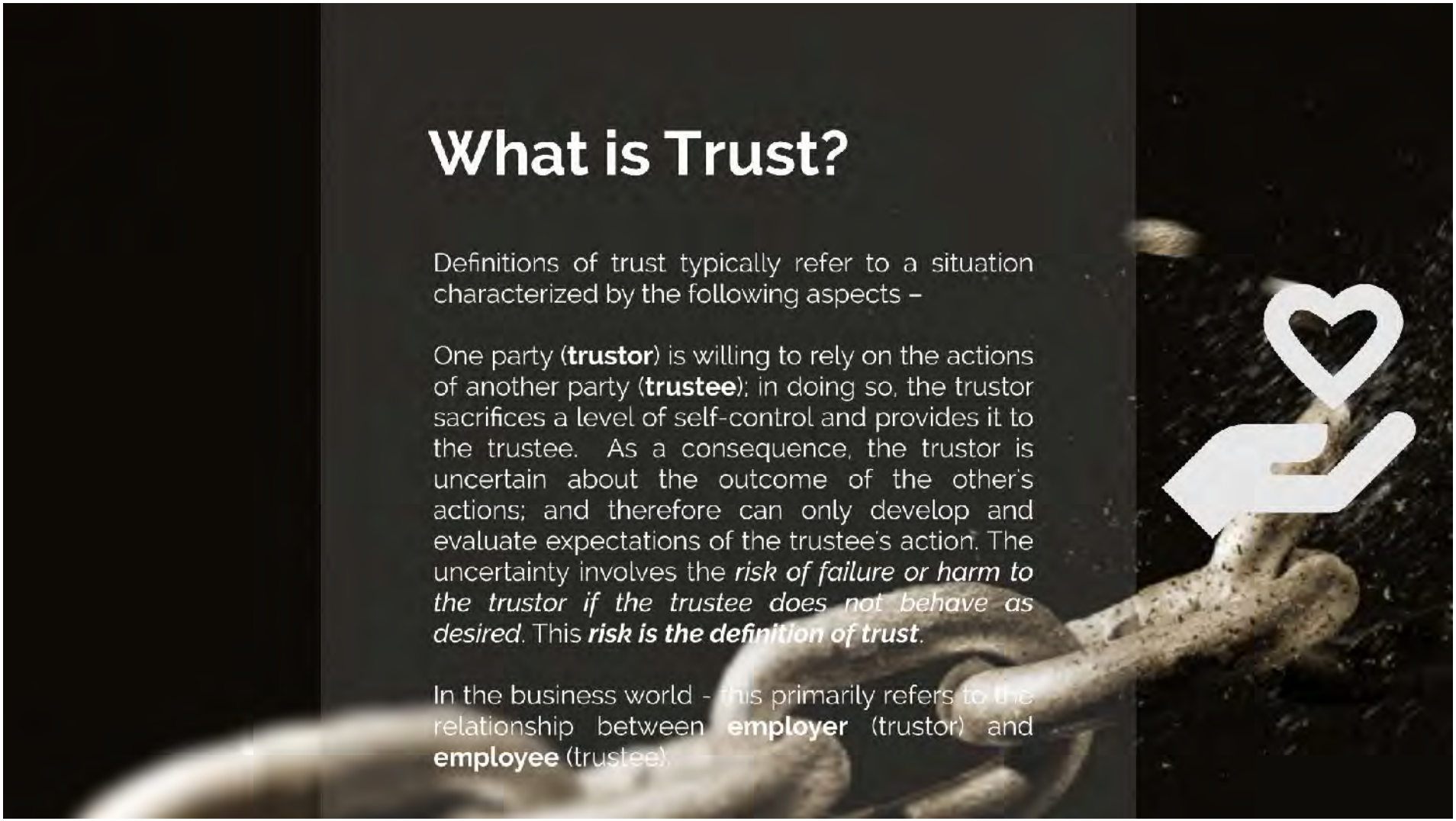

Misused Trust and Authorisation
An introductory Insider Threat Presentation
WFP
Humanitarian Aviation Webinar: AVSEC Insider Threats in Humanitarian Operations
Presentation Overview
Trust
Authorisation
What is Insider Threat?
Types of Insiders
Insider Characteristics and Motivators
Insider Threat Themes
Insider Threat Domains
Insider Threat Attacks
Insider Threat in Aviation
Deterring Insiders
Insider Threat Mitigation
Insider Threat Programs
Theories of Deterrence
Hypotheses of Prevention
Summary: Closure
Summary: What Now?
AEDIS


Presentation Overview
In this insider threat presentation, an overview of what constitutes an insider threat will be defined, and how insider threat is managed. The concepts of trust and authorisation will be addressed to complement your understanding of the subject. The susceptibility of business to insider threat and the increasing drive towards regulated insider threat management is the foundation of this presentation, and the presentation is intended to be informative so that you may become fundamentally informed and actively involved.
As the subsequent sections will discuss the diverse aspects of insider threat, we will fundamentally discuss insider threat for those not entirely familiar with the subject. This will allow a standardised comprehension of the subject moving forward.
By the end of this presentation, learners should be familiar with the terms and concepts of insider threat, and its management


What is Trust?
Definitions of trust typically refer to a situation characterized by the following aspects –
One party (**trustor**) is willing to rely on the actions of another party (**trustee**); in doing so, the trustor sacrifices a level of self-control and provides it to the trustee. As a consequence, the trustor is uncertain about the outcome of the other's actions; and therefore can only develop and evaluate expectations of the trustee's action. The uncertainty involves the *risk of failure or harm to the trustor if the trustee does not behave as desired*. This ***risk is the definition of trust***.
In the business world - this primarily refers to the relationship between **employer** (trustor) and **employee** (trustee).


What is Authorisation?
Authorisation can be considered as *the permission and granting of power or right to do something on behalf of the granting party*.
In the business context, this could be anything from granting the use of an access card to enter private property, making purchase decisions on behalf of the company or making official media statements.


What is Insider Threat?
The aviation industry is a unique industry wherein business, leisure, welfare and politics intersect - and security and safety is a significant factor. The Aviation Industry, despite its heavily regulated security requirements, it is not invulnerable to attack – *especially from within*.
Therefore, this high-profile industry becomes a high-profile target – especially susceptible to the threat posed by *trusted* and *authorised* individuals from within the industry itself. These trusted individuals are referred to as *insiders*, and the *threat* they pose is referred to as *insider threat*.
First, let us delve a little deeper into the definition of **insider threat**.
Threat
Insider
Insider Threat

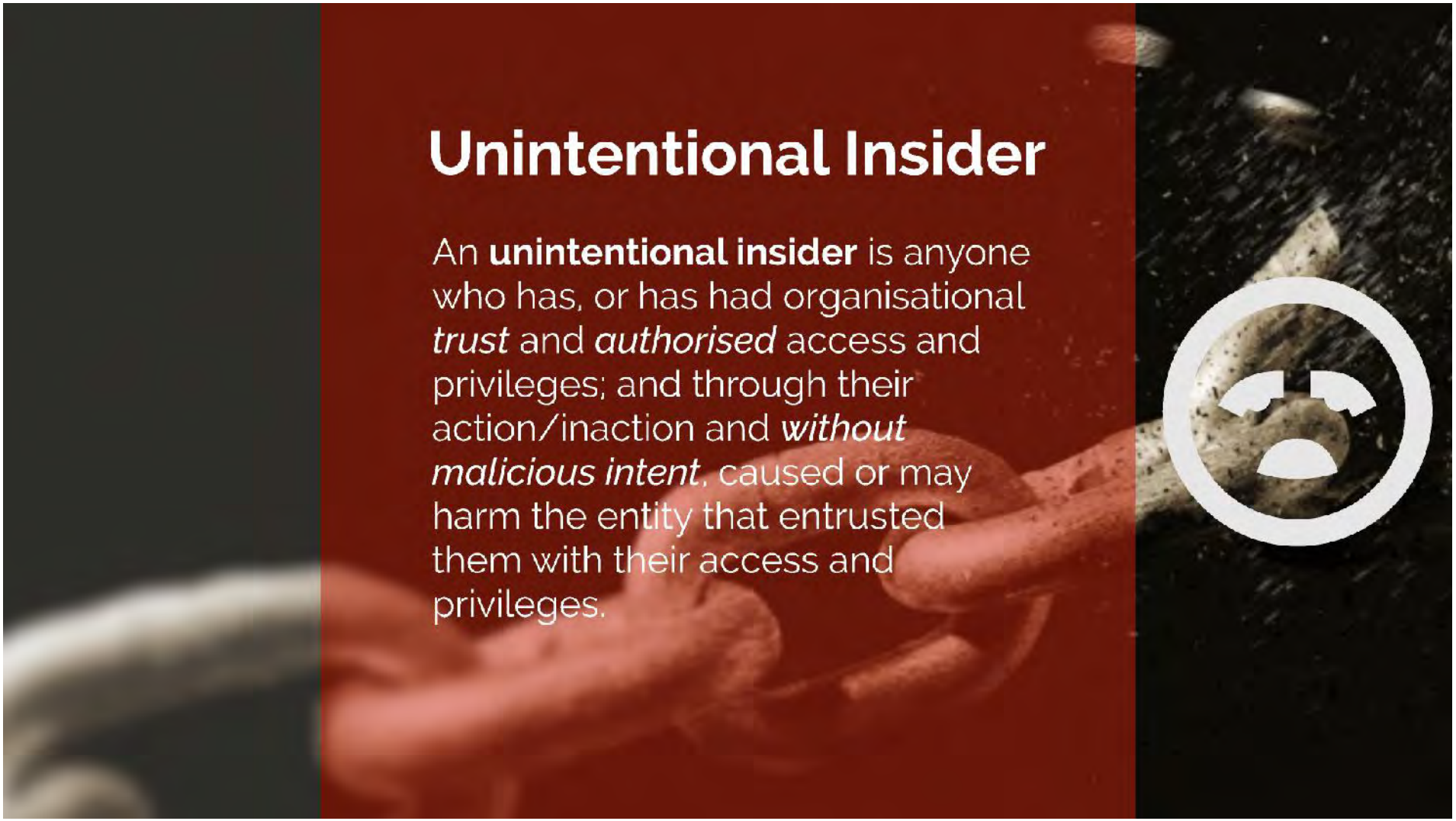

What is a Threat?
The simplest contextual definition of a **threat** is *someone or something likely to cause damage or danger*.
In the context of this presentation, the *threat of damage or danger* comes from individuals known as **insiders**.
So, what exactly is an **insider**?


What is an Insider?
An insider is any person who is trusted and authorised to access and control resources, including personnel, facilities, information, equipment, networks or systems.
For the sake of clarity, an **outsider** may be considered the opposite of an **insider** – that is, anyone who does not have access or privileges, or anyone whose access or access attempt would be considered *unauthorised*.
Considering the specific definitions of insider and threat, what is the definition of an insider threat?


What is Insider Threat?
Insider threat is *the risk an insider will use their authorized access, wittingly or unwittingly, to harm their employer, peers or government.*
This can include theft of resources, proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees or of the public within their duty of care; or any other action that could prevent the employer from carrying out business as usual.


Insider Threat types
Various types of insiders are identified.
They are categorised as:
• malicious insiders,
• unintentional insiders, and
• the threat of collusion between insiders.
The above shall be defined in the following sections.
Malicious Insider
Unintentional Insider
Collusion


Malicious Insiders
A **malicious insider** is anyone who has, or has had organisational *trust* and *authorised* access and privileges; and *intentionally* exceeded or used their access and privileges in a manner that caused or may harm the entity that entrusted them with their access and privileges.


Unintentional Insider
An **unintentional insider** is anyone who has, or has had organisational *trust* and *authorised* access and privileges; and through their action/inaction and *without malicious intent*, caused or may harm the entity that entrusted them with their access and privileges.

Collusion

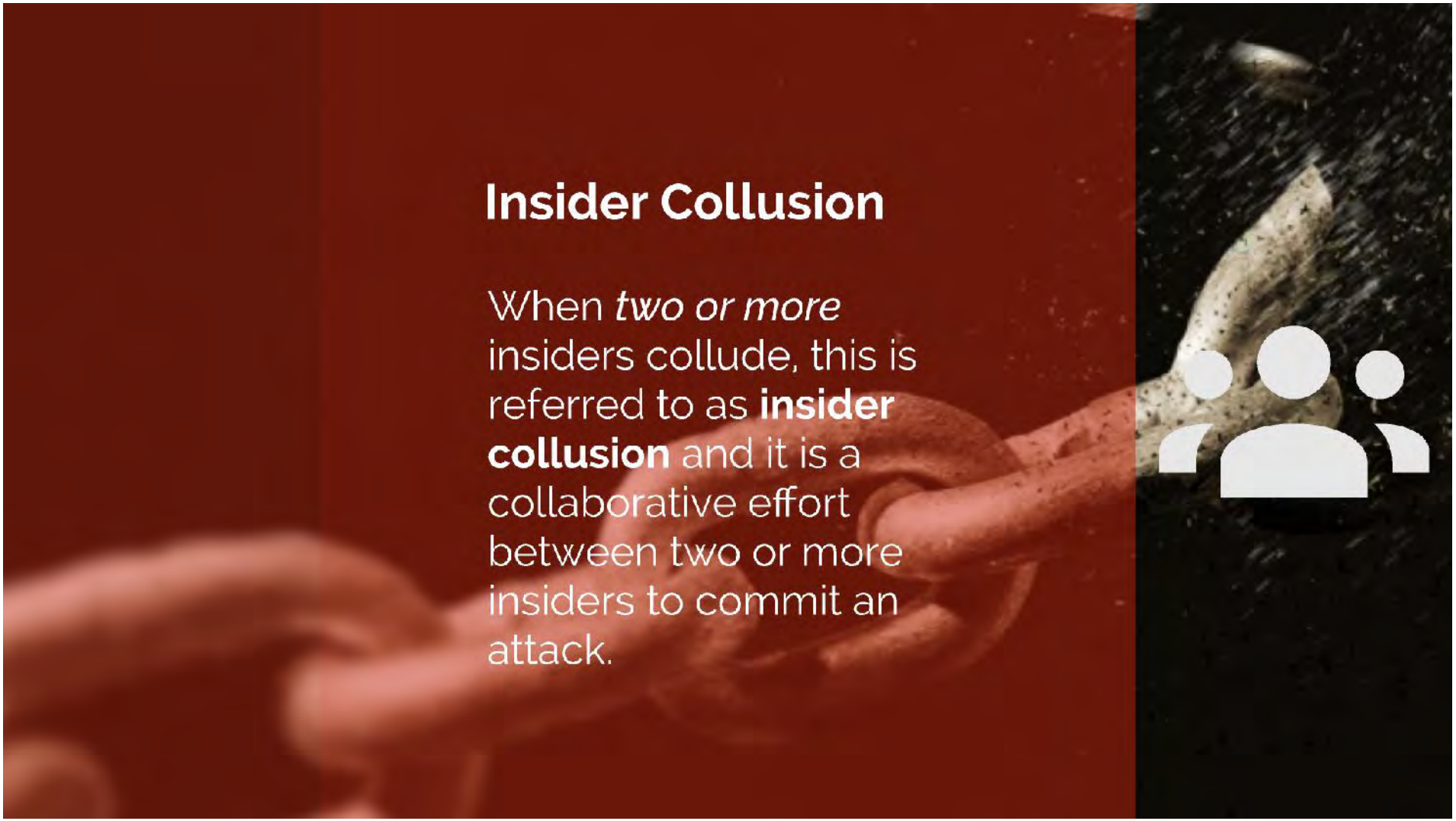
Collusion is a secret agreement or cooperation, especially for an illegal or deceitful purpose.

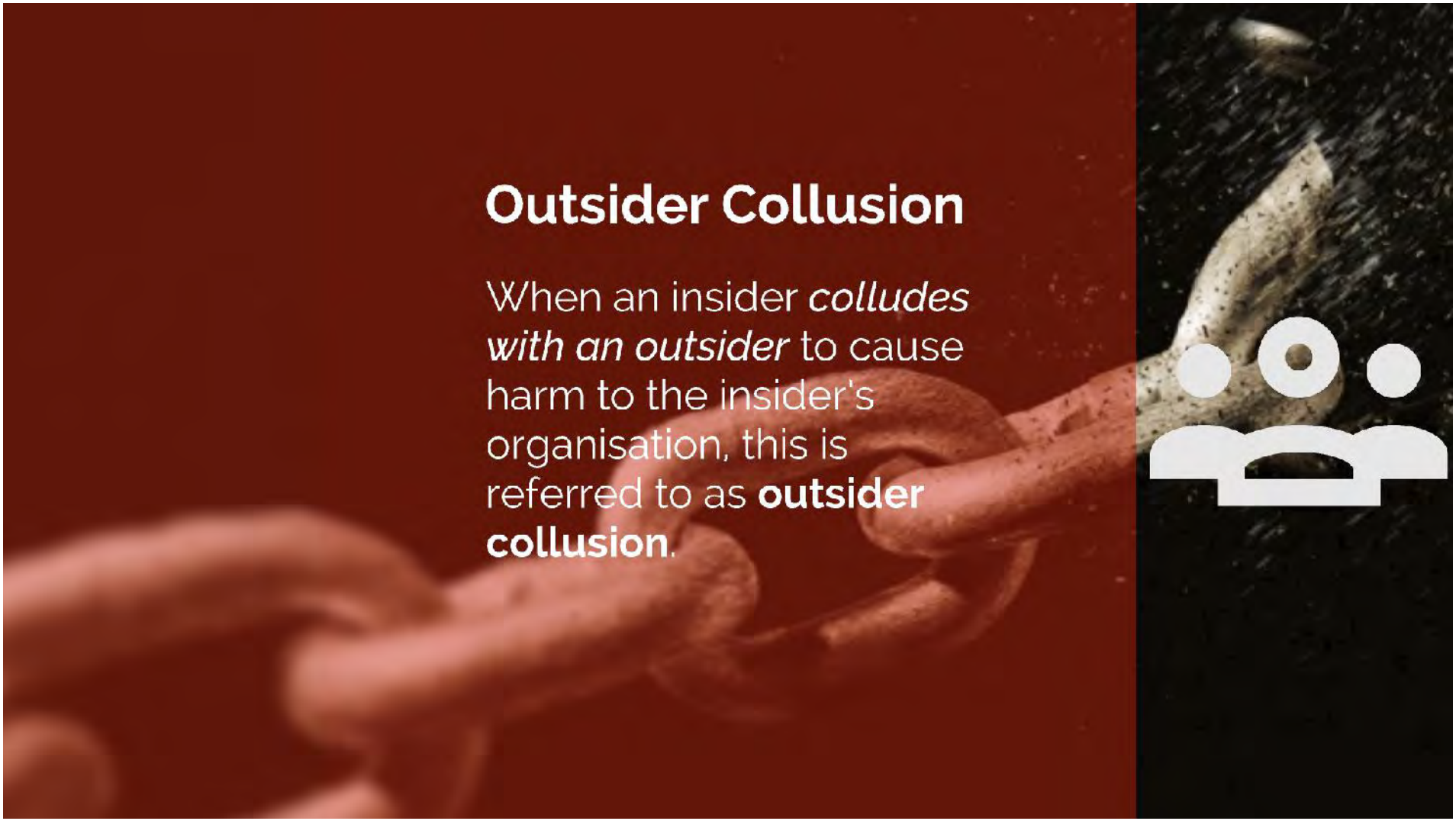
Collusion is a problematic issue to detect and manage, and the intersection of technical and social methods should be considered when developing insider threat programs.

Two forms of Collusion are considered, those being **insider collusion** and **outsider collusion**.

Insider Collusion

Outsider Collusion


Insider Collusion
When *two or more* insiders collude, this is referred to as **insider collusion** and it is a collaborative effort between two or more insiders to commit an attack.


Outsider Collusion
When an insider *colludes with an outsider* to cause harm to the insider's organisation, this is referred to as **outsider collusion**.

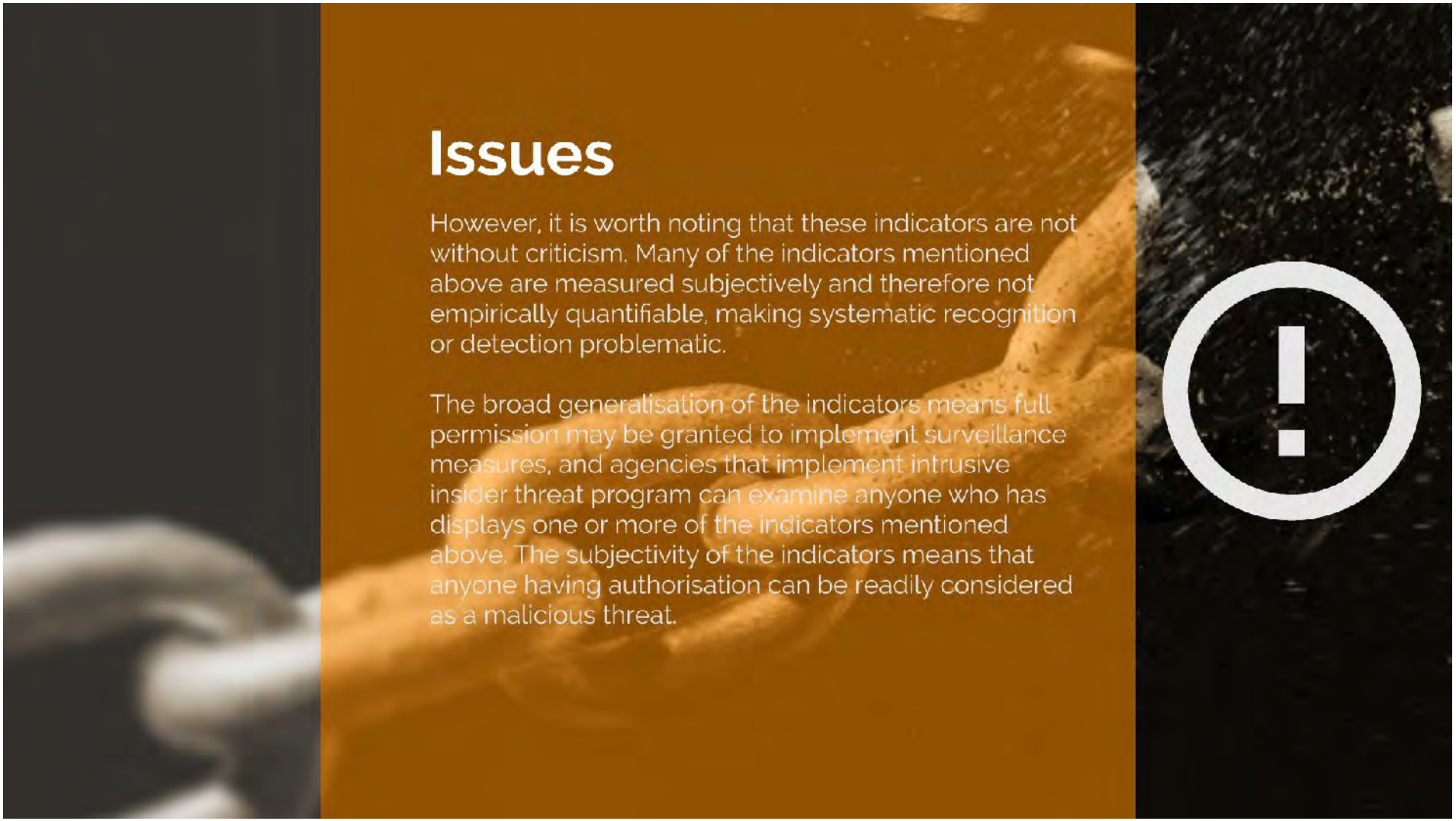
Insider Characteristics and Motivators

What exactly motivates a trusted employee, to betray the trust and authority vested in them, for the benefit of the insider and or outsiders – at the cost to their employer or a greater notion? Some of these concepts will now be briefly discussed.

Although the intent of this presentation is not to portray relevance or accuracy of what behaviors define an insider, it is prudent to list some of the indicators/motives that are considered as insider threat motivators for informational purposes.

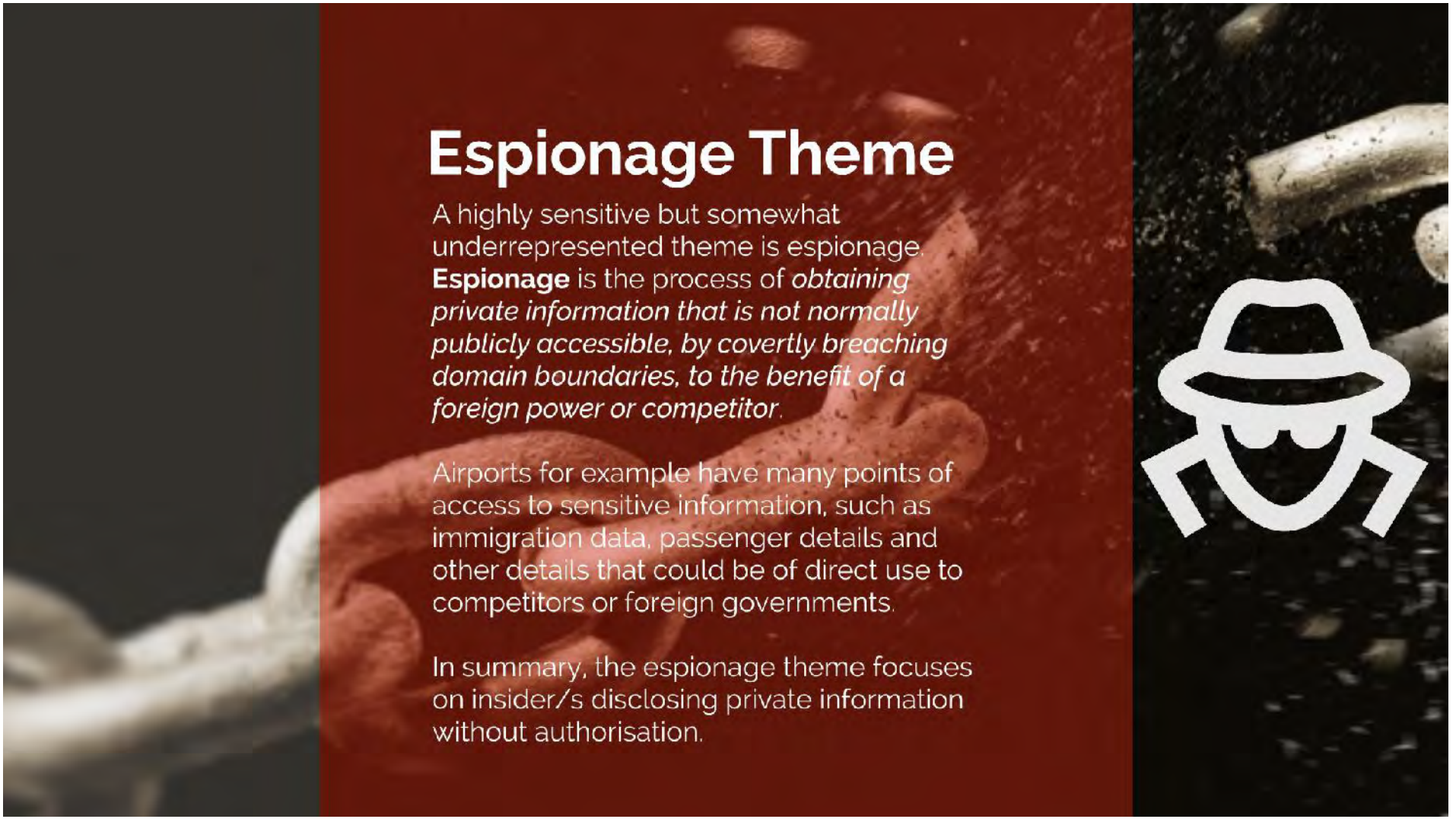

Motivators and Characteristics
• Introverted Personality
• Passive Aggressive Personality
• Narcissistic Personality
• Greed or Financial Problems
• Blackmail Vulnerability
• Compulsive and Destructive behaviour
• Rebelliousness
• Ethical "flexibility"
• Reduced loyalty
• Sense of Entitlement
• Hiding of faults or mistakes
• Inability to assume responsibility for their actions
• Criticism Intolerance
• Self-perceived value exceeds the performance
• Lack of empathy
• A predisposition towards law enforcement
• A pattern of frustration and disappointment
• Poor crisis management


Influences
There are a number of external factors which have been noted as influencing factors in increasing propensity towards insider threat behaviours.
• Mergers and acquisitions,
• Company downsizing,
• Cultural differences.
You may note that workplace uncertainty tends to increase the tendency towards insider threat behaviour. This does not neccesarily mean it will be malicious - during periods of personal uncertainty, people may tend to become less focused on policy and protocol.


Issues
However, it is worth noting that these indicators are not without criticism. Many of the indicators mentioned above are measured subjectively and therefore not empirically quantifiable, making systematic recognition or detection problematic.
The broad generalisation of the indicators means full permission may be granted to implement surveillance measures, and agencies that implement intrusive insider threat program can examine anyone who has displays one or more of the indicators mentioned above. The subjectivity of the indicators means that anyone having authorisation can be readily considered as a malicious threat.


Insider Threat Themes
The reasoning for an insider's malicious behaviour are categorised into **themes**.
These three recurring themes are **Terrorism**, **Espionage** and **Corruption**, and will now be discussed.
Terrorism
Espionage
Corruption


Terrorism Theme
Terrorism is by no means an easily defined term and or act. The United Nations adopted the definition of terrorism as any *criminal acts, including those against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public.*
In summary, the terrorism theme focuses on insider/s intending to cause or facilitate causing a state of terror.

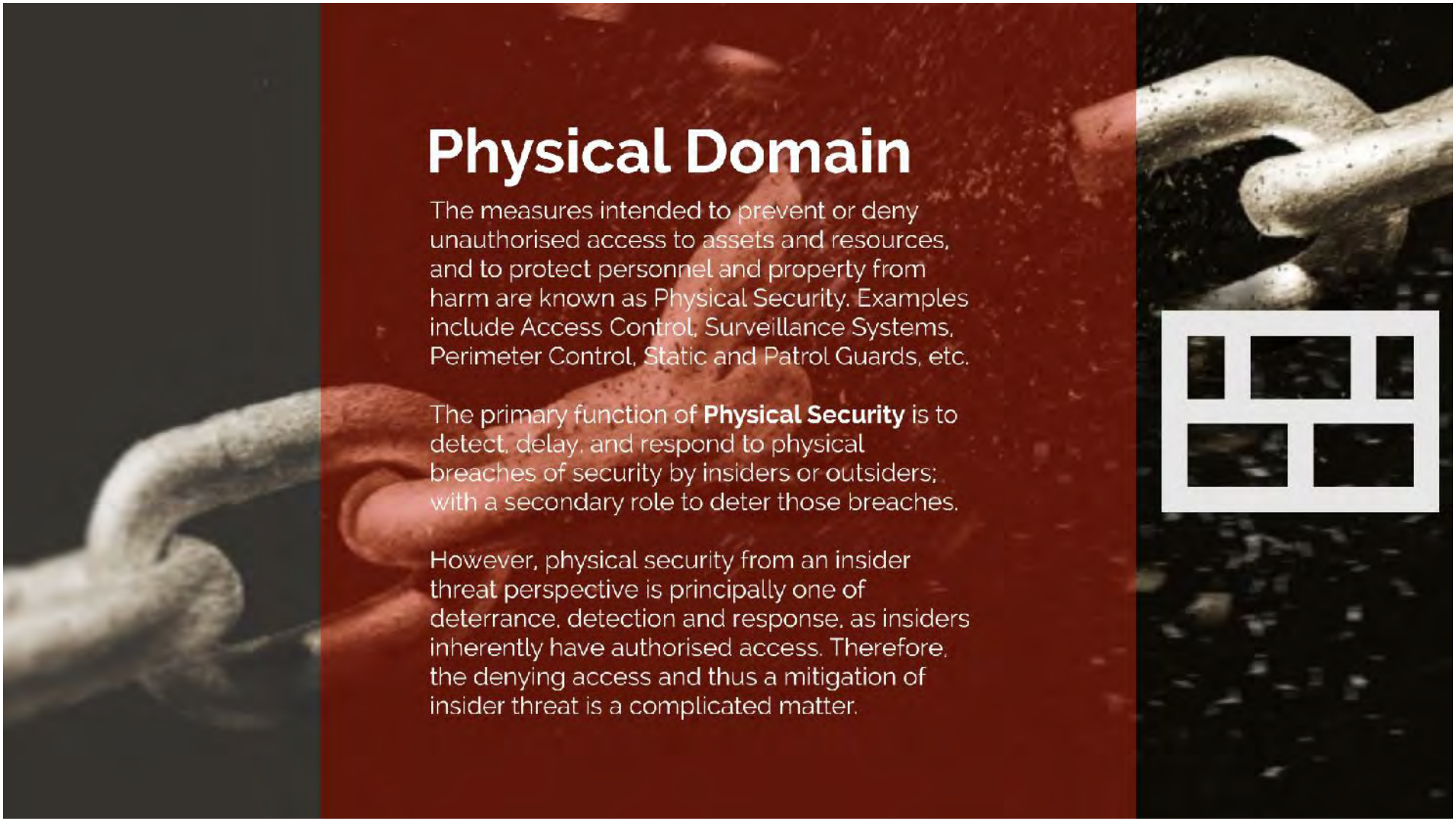

Espionage Theme
A highly sensitive but somewhat underrepresented theme is espionage. **Espionage** is the process of *obtaining private information that is not normally publicly accessible, by covertly breaching domain boundaries, to the benefit of a foreign power or competitor*.
Airports for example have many points of access to sensitive information, such as immigration data, passenger details and other details that could be of direct use to competitors or foreign governments.
In summary, the espionage theme focuses on insider/s disclosing private information without authorisation.


Corruption Theme
Corruption is defined as *conduct which is dishonest or fraudulent with the intention of private gain, such as theft, diversion, divergence, etc.*
Corruption has a multitude of negative impacts on society, costing people their freedom, health, money and even their lives. Corruption can be divided into four categories, those being political, economic, social and environmental.
In summary, the corruption theme deals with insider/s making an unauthorised private gain.


Insider Threat Domains
Concerning insider threat, domains can be considered as the boundary or vector through which an asset is exposed to a threat, and also by which the business is protected. Insider threat is split into three **security domains** exposed to insider threat; those being **personnel**, **cybersecurity** and **physical**. This section defines and discusses those domains of insider threat.
It is essential to not only understand the types of security domains and countermeasures, but also to understand how they integrate with each other, as well as the cross-sectional relationship with the other domains.
Personnel
Cybersecurity
Physical


Personnel Domain
The personnel domain is one of particular importance. The domain of **personnel security** relates to the policies and procedures which seek to mitigate the capability of an insider exploiting legitimate access for unauthorised purposes.
As insiders come from within an organisation, the importance of implementing personnel security measures and procedures is paramount to reduce the likelihood of an attack, by removing potential malicious insiders from the scenario, and reducing the likelihood on unintentional insider threat by increasing awareness.


Cybersecurity Domain
As more reliance is vested in IT and Electronics for the protection and retention of information and security-related access and data – the domain of cybersecurity garners ever-increasing interest.
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and assets.
Cybersecurity measures reduce the capability of insiders and outsiders from malicious or unintentional access to information or controls.


Physical Domain
The measures intended to prevent or deny unauthorised access to assets and resources, and to protect personnel and property from harm are known as Physical Security. Examples include Access Control, Surveillance Systems, Perimeter Control, Static and Patrol Guards, etc.
The primary function of **Physical Security** is to detect, delay, and respond to physical breaches of security by insiders or outsiders; with a secondary role to deter those breaches.
However, physical security from an insider threat perspective is principally one of deterrance, detection and response, as insiders inherently have authorised access. Therefore, the denying access and thus a mitigation of insider threat is a complicated matter.


Insider Threat Attacks
To attack, is to set upon or work against something using force – with the definition of force being that of violence, compulsion, or constraint exerted upon or against a person or thing.
With regard to insider threat, the nature of an attack is defined by its theme, and the attack means and its defense are categorised in one or more domains.
Terrorism Attacks
Espionage Attacks
Corruption Attacks

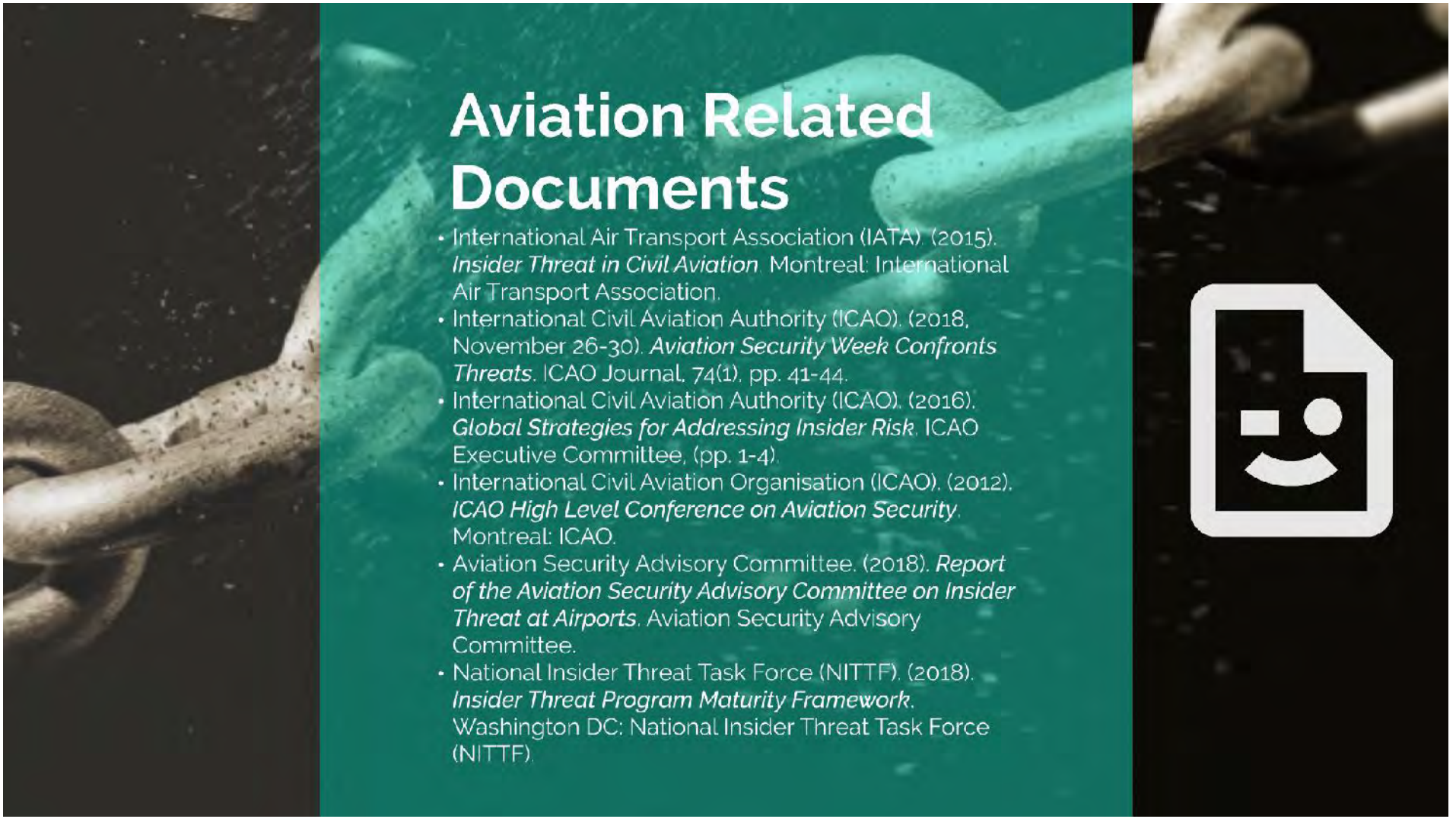

Terrorism Attacks
• 2011: a former UK airline employee was convicted of offering to help an FTO disrupt or damage airline computer systems.
• 2013: a former Wichita Mid-Continent Airport worker was arrested and charged with attempted use of a WMD and attempting to provide material assistance to an FTO.
• 2016: it was revealed that one of the Brussels Airport suicide bombers of had previously worked at the airport for five years, and at least 50 ISIS sympathisers potentially continued to work in the airport, with security passes in roles ranging from shop assistants, cleaners and baggage handlers.


Espionage Attacks
• 2007: Chinese national Chi Mak was covertly sending US Navy secrets to China for over 20 years, via a network of family members.
• 2010: US Army Private First-Class Manning used his privileges to access classified databases to leak classified information to Wikileaks
• 2013: Edward Snowden used his access to classified databases to steal and publish classified information, revealing details of classified US global surveillance programs.


Corruption Attacks
• 2012: a drug and gun smuggling ring at Los Angeles International Airport was discovered leading to the arrest of 4 security screeners, who accepted cash bribes on multiple occasions to allow the movement of illegal narcotics through X-ray machines.
• 2015: An insider at Oakland Airport was criminally charged in relation to the trafficking of narcotics, colluding with other baggage handlers and using their access and privileges to undertake criminal activities undetected for personal gain.
• 2019: the head of security at Geneva airport was arrested on suspicion of corruption and the misappropriation of public interests and funds.


Insider Threat in Aviation
The first recorded instance of an insider threat attack on Aviation is what is known as "Lockerbie", an event in 1988, named after the town where Pan America Airlines flight 103 (PAN AM 103) crashed after an IED detonated onboard.
The head of security for another airline, who was likewise an intelligence officer of a foreign intelligence service, was found guilty of having orchestrated the terror attack by bypassing security procedures and smuggling an IED onboard the aircraft.
This attack would have a significant impact on the industry and was the catalyst for significant Aviation Security reform.
Aviation Insider Threat
Documents


Aviation Insider Threat
Addressing the Aviation Industry's vulnerability to insider threat is necessary and crucial as the industry continues to expand rapidly.
Aviation insider threat is of particular concern, as Aviation insiders have specific knowledge of, and authorised access to critical infrastructure and systems. People other than passengers may either be directly involved in the act of unlawful interference or facilitate it by providing sensitive information or access, knowingly or otherwise by force, free will or corruption. Aviation insiders may know how to cause as much damage as possible and could deliberately plan for the worst scenario - and thus become valuable targets for criminals and terrorists.
Instances of Aviation workers using access privileges to smuggle weapons and drugs into security-restricted areas and onto planes has heightened awareness about security at commercial airports. - however, concrete statistics concerning insider threat incidents are not yet documented.
Failing to implement robust and sustainable methods to mitigate insider threat risk, can compromise the aviation security system in its entirety. Standards and Recommended Practices will be strengthened to ensure the effective implementation of regulatory measures to address insider threat.



Aviation Related Documents

- International Air Transport Association (IATA). (2015). *Insider Threat in Civil Aviation*. Montreal: International Air Transport Association.
- International Civil Aviation Authority (ICAO). (2018, November 26-30). *Aviation Security Week Confronts Threats*. ICAO Journal, 74(1), pp. 41-44.
- International Civil Aviation Authority (ICAO). (2016). *Global Strategies for Addressing Insider Risk*. ICAO Executive Committee, (pp. 1-4).
- International Civil Aviation Organisation (ICAO). (2012). *ICAO High Level Conference on Aviation Security*. Montreal: ICAO.
- Aviation Security Advisory Committee. (2018). *Report of the Aviation Security Advisory Committee on Insider Threat at Airports*. Aviation Security Advisory Committee.
- National Insider Threat Task Force (NITTF). (2018). *Insider Threat Program Maturity Framework*. Washington DC: National Insider Threat Task Force (NITTF).


How do we deter Insiders?
Unfortunately, the same principles that we utilise to find and retain a suitable employee, are the vulnerabilities that are exploited. By trusting and authorising individuals, an employer is creating an insider. The nature of business requires insiders for business to work efficiently, and the relinquishment of some autonomy and an increase in a risk of harm could be considered a necessary evil. However, this does not mean that business should accept insider threat as a certainty, and must take steps to mitigate it.

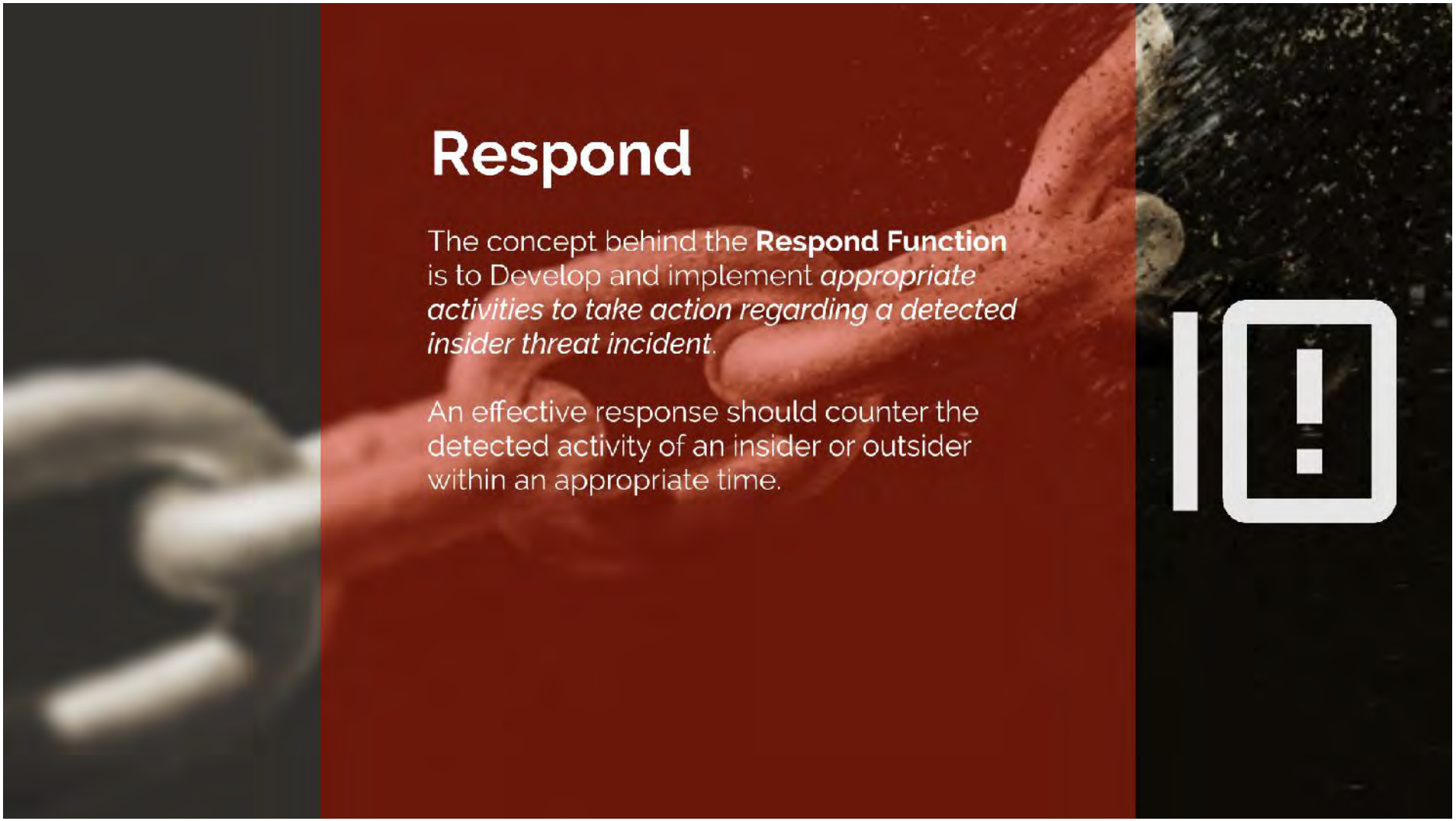

Insider Threat Mitigation
The humanistic and psychological motivation factors through which insider threats arise, make the reduction and mitigation of insider threat a complicated task. In that regard, what is considered as best practice in regards to mitigate exposure to insider threat?
Considering the complex and cross-disciplinary field of understanding insider threat, it is meaningful to outlay the concepts and strategies that are utilised to mitigate insider threat.
II

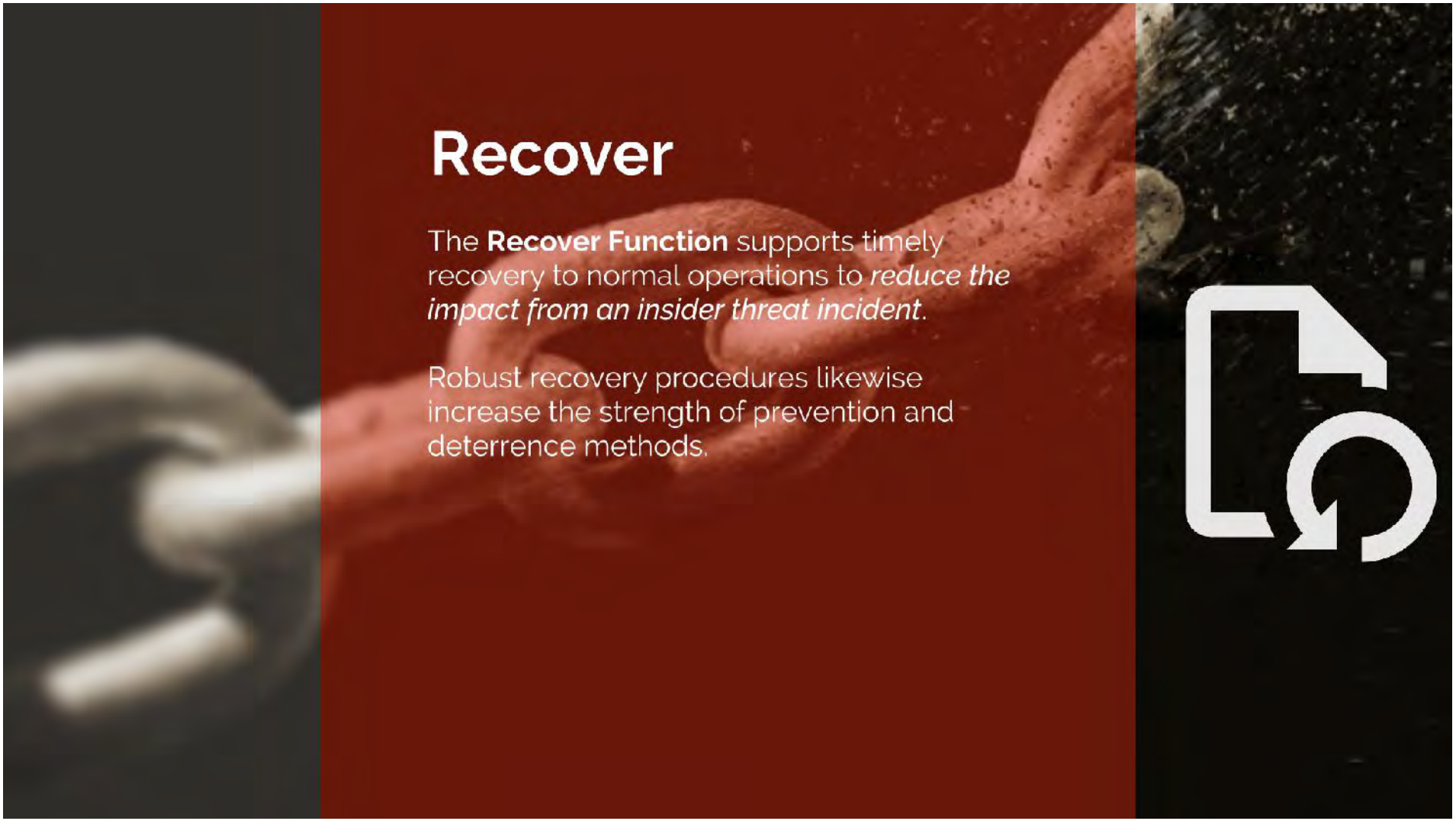

Insider Threat Programs
A critical step in reducing exposure to insider threat is to implement an **Insider Threat Program**.
Insider Threat Programs are intended to deter cleared employees from becoming insider threats, detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative or other response actions.
Identify
Protect
Detect
Respond
Recover
Program Effect Funnel
Issues

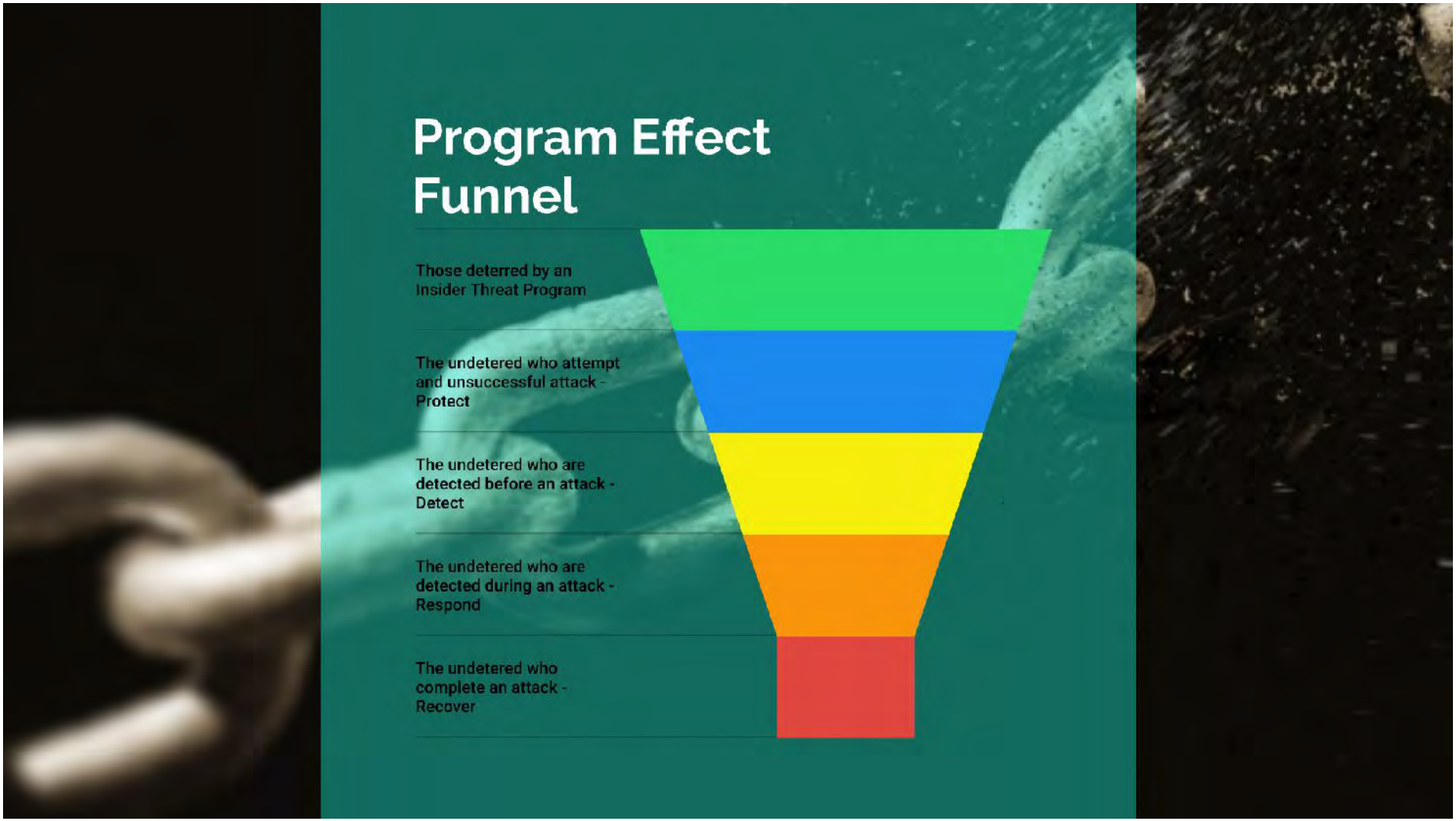

Identify
The processes of the **Identify Function** are foundational for effective insider threat mitigation. It tasks the organisation with *comprehending their own business, the resources that support critical functions, and the related risks.*
This enables an organization to focus effort in developing and understanding how to manage risk to the various domains.

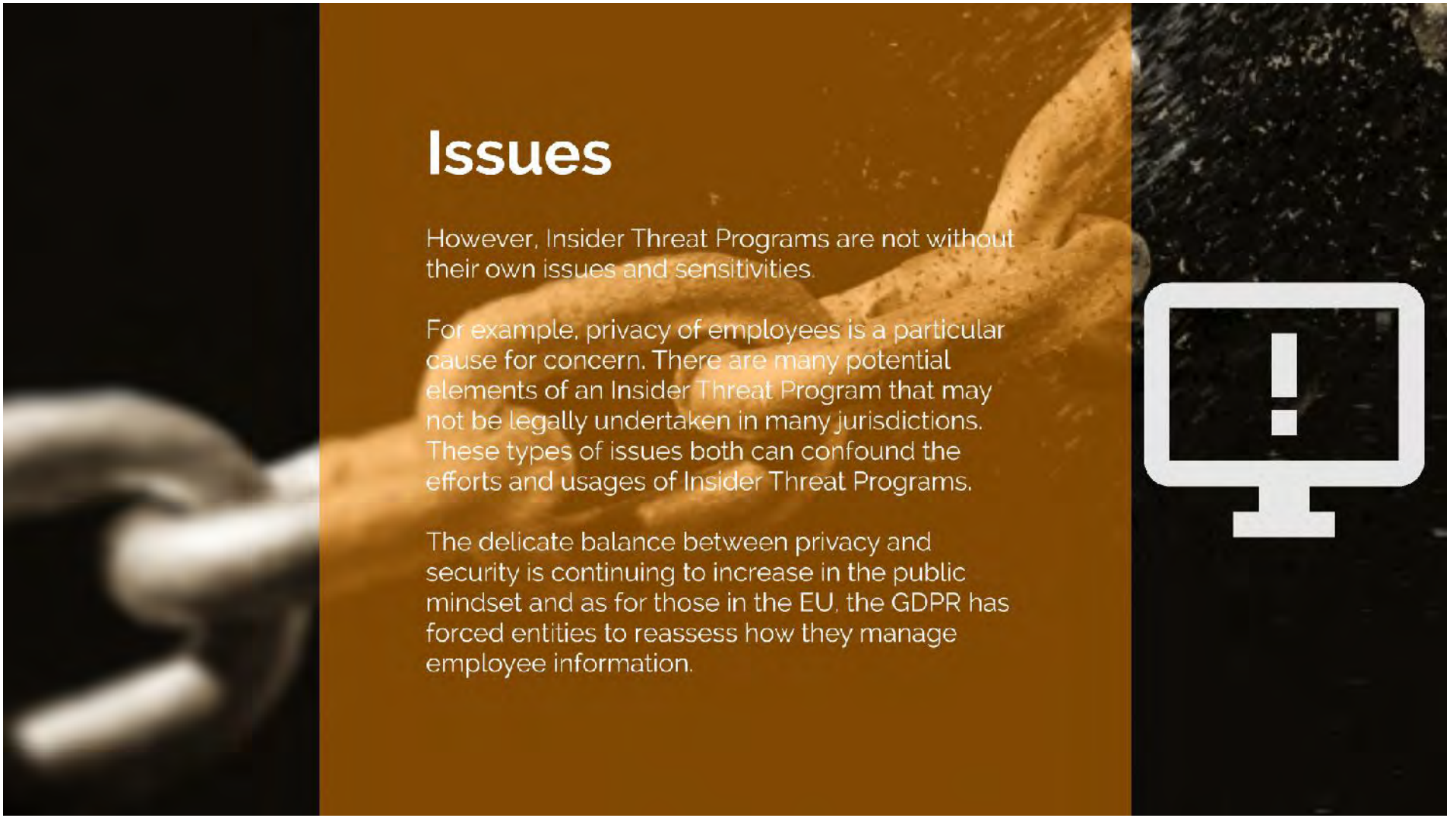

Protect
The **Protect Function** supports the ability to *limit or contain the impact of a potential insider attack*.
It focuses on developing and implementing appropriate safeguards to ensure the ongoing provision of critical services.
This could be achieved by implement measures that both insiders and Outsiders may perceive as too difficult or risky to access or defeat.


Detect
The concept behind the **Detect Function** is to develop and implement appropriate *activities to identify the occurrence of an insider threat event*.
Cybersecurity Intrusion Detection Systems (IDS) are one of these means, as are overt and covert security and surveillance.


Respond
The concept behind the **Respond Function** is to Develop and implement *appropriate activities to take action regarding a detected insider threat incident*.
An effective response should counter the detected activity of an insider or outsider within an appropriate time.


Recover
The **Recover Function** supports timely recovery to normal operations to *reduce the impact from an insider threat incident*.
Robust recovery procedures likewise increase the strength of prevention and deterrence methods.


Program Effect Funnel
Those deterred by an Insider Threat Program
The undetered who attempt and unsuccessful attack - Protect
The undetered who are detected before an attack - Detect
The undetered who are detected during an attack - Respond
The undetered who complete an attack - Recover


Issues
However, Insider Threat Programs are not without their own issues and sensitivities.
For example, privacy of employees is a particular cause for concern. There are many potential elements of an Insider Threat Program that may not be legally undertaken in many jurisdictions. These types of issues both can confound the efforts and usages of Insider Threat Programs.
The delicate balance between privacy and security is continuing to increase in the public mindset and as for those in the EU, the GDPR has forced entities to reassess how they manage employee information.


Theories of Deterrence
An essential element of mitigating insider threat, is to **deter** insiders from the propensity towards malicious behaviour, thereby discouraging insiders from engaging in malicious activities.
Many theories exist in the realms of psychology and criminology related to this topic, however for the sake of brevity we discuss three common **theories**, those being:
• General Deterrence Theory (GDT)
• Situational Crime Prevention Theory (SCPT)
• Theory of Planned Behaviour (TPB)
General Deterrence Theory (GDT)
Situational Crime Prevention Theory (SCPT)
Theory of Planned Behaviour (TPB)


General Deterrence Theory (GDT)
General Deterrence Theory (GDT) describes insider behaviour and decisions as a balance of minimising their risk and maximising their benefit. By *increasing the risk of being caught*, an organisation *decreases the risk malicious behaviour*.


Situational Crime Prevention Theory (SCPT)
In a similar manner as the GDT, **Situational Crime Prevention Theory (SCPT)** details how *decreasing malicious motivation* and opportunity *reduces malicious behaviour*.

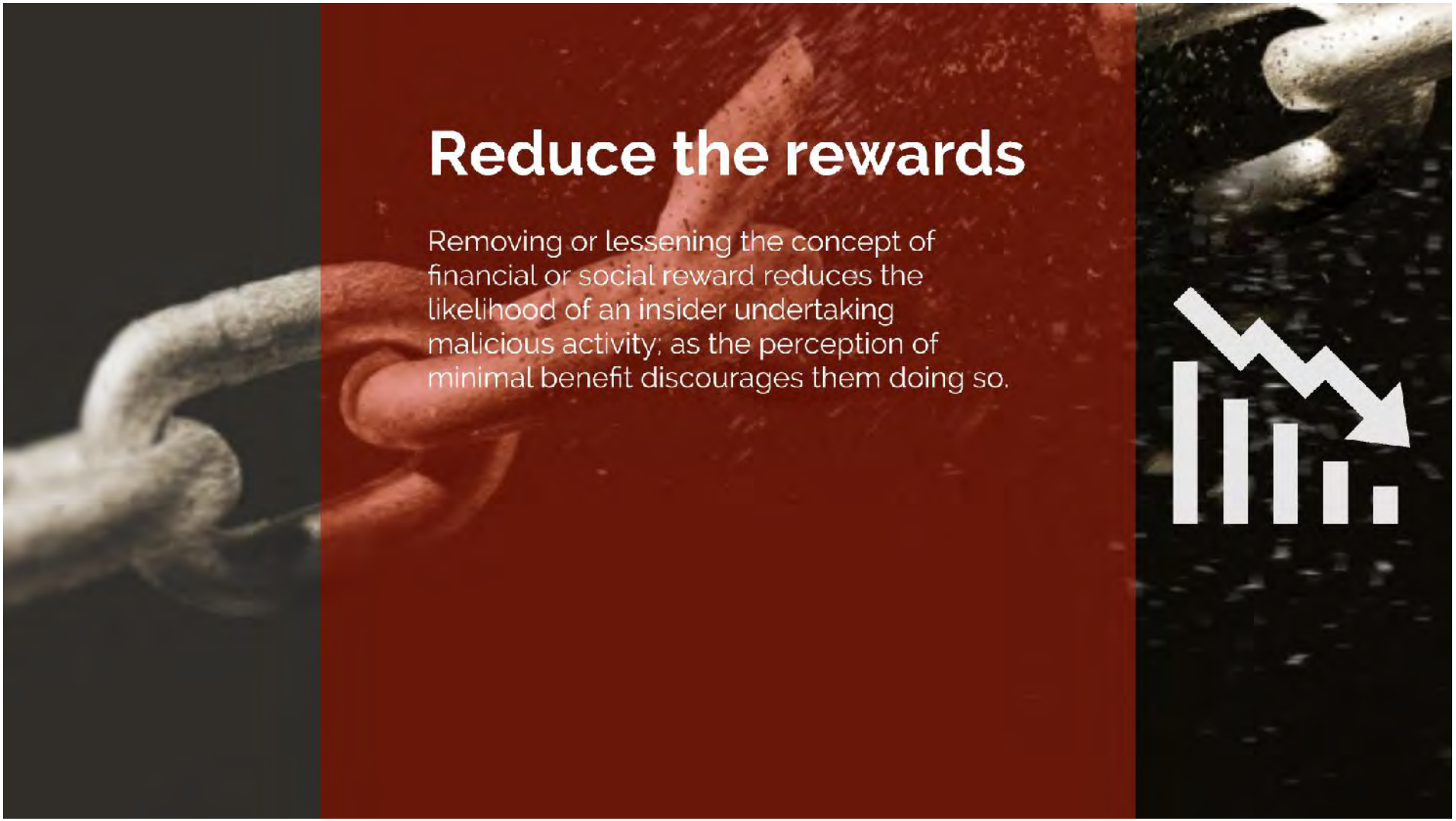

Theory of Planned Behaviour (TPB)
Theory of Planned Behaviour (TPB) encompasses the concept that individuals are more inclined to conduct a certain behaviour when:
• individual(s) evaluate a behaviour positively, and;
• they think that other individual(s) intend to partake in the same behaviour in the same way, and;
• they all believe they have the capacity to perform it.

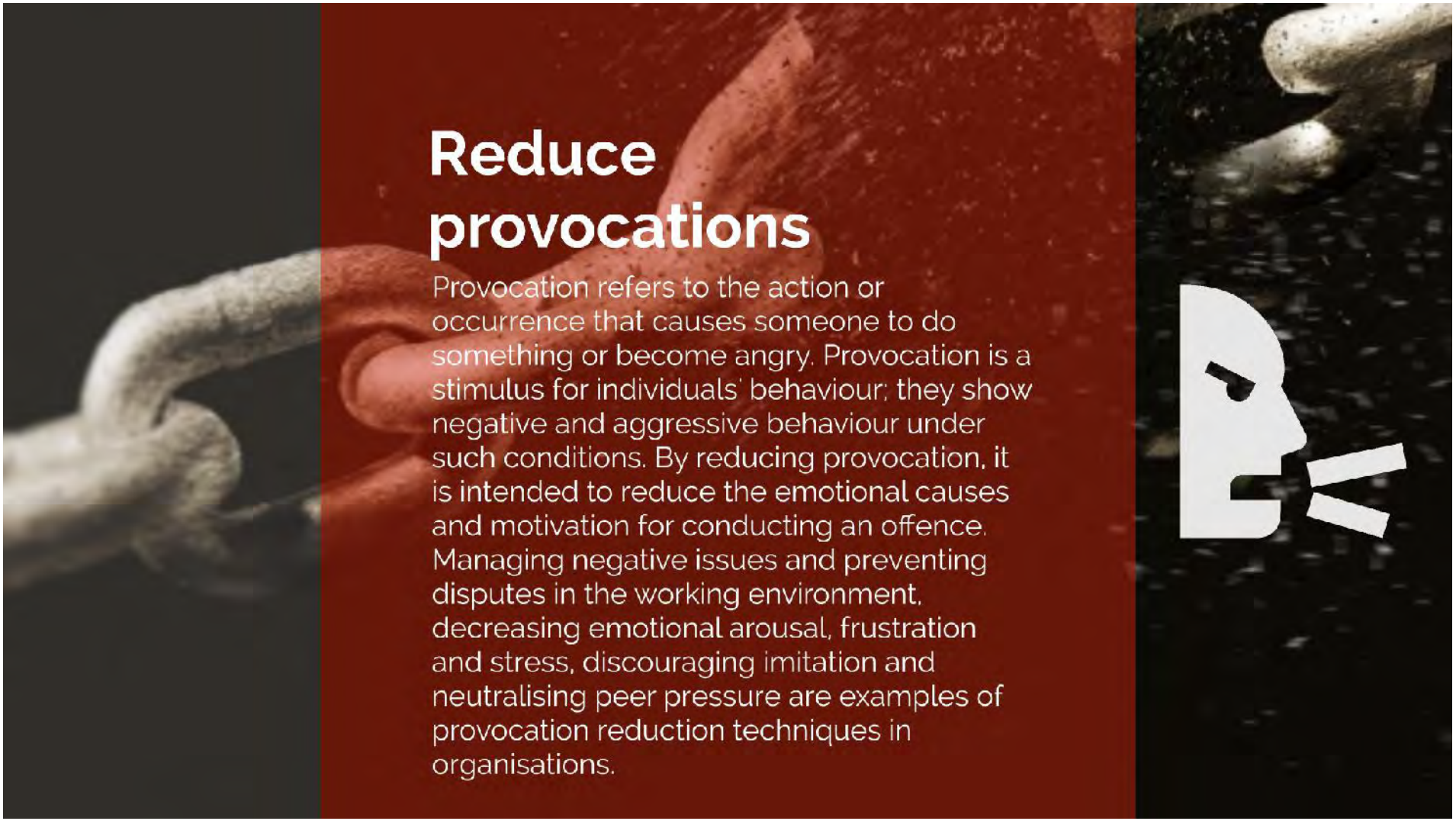

Hypotheses of Prevention
The hypotheses of prevention are intended to facilitate implementation of means to prevent malicious activity by insiders or outsiders.
These hypotheses will now be briefly discussed.
Perceived sanction certainty and severity
Increase the effort
Increase the risk
Reduce the reward
Reduce provocations
Remove excuses
Attitude
Intention

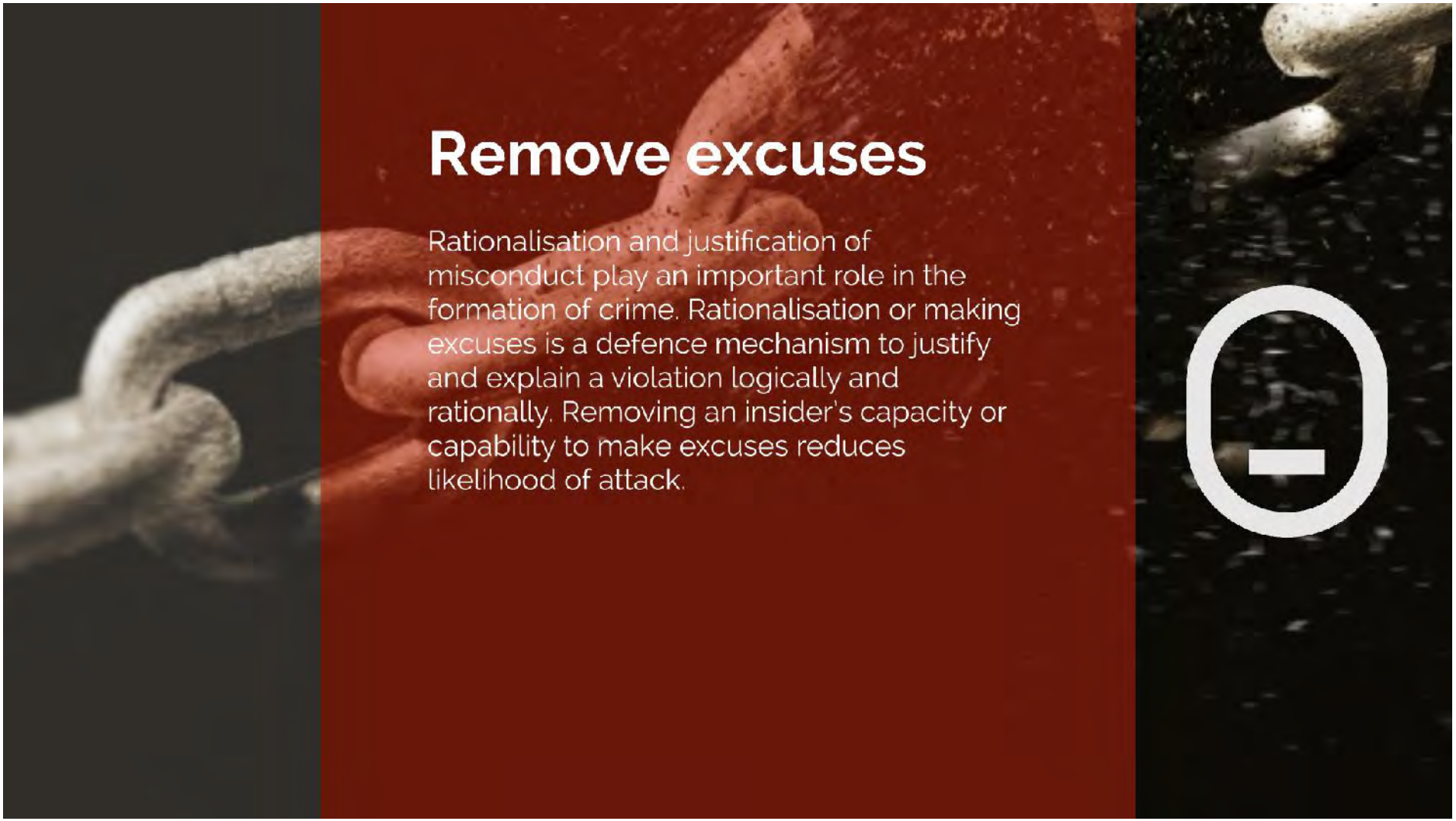

Perceived sanction certainty and severity
The concept of punishment, or sanction, can influence the minds of individuals and their decision to commit a malicious activity. The **certainty** element refers to how strong an insider believes they may be caught undertaking malicious behaviour and the **sanction** element refers to their understanding of the severity of the punishment when they are caught.


Increase the effort
This hypothesis focuses on the concept that the perceived difficulty in undertaking a malicious activity negatively impacts an insider's attitude towards undertaking the activity.

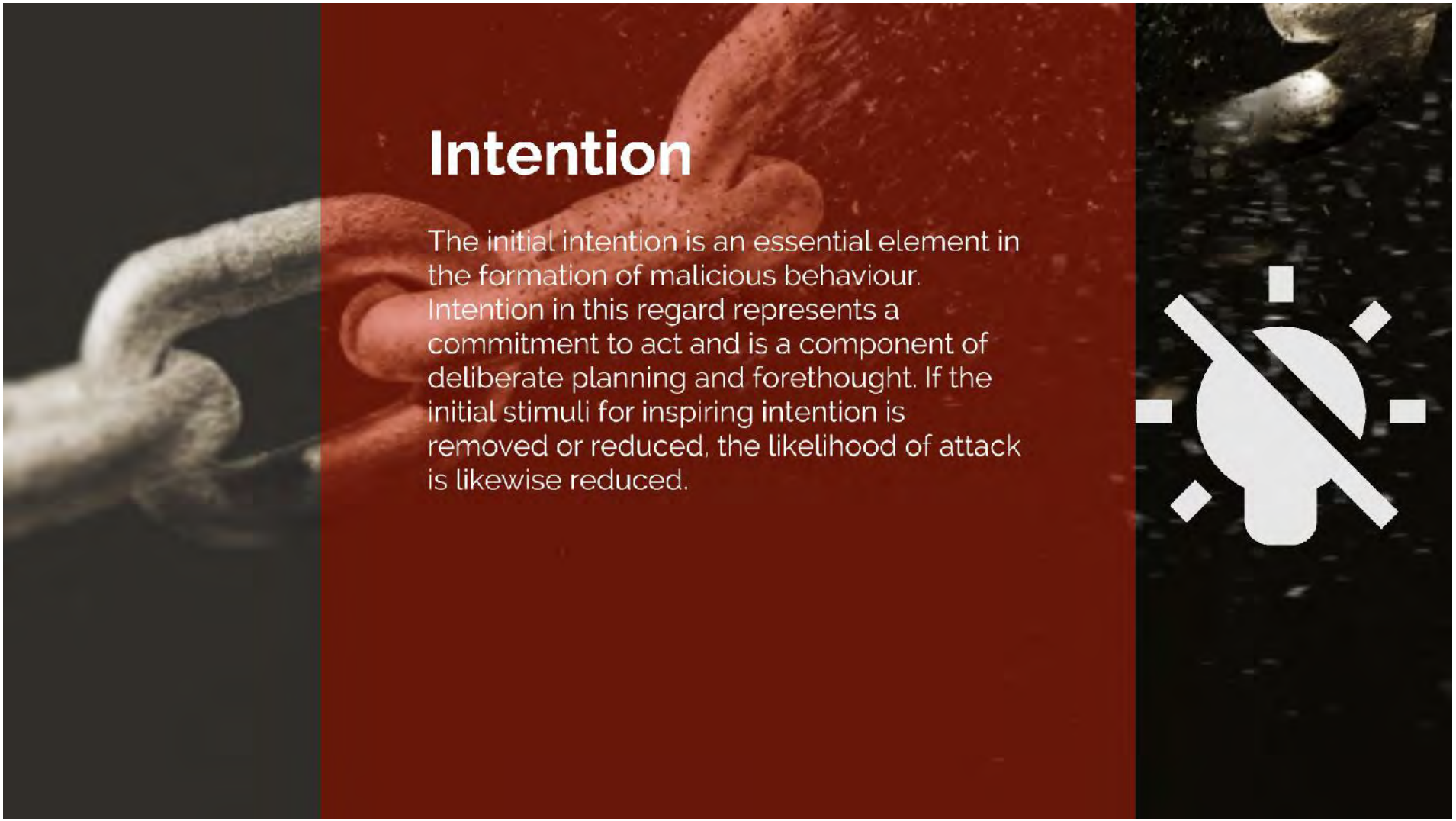

Increase the risk
Risk is considered as the potential for gain or loss. The prediction of the positive outcome of undertaking a malicious activity increases the likelihood of attack. Increasing the perceived risk of being caught reduces attack likelihood.


Reduce the rewards
Removing or lessening the concept of financial or social reward reduces the likelihood of an insider undertaking malicious activity; as the perception of minimal benefit discourages them doing so.


Reduce provocations
Provocation refers to the action or occurrence that causes someone to do something or become angry. Provocation is a stimulus for individuals' behaviour; they show negative and aggressive behaviour under such conditions. By reducing provocation, it is intended to reduce the emotional causes and motivation for conducting an offence. Managing negative issues and preventing disputes in the working environment, decreasing emotional arousal, frustration and stress, discouraging imitation and neutralising peer pressure are examples of provocation reduction techniques in organisations.


Remove excuses
Rationalisation and justification of misconduct play an important role in the formation of crime. Rationalisation or making excuses is a defence mechanism to justify and explain a violation logically and rationally. Removing an insider's capacity or capability to make excuses reduces likelihood of attack.
10


Attitude
The experiences and personal beliefs an insider have towards a potential target affects an insider's attitude. Inspiring a positive attitude of an insider towards what may be the target of a malicious act, reduces the likelihood of attack.


Intention
The initial intention is an essential element in the formation of malicious behaviour. Intention in this regard represents a commitment to act and is a component of deliberate planning and forethought. If the initial stimuli for inspiring intention is removed or reduced, the likelihood of attack is likewise reduced.


Summary: Closure
You should now have a fundamental knowledge of Insider Threat, which should enable you to:
• Define Insider Threat.
• Define the type of Insiders.
• Define the themes and domains of Insider Threat.
• Understand the susceptibility of business to Insider Threat.
• Understand the basics of Insider Threat Programs and Management.


Summary: What now?
• Remain aware of the threat Insiders pose.
• Maintain healthy levels of distrust.
• Be cautious with the dispensation of authority.
• Establish and maintain an Insider Threat Program.
• Ensure that policy/law is able to be exercised to deter and punish offenders.


Misused Trust and Authorisation
An introductory Insider Threat Presentation
WFP
Humanitarian Aviation Webinar: AVSEC Insider Threats in Humanitarian Operations
Presentation Overview
Trust
Authorisation
What is Insider Threat?
Types of Insiders
Insider Characteristics and Motivators
Insider Threat Themes
Insider Threat Domains
Insider Threat Attacks
Insider Threat in Aviation
Deterring Insiders
Insider Threat Mitigation
Insider Threat Programs
Theories of Deterrence
Hypotheses of Prevention
Summary: Closure
Summary: What Now?
AEDIS