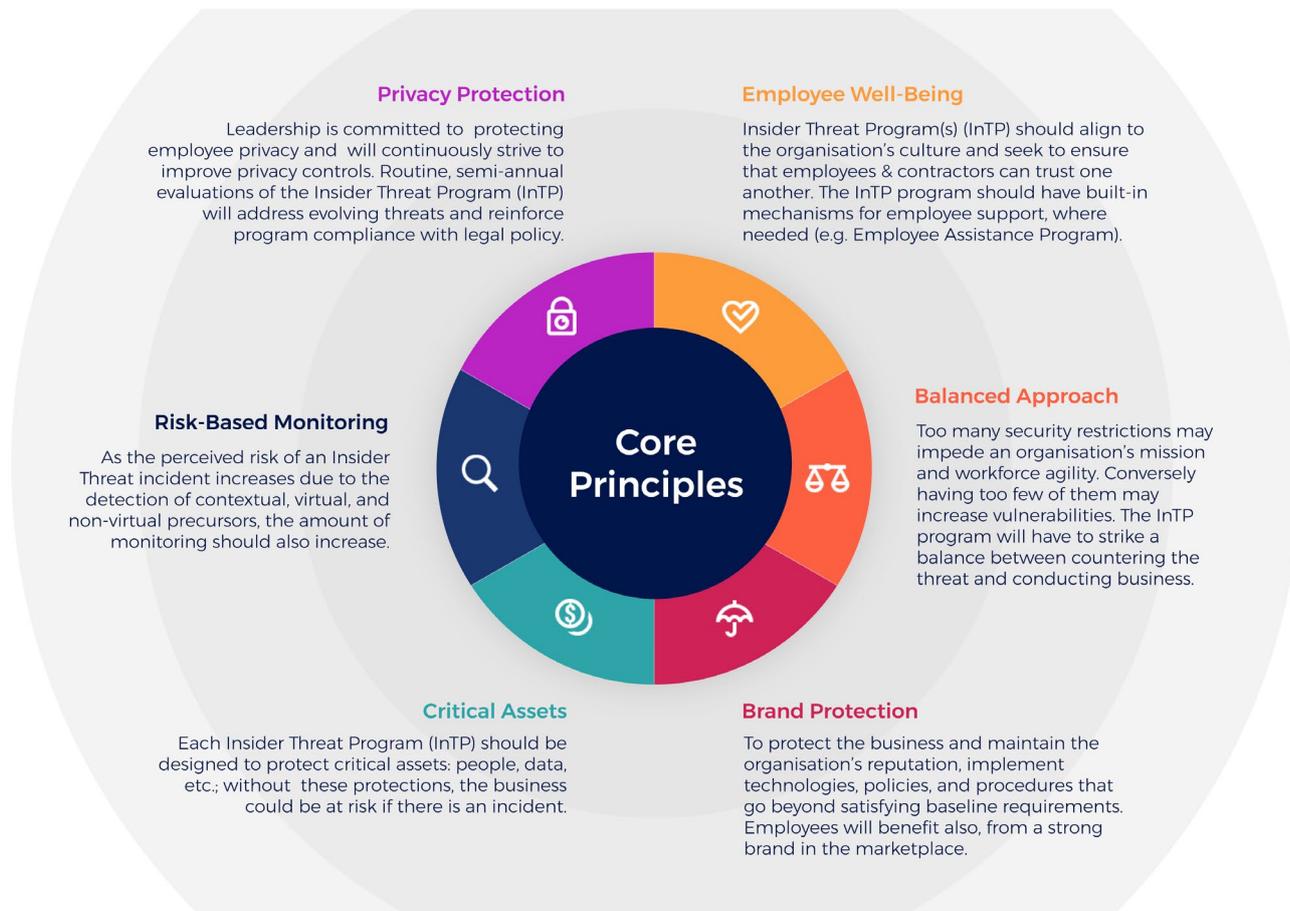
- Business Operations;
- Oversight;
- Board of Directors;
- Unions.

### **External Stakeholders:**

- Law Enforcement agency/ies;
- Regulatory agencies;
- Suppliers & Supply Chain;
- Customers;
- Subcontractors (e.g. Interim Agencies, ITC, etc.).

Companies should create a dedicated Incident Response Team with an Incident Communications Team and generate user alerts (particularly useful when triggered by any kind of suspicious behaviour, so users learn to know what is and what isn't good practice).

Fighting against Insider Threat is a multidisciplinary company challenge, not only ICT driven! The ICT department cannot address the Insider Threat completely by itself. People unfortunately tend to think that the ICT department is solely responsible for all computer security issues.



There are many more internal stakeholders:

- **Legal:** Are policies in place?  
Are they realistic? Does the legal department support ICT practices?
- **HRM:** Who is coming and going?  
Who has workplace issues?  
Are there soft solutions?
- **ICT:** Is the privacy of end users adequately protected? (GDPR)

The most important part of Insider Threat risk mitigation is breaking

down the silos and establishing communication with all relevant departments within the organisation. A question, which must be repeated again and again during the InTP program creation, introduction and operation is:

- What impact on workplace harmony are policies, monitoring, and enforcement having, and is the company applying policies consistently?

## 2.8.6

# Workforce Consent

Too many companies that have introduced Insider Threat Programs don't get their employees' consent to the following program functions, which touch the workforce private sphere:

- Credit Check;
- Background Check (Checking databases);
- Rules of Behaviour;
- Login Banners<sup>23</sup>.

For continuous employee evaluation (infinity vetting), having a statement in individual working contracts or employee handbooks, explicitly stating that this is a "continuous process", is essential<sup>24</sup>. Privacy considerations and GDPR rules must always be taken into account, and especially:

- Address Privacy Considerations in Employee Communications;
- Coordination with Corporate Privacy General Counsel;
- National and International Privacy Laws;
- Restricted Access to Data;
- "Red Team<sup>25</sup>" Detection Systems.

<sup>23</sup> Login banners provide a definitive warning to any possible intruders that may want to access your system that certain types of activity are illegal, but at the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use of the computerized or networked environment(s).

<sup>24</sup> Where allowed under EU and national laws.

<sup>25</sup> "Red Team" A process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access.

## 2.8.7

# ICT Usage Information

Many companies don't have the right (ICT usage) information or policies/procedures on a wide array of devices:

- Computer activity (Event Logs);
- USB, CD/DVD usage rights;
- Network folder & file access rights;
- E-Mails being sent & received (including attachments);
- Databases (access, queries, exports);
- Software application usage, custom software applications;
- Remote access / VPN access;
- Print usage monitoring;
- Network bandwidth analysis;
- Internet usage (websites visited, uploads, downloads, searches), web chat / messenger;
- Copy machine usage;
- Multi-function printer usage (copier, scanner, fax);
- Fax machine usage (where still relevant).

It is strongly recommended to use a comprehensive Insider Threat management solution, generally called Enterprise Monitoring Tools from vendors like Ekran, Netwrix, Veriaton, ObserveIT, One Identity, Resolver, etc.

These systems offer a wide variety of solutions and possibilities to create a holistic view of your ICT network usage and detect data security risks, and anomalous user behaviour, before it would result in a data breach harming the company.

# 2.9

## Communications Strategy

Arguments in favour of providing an Insider Threat awareness training:

- Companies base their threat assessment on past occurrences in the industry;
- The company wants to protect its employees, customers and assets against harm, Insider Threats especially, as the damage they can inflict is considerable, and, many times, without the company knowing it, or too late;
- The company places this in a general security (system) review and wants to close as many threat gaps as possible;
- Employees should want to be sure that their (future) colleagues do not pose a threat, as the damage from an Insider Threat could seriously hurt the company, affecting each employee's position within the company;
- Unions (social partners), insurers, shareholders, etc. should be partners in protecting the company against threats, especially Insiders, as they understand that an attack, successful or not, will create a loss of confidence with serious financial consequences.

The InTP Insider Threat Program message must carry only positive statements, while discussing only negative behaviour, which should be detected.

It is imperative that the following messages are used to describe the goal of the InTP:

- Absolute transparency and fairness in purpose and objective;
- The communication will adhere to corporate values;
- Communication in a language easy to understand;
- **No** profiling;
- Unions involved in every step of the way;
- Positive message: the **PROTECTION** of self, colleagues, customers & company (assets);
- Help prevent harm done to self, colleagues, customers & company (assets);
- The keyword is: **PROTECTION**.

**Help2Protect**

# 2.10

## Insider Threat Training

### 2.10.1 Insider Threat Awareness Training

Awareness plays an extremely important role in the InTP Program scope. It is imperative that companies consider what follows:

- The Insider Threat Awareness program is not an isolated program and fits in the general security system/program(s) that the company has developed, or is going to develop in the future;
- The InTP Awareness module is but one part of a chain of company security measures, and we all should know the saying: “the chain is as strong as its weakest link”;
- The InTP Awareness module is to be mandatory for all, including all company (senior) executives and/or board of directors;
- The InTP Awareness module is performed under the express authorisation of the Chief Executive in a “lead by example approach”;
- Not all the InTP measures are to be disseminated to all employees in the Awareness module, certain elements obviously are on a “need-to-know” basis and should be carefully reviewed and evaluated;
- The InTP Awareness module and the entire company security program/system should be under constant review and developed as threats evolve;
- The InTP Awareness module will avoid the use of difficult terms/jargon and be kept as “Simple as Possible”.

### Policy Evaluation Criteria



#### Exists

Policy exists or the provisions of the policy are present in another policy.



#### Routinely-Acknowledged

Staff are required to re-acknowledge the policy at regular intervals beyond the initial acknowledgement.



#### Enforced

Compliance with the policy is actively tracked and the organization takes steps to confirm compliance.



#### Centrally-Located

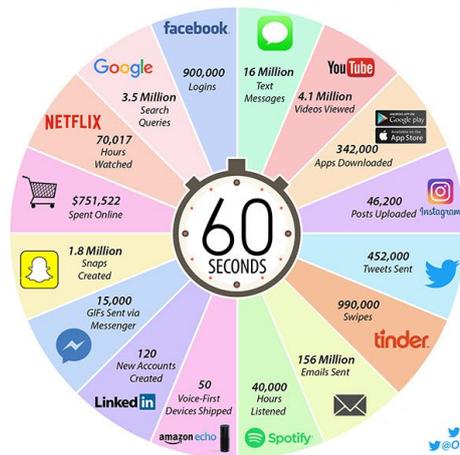
The policy is directly available to employees and easily accessible.

### Insider Threat Mitigation Policies

Non-Disclosure Agreements	Password Policy	Removable Media	Social Media Policy	Separation of Duties
Mobile Device BYOD	Log Management	Least Privilege	Acceptable Use Agreement	Account Management
Cloud Computing	Employee Assistance Program (EAP)	Data Transfer	Information Classification	Intellectual Property

While developing strong policies is an important first step in Insider Threat mitigation, consistent enforcement is critical to the program success.

## 2017 This Is What Happens In An Internet Minute



Created By:  
@LoriLewis  
@OfficiallyChadd

## 2018 This Is What Happens In An Internet Minute



Below are some ideas regarding the scope of the InTP Awareness module:

- The InTP awareness module will keep the theoretical model information as limited as possible, but some basic Insider Threat types must be explained, as most will only associate Insider Threats with terrorism in the current climate. (However, crime is an equally important driver together with terrorism);
- Dedicate separate time to cybercrime<sup>26</sup> - which is spreading at unprecedented rates;
- Companies should discuss the different Insider Threat Indicators in detail, and the basics of the pathway/ evolution from “idea to action” that an Insider Threat actor usually follows;
- Also, these topics are worth mentioning in follow-up sessions: disgruntled employees (seeking revenge), divided loyalties, habit of security violations, access seekers, personal stress effects, mental instability, extravagant lifestyle & finance issues, foreign contacts, company technology misuses, allegiance/support of terrorist/state actors, testing security procedures & boundaries, violent behaviour, family ties, ego and self-worth issues & personality, radical faith or politics, etc.

<sup>26</sup> A good source on many cybercrime matters is the website of Symantec: <https://www.symantec.com/security-center>.

## 2.10.2

# Insider Threat Program Building Training

Providing the right training will be essential:

- The Insider Threat Program Manager, Insider Threat Analyst, Insider Threat Program Support Personnel positions require a specialized skill set and most likely will require additional training;
- Insider Threat Program concepts must be developed in depth and procedures for conducting “Insider Threat Incident” response actions must be subject to training and exercises;
- There are EU and national laws and regulations on gathering, integrating, retaining, safeguarding and using records and data. The consequences of misuse of such information must be taken into account (especially with EU GDPR laws which entered in force in May 2018);
- Legal, civil liberties and privacy policies must be adhered to.



# 03.

---

## Best Practices

The InTP should be an important element of a company's security program and should seamlessly tie in with all other security measures in the company:

- Physical security;
- ICT security;
- Operational security;
- HR security.

Addressing the Insider Threat is a team approach:

- The Insider Threat is not just a security or counterintelligence problem;
- The Insider Threat team should include Security, Human Resources, Health Programs, Internal Affairs, Legal & Counterintelligence departments;
- Since Insiders are hard to find, investigators need to look for clues throughout the organisation;
- Information sharing is key as a clue in one department may not be known in another department;
- Mitigating the (Insider) Threat may require action from across the entire organisation;

All employees, including (top) management, should follow basic security training which includes Insider Threat and Insider Threat Awareness as a major component.

Also note that Security Training, and Insider Threat training in particular, should ideally be planned both as "initial" with (yearly) "recurrent" training.

# 3.1

## Obstacles

Some of the most cited obstacles to a successful InTP implementation are:

- Lack of Executive Management (C-Suite) support;
- Lack of understanding of Insider Threat(s);
- Resistance from staff and/or their trade union representatives. InTP Insider Threat program could be viewed as “Big Brother” or be perceived as a “Witch Hunt” (Strongly consider naming the InTP with positive connotations; such as: “asset protection & compliance program”);
- Unions (This may be due to poor communication);
- No dedicated Insider Threat analysts/ investigators;
- Lack of clear policies that define data protection;
- Lack of funding and resources;
- Cultural barriers to implementation;
- Difficulty in obtaining and/or processing data;
- The company feels they are “compliant”; is this really sufficient? (Scope of InTP);
- Possible lack of understanding of the threat and its possible magnitude;
- Difficulty to secure funding for InTP Program;

- Possible legal resistance and/or stakeholder resistance;
- Employees reluctant to report due to lack of “just culture” or anonymous reporting possibilities;
- Stakeholder(s) reluctant to share vulnerabilities with Insider Threat program manager & working group that identify security weaknesses in other security disciplines & departments;
- Underestimation of possible cultural barriers to implementation.

Some other obstacles or perceptions that should be checked carefully:

- The InTP should fit seamlessly in the general Corporate Culture, has this been considered?
- The company already has established “Pre-Employment Checks”; is this sufficient? (Critical review of existing program is required to determine effectiveness);
- The company performs Computer User Activity Monitoring; is this sufficient? (Critical review of existing program is required to determine effectiveness).

# 3.2

## What others have done

Companies need to focus on Insider Threat deterrence, detection and mitigation within their security framework. This should include comprehensive measures (where possible) to secure and monitor those critical assets that absolutely need to be protected. Cyber protection measures need to capture any interaction with data sources (especially trade secrets, IP or sensitive materials).

It pays to reduce the incentives (read: access) for Insider actions and prevent Insider Threat attacks before they even start. This will also reduce/eliminate the resources to search for those willingly or unwillingly aiming to commit Insider Threat crimes.

Please study these Ernst & Young takeaways from their InTP consulting projects (2017):

- Corporate proprietary information and intellectual property are hot targets!
- Reporting indicates steady upward trend in targeting;
- Threat is real, formidable and aggressive;
- Current business environment exposes organisations to more vulnerabilities;
- Strong partnerships are key (internal and external);
- Automated analysis capability is essential for any large organisation;

- Data loss prevention tool does not equal Insider Threat detection capability;
- Program transparency: mitigates concern, promotes deterrence, garners program support;
- Law enforcement agency can request to allow the (criminal) conduct to continue (weighing liability and reputational concerns) for investigation purposes;
- System monitoring considerations;
- Addressing the employee's own devices;
- Issues related to remote access;
- Disclosure considerations where data is lost (GDPR!);
- Legal challenges involving an employee who exceeds authorized system access.
- Functional area partnerships are key to program success;
- Counter-intelligence team<sup>27</sup>, security, HR, ethics, legal, communications, operations, should all work together;
- Continuous coordination with Legal/General Counsel is required;
- Internal audit engagement (where possible);
- A well thought-through communication plan is indispensable;
- Suicide and workplace violence prevention (part of the general security policy) should be tied into the security program. (e.g.: in France: Risques Psychosociaux<sup>28</sup>/RPS);
- Break down the company's "business as usual" mindset.

Also note some of the hard lessons learned by companies that have started and initiated Insider Threat Programs:

- Organisational leadership buy-in is NOT "won and done"! Buy-in needs to be earned along the entire program (introduction) lifecycle;
- The development of an Insider Threat Program is a long process; expect funding to be made available incrementally;

<sup>27</sup> Counter-intelligence teams are generally only found in large corporations.

<sup>28</sup> Psychosocial risks at work are defined as "the probability that one or more workers will suffer psychological damage which may also be accompanied by physical damage as a result of exposure to components of work organisation, work content, working conditions, working conditions, living conditions at work and interpersonal relations at work, on which the employer has an impact and which objectively involve a danger".

# 3.3

## Some Legal Considerations

There is increasing public recognition of the need for companies to adopt practices that are both legal and ethical. This applies not only to recruitment procedures but also to security program (elements) and InTP programs/procedures.

Some examples:

- Recruitment processes are being increasingly influenced by the explosive development of social media. In the UK, 2 in 5 employers say they look at candidates' online activity or profiles in order to inform recruitment decisions. There may be legal hurdles<sup>29</sup> in doing so, and organisations need to check the legal framework before doing so;
- The continued trend towards outsourcing the vetting process means that it may be unclear which organisation is responsible for conducting pre-employment checks, and under GDPR organisations processing or storing data on behalf of others fall under this scope;
- Checking applicants' credentials and references through following up with former employer references may be of limited value since many of these companies have become very reluctant to make negative comments for fear of any legal challenge;
- Poor hiring practices may be unfair, or perceived as such, to individual applicants, for example by discriminating against members of particular groups or by giving undue weight to inaccurate or misleading information (found online).

<sup>29</sup> For example, consult:  
<https://www.acoi.ie/2017/07/13/art-29-wp-guidance-22017-on-data-processing-in-the-workplace/>

# 3.4

## Top 10 Question List to Check Basic Due Diligence

To begin, let us present a top 10 question list, which any company should ask itself before starting to build an InTP Program:

- What are our critical assets, i.e. those that, if compromised, would impact the business the most?
- Are those critical assets aligned with our business continuity team's priorities?
- What measures are in place to protect our critical assets? How do we identify Insider and External Threats?
- Who are the potential threat actors that put those critical assets at risk?
- What is the probability of them to effectively act?
- What is the impact if they should act?
- What is the likelihood of them doing (serious) damage?
- How will we respond once a critical threat against a critical asset is detected?
- If we lost sensitive data, how would we respond and minimize risk (GDPR)?

Keep in mind that Insiders will use privacy protections (laws) to their advantage!

# 3.5

## Safe Hiring & Pre-Employment Screening/Vetting (Onboarding)

Personnel security is a system of policies and procedures that seek to manage the risk of people exploiting, or having the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

The person who causes harm to your organisation could be given access to assets for one day a month or every working day, (s)he may be a full-time or part-time permanent member of staff or an individual in attachment or secondment, a contractor, consultant, intern, agency or temporary employee and his/her access may be in a traditional office or site setting, or via a remote working station.

An Osterman Research white paper quotes a US survey published by Biscom in late 2015 found that 87 percent of employees who leave a job take with them data that they created in that job, and 28 percent take data that others had created. Among the majority who took company data with them, 88 percent took corporate presentations and/or strategy documents, 31 percent took customer lists, and 25 percent took intellectual property.

Another study, by Imperva, this time in Beijing and Shanghai (People's Republic of China), came to similar results:

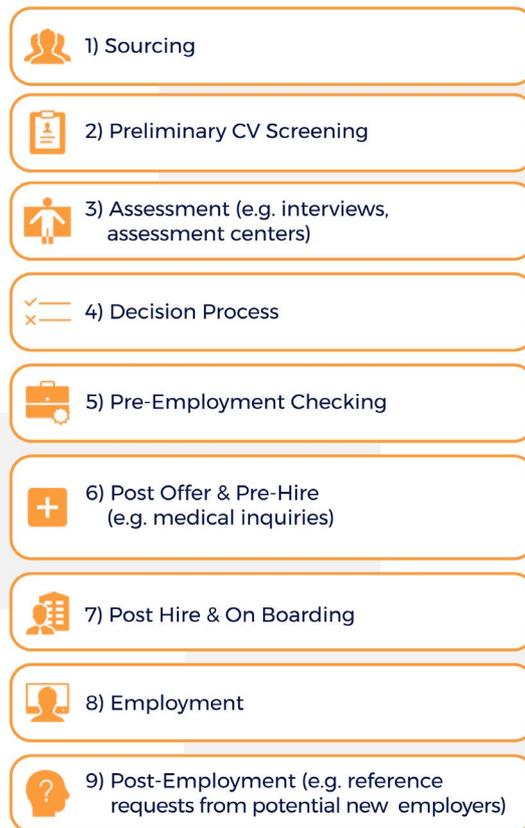
The respondents stated that:

- 62% took data when they left a job<sup>30</sup>;
- 56% admit to internal hacking;
- 70% of employees admit to accessing information they shouldn't have;
- 36% feel they own the data.

<sup>30</sup> <http://www.sonian.com/wp-content/uploads/2017/01/Best-Practices-for-Protecting-Your-Data-When-Employees-Leave-Your-Company-Sonian.pdf>

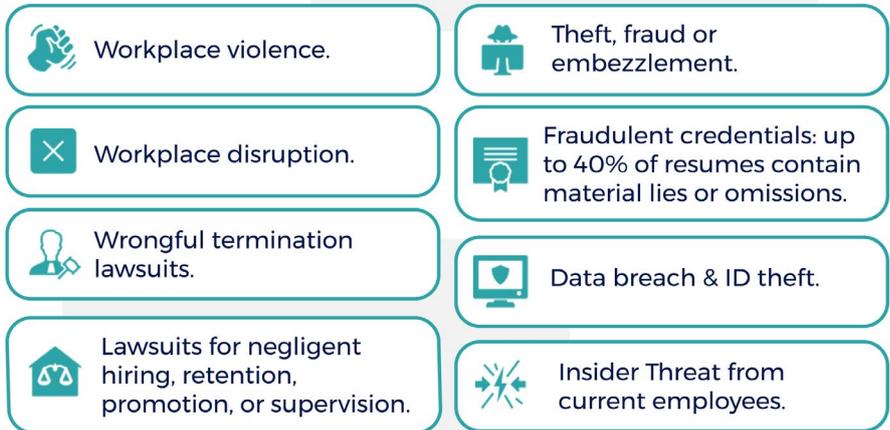
## Safe Hiring - Stages of the recruitment / hiring process

Hiring occurs on a continuum. It is critical to understand different legal obligations depending upon each stage of the hiring process.



## Safe Hiring - Why should we be concerned?

Past criminal conduct raises concern about propensity to repeat criminal behavior - 10% rate of criminal records.



Prevention of potential Insider Threats starts with the onboarding process within any given company. The pre-employment check process is the first security barrier, and when this is not performed or not performed with the required skills and depth, you are opening the door for those candidate Insiders who are exploiting their access to harm your organisation. Conducting pre-employment checks on job applicants should therefore be an integral part of the recruitment process.

However, careless approaches to vetting and pre-employment screening risks employing the wrong people, with resultant damage in terms of increased turnover and costs, and lower morale. They also risk legal challenge, which can undermine an employer's reputation.

In conducting pre-employment checks, employers should aim to:

- Protect the organisation;
- Protect clients and customers;
- Be fair to all candidates;
- Ensure **non-discrimination** and compliance with EU/national data protection laws;
- Rely on fact, not opinion;
- Validate information to be relied on;
- Ensure relevance to the position to be filled;
- See the candidate in full and realistic detail;
- Be transparent and open to candidates about the pre-employment check/vetting process;
- Build a degree of unpredictability in the vetting process.

### Safe Hiring - The Need For A Safe Hiring Program

Identification and prevention of "Bad Hires" and/or (potential) Insider Threats requires an inter-disciplinary approach that can include:



When companies fail to exercise due diligence in their hiring process, and just one “Bad Hire” slips through, the consequences could be:

- Lost customers or business;
- Damage to employee morale;
- Lower employee retention;
- Brand damage/destruction;
- Damage to corporate culture;
- Litigation;
- High profile cases that can have far reaching consequences, especially when mentioned on social media.

It is therefore essential that companies have a “safe hiring” program in one form or another. Companies should reflect about:

- Economic fallout from a “Bad Hire”;
- Replacement cost & damage control;
- Upset present workforce and/or trade union(s);
- Litigation and legal fees;
- Workplace violence fallout (More an Anglo-Saxon issue);
- Shareholder lawsuits (Especially in litigious societies);
- Brand damage.

Note: An organisation that hires someone it either knew or should have known was dangerous, unfit, or unqualified for the work, (“Bad Hires”) can be sued for negligent hiring. This is especially the case in Anglo-Saxon countries.

## Checking CVs/Resumes

Unfortunately, many candidates admit, or have been found out, to having lied on their CV, particularly about their experience, qualifications or salary. Some candidates may submit false documents<sup>31</sup> (diplomas, references, ID documents, etc.). Unfortunately, fake degrees are very frequent, and:

- Fraud can range from false claims about real schools to presenting worthless degrees from “diploma providers”;
- Authentic-looking counterfeit diplomas from most schools in the EU and USA can be found on the internet.

In order to (partially) protect against candidate dishonesty, it is strongly recommended to insert the following phrase<sup>32</sup> on application forms:

*“I declare that the information given in this form and in any accompanying documentation is true to the best of my knowledge and I herewith give my permission for enquiries to be made to confirm qualifications, experience, dates of employment, right to work in the EU (or national country) and for the release by other people or organisations of necessary information to verify the content. I understand my application may be rejected and/or I may be dismissed following appointment if I have given any false or misleading information or have withheld any relevant details.”*

Remember: employees are typically a company’s greatest investment and

largest cost; especially in service provider companies. Every single new hire also represents a (large) potential risk, it is therefore normal that every employer has the obligation to exercise “Due Diligence” in hiring.

Employers, especially in industries with higher risk (aviation/ transportation and critical infrastructure operators), need to be able to vouch for the integrity and honesty of all their employees.

## Candidate Interviews

Most experienced interviewers cannot identify potentially bad hire(s) during the interview and recruitment process. Even though many experienced HRM people believe they can effectively detect liars, they only have a 50% chance, at best.

Some applicants tell their lie(s) so often it comes across naturally - they actually believe their own story/lies. Body language, eyes, voice, etc., are unfortunately not always reliable indicators.

There are a few additional things to look out for during candidate interviews, while keeping any bias out of it. For example: it can be important to recognise logos and symbols when being worn as visible tattoos by applicants.

Remember: what makes a person suspicious, however, is not their skin colour, religion, gender, ethnicity or position in society. It is what they are doing, where they are or how they are behaving.

<sup>31</sup> There are companies specialising in providing fake references against payment: one of these: <http://www.careerexcuse.com> explains how they work online.

<sup>32</sup> The exact legal wording may need to be adapted to local national laws in order to be effective in eventual later litigation.

## Checking Social Media/On-Line

There has been a marked increase in the proportion of employers making use of social media to research candidates' backgrounds. Using a search engine or social media in this way is not necessarily unlawful. However, it is important to balance employers' interests with those of individual applicants, and companies should be cautious about the way in which they approach such searches<sup>33</sup>.

It should be kept in mind that online information may not always be accurate. Companies should allow candidates to respond to any information, which has been obtained through online research. Then, appropriately to the role, companies should consider any mitigating facts or explanation of inaccuracies before withdrawing offers. Furthermore, in order to avoid risk of a legal challenge, companies should make applicants aware at a very early stage that they may conduct such searches.

## Checking Employment References

It is strongly recommended that potential employers contact referees to obtain references before offering a position to a candidate employee. Employers should also contact a candidate's former company for a reference even if no contact is supplied by the candidate.

Some employers may not be willing to provide reference letters because they may be worried about potential lawsuits. In this case, the employer

may only provide the job title and dates of employment for the employee. Finland, Germany, Austria, Switzerland, Hungary and Bulgaria<sup>34</sup> are the only countries in Europe where employees can legally claim an employment reference, including the right to a correct, unambiguous and benevolent appraisal.

The employment reference letter can cover topics such as:

- The employee's tasks and responsibilities;
- The duration of employment or tasks/ responsibilities;
- The position relative to the author of the reference letter;
- The employee's abilities, knowledge, creativity, intelligence;
- The employee's qualifications (foreign languages, special skills);
- The employee's social attitude;
- The employee's interpersonal skills;
- Reason(s) for employment termination;
- The actual recommendation basis itself.

Factual evidence must always be available to support any such statements in a reference.

*33, 34 Information on National law variances must be carefully checked.*

## Data Protection Implications

The implications of the EU GDPR data protection legislation (and national laws) are likely to become much clearer over time. In the meantime, companies should strongly consider applying the following general principles<sup>35</sup> if they wish to access candidates' social media profiles and check employment references supplied by candidates:

## Online Checks

Although online checks of candidates by potential employers can yield some results, it has in the last few years become a lot like looking for a needle in a digital haystack. How can potential employers know what is relevant and who the information belongs/relates to?

Online checks require an "investigative" review and screening large numbers can be expensive, when done manually, by trained professionals or organisations.

There is an emergence of software tools promising fast results, at considerable cost, but they are in essence just looking for key words and the presented results are going to be hit or miss, lacking any nuance(s).

The manual online search by the company HR/Security department is also becoming less useful as more applicants are aware of the "danger" and either keep "off the web" or use privacy protection settings to secure access to their social media accounts<sup>36</sup>.

If on-line checks are to be performed, these issues should be carefully observed:

- Respect the same restrictions that apply to offline checks (for example interviews) in relation to discrimination;
- Take reasonable steps to ensure the accuracy of information accessed online;
- Distinguish between social media for mainly private purposes and social media for mainly professional purposes. Therefore, use of LinkedIn is legitimate but Facebook, Instagram, etc. is questionable;
- Personal data may be accessed insofar as it is relevant to suitability for the (future) role/position and relates to candidates' personal capabilities and skills, education and experience;
- Social media searches should be used to look for specific information and not as a general trawling/snooping exercise;
- Social media searches should be carried out as late in the recruitment process as reasonably practical;
- Applicants should be informed at the outset if online sources may be used to collect information about them;
- Information generally available online (for example through Bing or Google) can be used;
- However, employers should collect no more personal information than is needed and should not collect information that is irrelevant or excessive;

<sup>35</sup> Based on the UK's CIPD Pre-Employment-Check best practices,

<https://www.cipd.co.uk/knowledge/fundamentals/emp-law/recruitment/pre-employment-checks-factsheet>

<sup>36</sup> Counter-intelligence teams are generally only found in large corporations.

- Applicants should be given an opportunity to respond to material findings from online searches, where the findings form part of the decision-making process;
- Personal data collected during the recruitment process, where the applicant was not hired, should not be kept for more than the period allowed under EU GDPR laws;
- Employers should develop a clear policy towards the use of social media for recruitment purposes, in consultation with employees or their representatives.

Potential employers must weigh the benefit of obtaining information early (pre-hire) against the legal risks (mainly discrimination):

- Have documented training in discrimination (for HR/recruiting staff);
- Establish precise standard practices to show hiring decisions are made on an objective basis;
- Perform social media checks behind an “ethics wall”, a neutral company employee (or outsourced) who does not make final hiring decisions, who filters out material using described standardized procedures, and who only provides job-related data to the final decision maker (preferably after there has been an employment offer);
- Do not let the key decision maker view unfiltered internet/social media data;
- Consider showing negative material to the respective applicant(s) first.

## Employment Reference Checks

- Employers should ensure that references they supply are true, accurate and fair in substance;
- References should offer facts, not opinions;
- References should mention negative issues such as gross misconduct or events giving rise to a disciplinary process in a way which is overall accurate and correct;
- Employers should seek employment references once a job offer has been made, not prior to interview;
- References should be read with a positive mindset, and not seen simply as an opportunity to pick holes or find fault;
- Applicants should be shown phrases which have caused the withdrawal of an offer.

Where potentially damaging information about the candidates' history is referred to in informal telephone conversation, it is good practice that:

- It should not be used as a substitute for the employer making their judgement.
- Such evidence needs to be weighed against evidence from other sources and should be used to support a balanced decision, not as a shortcut to replace the employer's own judgement.

- An individual's circumstances may change, and it will generally be appropriate to check out adverse inferences by raising them with the candidate concerned.

## **Outsourced Employment Agencies Checks**

Where companies consider the use of employment agencies or other intermediaries to help recruit or performing vetting on future employees, they should:

- Choose a reputable agency that takes steps to protect its own reputation;
- Agree what specific pre-employment/vetting checks are necessary and appropriate, ensuring that these are non-discriminatory and relevant to the job(s) to be carried out;
- Specify in a contract or service-level agreement with the supplier what checks are to be carried out;
- Be clear about the respective responsibilities of client and agency, particularly in relation to vetting: if in doubt, duplication is preferable to leaving gaps;
- Be clear about the employment status of staff supplied by an agency: are they employed by the agency or the employer?
- Ensure that appropriate checks are in place for both temporary and permanent staff;
- Be aware of any secondary sub-contractors and establish which agency takes responsibility for the integrity of the vetting process as a whole.

# 3.6

---

## **Temporary Workers, Interim Staff, (Sub-)Contractors & Interns**

Potential employers should apply the same risk-management steps towards contingent workers (temporary workers, interim staff, independent contractors and sub-contractors, interns, job students and consultants) and vendors.

It cannot be repeated often enough, also non-employees (can) have access to computer systems, trade secrets, customer lists, proprietary and/or restricted (classified) information.

Employers can be held liable for contingent workforce under theory of "co-employment."

# 3.7

---

## During Employment

It is recommended that companies practice continuous evaluation processes or “infinity” screening that occurs periodically after hiring. The main argument for this is that employees may commit crime(s) after being hired.

There are some important questions that arise with the introduction/operation of infinity vetting programs:

- Is infinity vetting an effective deterrence?
- What will be the return on investment given the time, cost, and administrative issues involved?
- Legal use: what rules or criteria should be used if a criminal matter is found?
- Employers may consider “random screening” similar to random drug testing, but this may prove to be cumbersome and subject to many legal obstacles.

There are also some very important arguments to be made for infinity vetting/screening:

- Insider embezzlers/criminals often come disguised as your best employees;
- Trust is needed to have the access required to steal or cause harm;
- Background checks are critical, but insufficient as a “sole line of defence”, in the absence of proper internal controls;
- A 2018 US study (ACFE Report to the Nations), confirms that most occupational fraudsters are first-time offenders<sup>37</sup> with clean employment histories and clean criminal histories. (They also tend to be 70% male and in a 36-45 age bracket).

Remember: although pre-employment and infinity vetting are critical to detect and deter fraud, internal controls seem to be the critical tool to prevent unpleasant surprises.

<sup>37</sup> The PDF version of the report can be downloaded here:  
<https://s3-us-west-2.amazonaws.com/acfe-public/2018-report-to-the-nations.pdf>

# 3.8

## Offboarding - Exit Procedures

The company's ex-employees could potentially become the most dangerous Insider Threats. One kind of internal breach that ICT managers may not be aware of is that of ex-employees continuing to access work data systems and networks following the termination of their employment.

Some studies have shown that over a third of people are aware of having been able to access the work network of an old job after they have left. The number that have then actually chosen to use that access and trespassed upon their former employer's network is much lower, at some 9%, but this still constitutes nearly one in ten ex-employees snooping around or stealing data.

A CERT Insider Threat Database review shows that eliminating potential methods of access, after termination, was identified as one of 4 mitigation patterns of Insider Threat sabotage. It strongly suggests that security breaches could have been prevented, detected earlier or responded to more effectively, if the suggested solutions were implemented within the company.

These 4 mitigation patterns identified by CERT are:

- 1:** Constrain remote work outside of normal hours;
- 2:** Increase monitoring within a time window of a negative workplace event,
- 3:** Monitor for Insiders' machines using co-workers' accounts remotely and;
- 4:** Eliminate potential methods of access after termination.

CERT case data also indicate that many Insiders who commit Insider ICT sabotage do so because of prior disgruntlement at work or because of their job termination. This kind of attack should not be possible if effective and comprehensive termination procedures were followed every time, since all of the Insider's system access should be closed off.

The occurrences of ex-employees continuing to access their systems from their former jobs are rampant, and without the proper restrictions or monitoring in place, ICT management could be completely oblivious. This represents a considerable risk, especially given that ex-employees are far more likely to have malicious intentions and a lot less incentive to consider the sensitivity of the business and its data.

Some offboarding best practices are shared here to keep the company protected from departing employees.

**Professional onboarding (hiring):**

pre-employment checks must be performed and screening for the right behaviours and intentions is a must. Once the candidate is hired, the use of an identity management system to record and pattern the employee's access by role is recommended, so companies can quickly and easily turn off all privileges after offboarding. If it's an employee with elevated access, notify your security management in advance to closely monitor their account until all access is completely turned off.

**Clear Company Policies & Compliance Training:**

every new employee's employment contract should include policies regarding the treatment of confidential data while working for, and when leaving, the company. Regular compliance training for all employees, including management, should include updates on handling sensitive information. HRM management should work closely with ICT management on policies and procedures for backing up all company-issued devices (and where applicable all BYOD), as well as wiping them clean.

**Company Security Culture:**

a robust cybersecurity program should be established by the company's ICT department. This allows mapping acceptable behaviour, access and data use against employee types. When anomalous behaviour is detected that doesn't fit with the employee profile (e.g. accessing certain folders/files/ programs), there will be an alert. With basic cyber hygiene, automatic HR workflows can make sure email and online accounts are disabled upon employee departure.

**Offboarding Checklist:**

HR management should collaborate with ICT management in determining employee data accesses. As part of the offboarding process, the exit checklist should include a review of non-disclosure agreements, removal of data and a termination distribution list of who to notify to remove logins and accesses.

**Employee Devices Remote Access:**

an ICT and HRIS<sup>38</sup> system that allows remote access at all times<sup>39</sup> should be implemented. Upon an employment termination or security breach, ICT and HRM can log in to secure the data or remove access immediately. This brings prompt attention to the matter, regardless of where you are located.

**Employee Experience:**

companies obviously should try to hire the best people. Conflict should be managed promptly, thoroughly and with care. Strong personal relationships should be forged and fostered, and company leaders/management should really connect with their team members

as well as leading and managing well. They should conduct thoughtful exit interviews during offboarding and if all that runs smoothly and well, companies will be less likely to need to rely on these best practices regarding offboarding security policies and agreement (but the company should have them anyway).

When an employee departs the company, HR management's role is to conduct the efforts of everyone who needs to be involved (line manager, HRM, payroll, ICT and security management). A departure date must be set and it is time to set the logistical wheels in motion. Remember:

- Communication is key;
- What impact will this employee's departure have on stakeholders, processes and systems?
- What needs to be prepared in advance?
- What needs to happen post-departure, and beyond (reference checks)?
- How will it all come together to protect the company's, employee's and customer's data?

<sup>38</sup> HRIS: human resource information system, also referred to as human resources management system (HRMS), is software that provides a centralized repository of employee master data that the human resource management (HRM) group needs for completing core human resource (HR) processes.

<sup>39</sup> Where possible, EU and national laws need to allow the operation of HRIS systems which can track employee usage.

# 3.9

## Risk Assessment

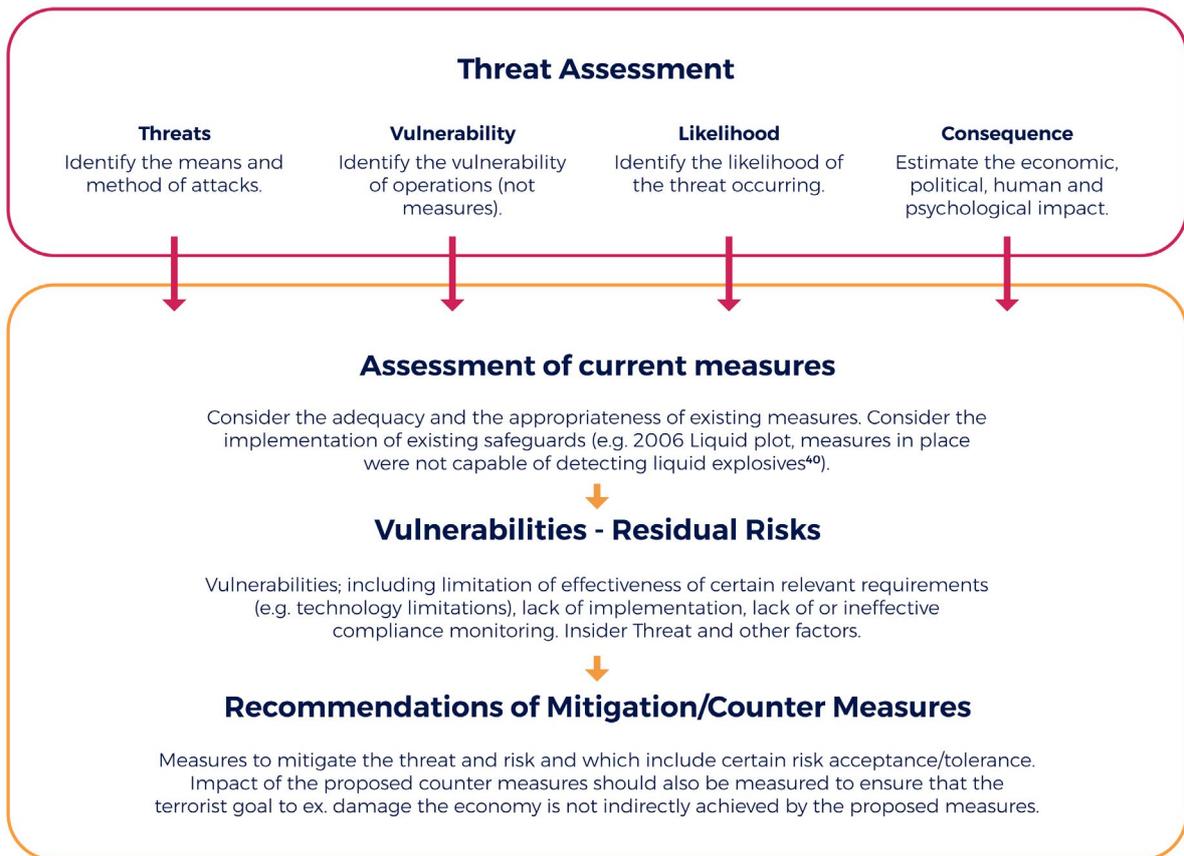
Using appropriate security measures can prevent a wide variety of Insider attacks. These could be from Insiders committing theft/fraud, or the facilitation, planning or actual conduct of a terrorist attack.

It should be noted that many of these measures can be labour intensive and therefore carry a substantial cost and may also result in delays to business processes, such as recruiting or moving of staff between different business areas. Therefore, it is very important that they are implemented in such a way that they reflect the severity of the risk.

Risk management will provide a systematic basis for efficient and proportionate employee security; it is the foundation of the employee security management process and is a continuous cycle of:

- Risk assessment - assessing the risks to the organisation and its assets in terms of the likelihood of a threat taking place, and the impact that such an event might have;
- Implementation - identifying and implementing effective security measures to reduce the likelihood and impact of the threat to an acceptable level (remember that risk can never be 100% eradicated);
- Evaluation - assessing the effectiveness of the countermeasures and identifying any necessary corrective action(s);
- Do not assume but assess, and assess as often and realistically as possible. Check your assessments in real life by testing out threat scenarios to check your resilience, mitigation, business continuity and after-incident response/investigation.





40 The 2006 transatlantic aircraft plot was a terrorist plot to detonate liquid explosives, carried on board an airline aircraft travelling from the United Kingdom to the United States and Canada, disguised as soft drinks.”

# 3.10

---

## Infinity/ Continuous Screening

It should be very carefully explained why “vetting” is so important in the recruitment process.

- It is important to address the vetting issue, not only during recruitment processes, but also the concept of continuous (infinity) vetting;
- The multiplicity of facilitators that provide falsified information, which looks very credible, make careful vetting a must. Fake diplomas, references, statements about previous employers, titles/functions, salaries & benefits, work content and achievements are rampant and should be carefully checked;
- The key message is also: if a person was initially dishonest in an interview to get a job, (s)he’s most likely going to be dishonest once (s)he’s in the job (and effectively steals the work, recognition and trust of colleagues and management).

Companies need to protect all bona-fide employees, their customers and their assets from imposters.

# 3.11

## Managing Trust & Suspicion

Many companies in the recent past, many companies have learned to find a balance, which is required to protect themselves against Insider Threats without surrendering to collective paranoia and seeing a threat around every corner. It is therefore important that companies:

- Establish a well thought-through and documented process for responding to Insider Threat alarms, which should be perceived by the entire workforce as transparent, fair and which protects employees' rights at all times. (Always grant the "benefit of doubt");
- Employees should be convinced, not by words and procedures, but by actions, that Insider Threat concerns will on every single occasion be taken seriously, while at the same time they will be placed in context and investigated carefully. (Not a quick jump to conclusion based on loose unverified information);
- Should an actual Insider Threat case have taken place, it pays to have a process in place in which the entire company is briefed about the details, which in turn should serve as a warning for the future. Doing so will also curb rumours from spreading through the company, which could cause even more harm.

Note: a workforce that notices that their reports and feedback are taken seriously and dealt with fairly will respect the company's leadership and will lead to more and better reporting, as they understand that this protects their position and livelihood.

# 3.12

## Reporting Suspicious Behaviours & Issues

A key element in any security management system is the importance of having a “no blame” (or “just”) culture. This requires systems that support individuals making reports, even in situations where they need to admit to making a mistake. Fear of blame or punishment will more often than not result in a wall of silence and lack of action. Individuals need to understand that a mature organisational security culture can accept that humans make mistakes without imposing immediate punitive measures.

The company should clearly explain how reporting should be performed and assure that anonymous reporting systems are fair, robust and respected by all. Some important elements are:

- The “anonymous” element of the reporting should be credible and well documented/explained;
- Reporting should be simple and free of administrative hurdles;
- Reporting should be possible at department level;
- Reporting should contain multiple choice items to better define the reported issue but should also offer a free text option;
- Post-reporting feedback should be clearly defined and complied with.

**If any employee finds him/herself in a situation where (s)he hesitates “should I report this?”, then the answer should always be, without a single doubt:**

**YES!**

Companies should take a pro-active stance and encourage employees to report anything out of the ordinary.

Where employees hold security clearance(s) they should be required, or it should be mandatory, to report adverse information, including potential threats.

- Have employees trust their instincts, if they see something, they should say/report something!
- It should be policy that it is better to report something that turns out to be nothing than to not report something, which later turns out to be a serious security issue;
- Make sure that all employees know and understand the threat indicators. (Conduct regular awareness training and update the course regularly);
- Ensure that every manager/supervisor knows their staff and therefore will recognize concerning behaviours as potential indicators;
- Pay close attention at termination(s) (offboarding/exit) procedures;
- Monitor all facility ingress and egress points. (Both for ICT systems and physical security)!
- Baseline<sup>41</sup> normal activity and keep a sharp lookout for any anomalies;
- Work together across the organisation;
- Educate employees regarding potential recruitment.

<sup>41</sup> A minimum or starting point used for comparisons.

# 3.13

---

## Post Reporting

The company's response mechanism when reports are received needs to be appropriately reactive to ensure company employees continue to make reports. This might require coordination with all involved company departments and, where applicable, also the law enforcement and security agencies that have been involved.

A set of standard operating procedures should be developed to deal with a range of likely scenarios. These procedures must be regularly tested for effectiveness and can be included as a component of any security exercise.

- Internal investigation procedures should be robust and clearly defined;
- Internal investigation procedures should be agreed with all social partners (employee representation, trade unions, etc.);
- Organisations should make a commitment and take responsibility to effectively handle all Insider Threat reports;
- The entire procedure should preferably be anonymous.



# 04.

---

## Protective Measures



Companies are bound to trust their workforce, which can leave them vulnerable to malicious Insiders, who often use particular methods to hide their (planned) illicit activities. Companies can effectively detect, prevent, and respond to the unique threat from Insiders if they took sufficient specialised action. The best time to develop an effective Insider Threat Program which mitigates both malicious Insider incidents and the unintentional Insider Threat is before they occur, not as one is unfolding or discovered at a later stage. When an Insider incident does occur, the process can be modified as appropriate, based on the investigation results from prior Insider Threat incidents.

The most effective protection against Insider Threats always involves some combination of managing the potential Insider perpetrators and the items/ persons which must be protected against them.

### Screening Tools for Insider Threats

 Ongoing, continuous (infinity) evaluation.

 "Post Mortem" screenings.

 Credit reports (if legally allowed).

 Asset searches (if legally allowed and relevant).

 Social media (if legally allowed and relevant).

 Issues with temporary workers, contractors, interns.

 Preventing identity fraud

 Screening current workers.

 Search for fake diploma's & employment.

 3rd party data theft.

## ICT Tools

Insider Threat mitigation is a multi-faceted challenge that involves the collection, storage and analysis of data to identify threat(s) posed by many different employee types who possess authorized access to (company) assets such as people, information, technology, and facilities.

The secret to truly protect a company against Insider Threats lies with greater data-level protection. This is particularly true for any company making the move into the cloud, as cloud-based ICT services are often staffed by non-employees who manage service platforms beyond the control and visibility of the organisation.

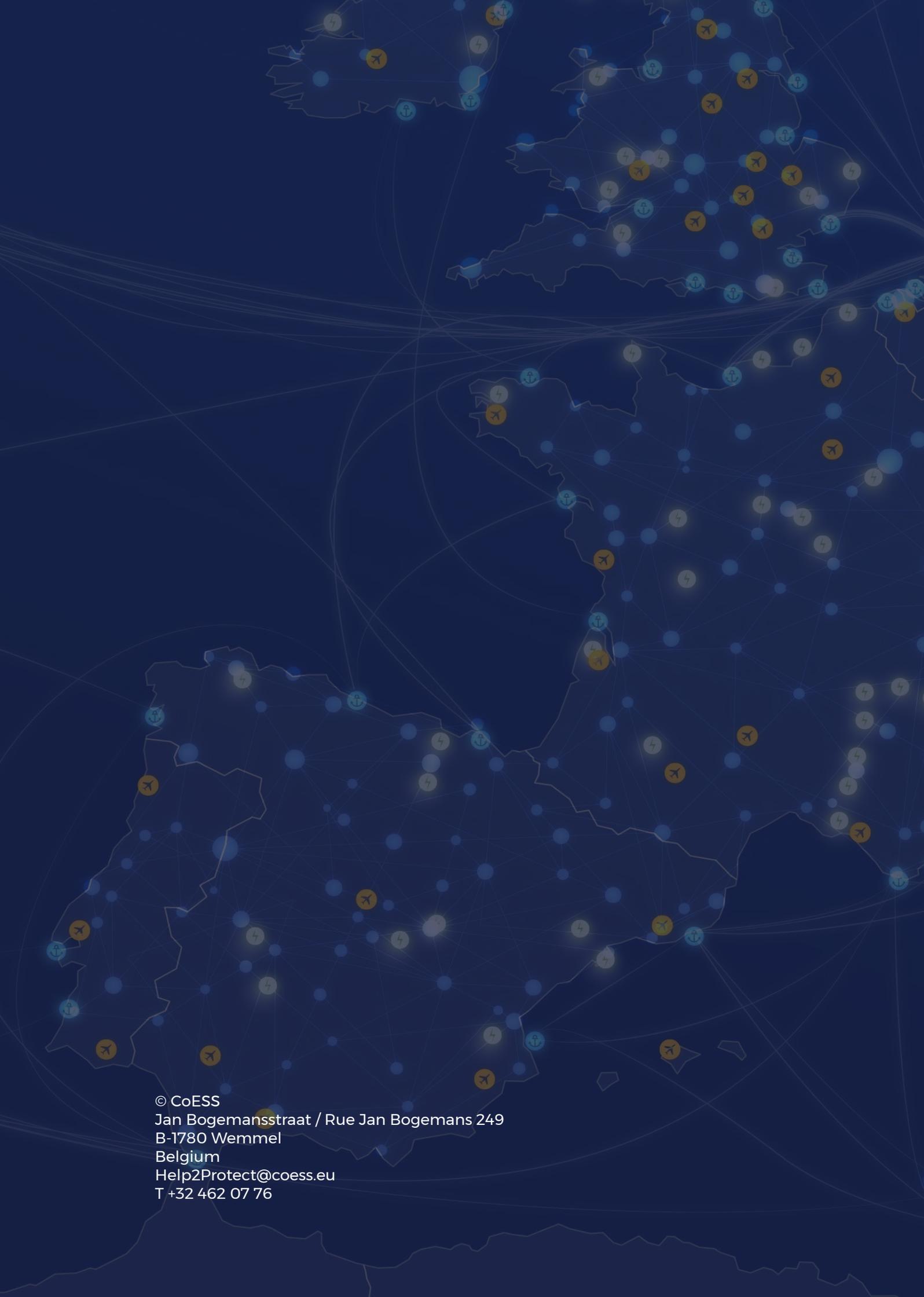
The ever-changing landscape of software solutions designed to aid in Insider Threat protection is almost as wide and varied as the problem itself, which leaves companies with the challenge of understanding not only the complexities of Insider Threats, but also the wide array of tools and techniques that can assist with Insider Threat mitigation.

There are many features to prevent, detect, deter, and respond to Insider Threats. This list is of course not exhaustive, but it does provide some examples that

might be considered as part of your own robust and comprehensive Insider Threat prevention platform.

- Above all, be capable to preserve forensic artefacts in the event of litigation;
- Perform continuous audit of network and host-based activities;
- Monitor data and prevent it from leaving authorized locations;
- Correlate and resolve user and system entity activity across various data sources;
- Perform analysis on data being gathered in the form of rule-based alerting, statistical anomaly detection or both, and prioritize those alerts;
- Generate data visualizations to aid in analysis;
- Manage and track the status and resolutions of cases and incidents;
- Install accurate sentiment, attitude and affect analysis<sup>42</sup> for text-based data sources;
- Mask or anonymize sensitive information that is presented to analysts. (Privacy laws).

<sup>42</sup> The process of computationally identifying and categorizing opinions expressed in a piece of text, especially in order to determine whether the writer's attitude towards a particular topic, product, etc. is positive, negative, or neutral.



© CoESS  
Jan Bogemansstraat / Rue Jan Bogemans 249  
B-1780 Wemmel  
Belgium  
[Help2Protect@coess.eu](mailto:Help2Protect@coess.eu)  
T +32 462 07 76