Insider Threat in the Art World
Theft of Art and Heritage Objects from Museums with Inside Help

Kim Covent[1]

Any museum employee with privileged access and knowledge can, in principle, steal or help steal an artwork or cultural heritage object. Insiders become a threat only when they are sufficiently motivated to use their abilities to attack the institution or its collection. This contribution aims to provide an overview of what we currently know about insider threats in the world of art and heritage crime and what we can measure. That is not much. We will then limit ourselves to the discussion of theft and leave other phenomena out of consideration. Through a number of historical and high-profile art thefts, we will discuss various forms of insider threats. We will describe the types of insiders and their motivations. Finally, we offer an initial approach to insider threat management based on a threat analysis linked to a non-exhaustive overview of preventive and repressive measures.

1 What is the Insider Threat in Museums?

An insider is any person connected to a museum institution with authorized access to and knowledge about the museum, the collection, and the artworks. An insider is (in principle) able to steal an artwork or cultural object or help an external accomplice do so. Every employee is an insider because they have exclusive access and knowledge. The insider only becomes a threat when they exploit their privileged access and knowledge to (help) steal art objects. Thus, the insider threat is the danger that museum employees or other persons with access and knowledge to the institution (maintenance, catering, security, transport) will abuse their privileged access and knowledge to steal art and cultural heritage.

This contribution is limited to managing insider threats from staff members connected to museum institutions and art theft.

2 Not In My Organization (NIMO)

In a recent study on insider threat awareness among Belgian security officers (Reveraert & Sauer 2021), nearly 10 percent of the surveyed organizations were not concerned about insider threats. In this study, insider threat was interpreted as *"the possibility that persons trusted by the organization with access to and/or knowledge about the organization's assets might intentionally misuse that access or knowledge to harm the organization."* This is a plausible definition that aligns with the definition we use above for the museum world.

The study showed that organizations fear the following internal threats: theft (61 percent), negligence (58 percent), and fraud/corruption (57 percent). Employees who spy (45 percent) or commit sabotage (40 percent) complete the top five (supra).

[1] Advisor, Local Police Department Ghent, Belgium

Organizations that carefully screen and select their staff (including intelligence services and nuclear institutions) and repeatedly emphasize high loyalty are often the ones who mistakenly believe that insider threats exist in other institutions but not in their own (Bunn & Sagan 2014). Insider threats exist in every organization! When organizations acknowledge the existence of insider threats but simultaneously reject that insider threats are present in their own organization, we speak of the Not In My Organization (NIMO) bias. From this, we must remember three lessons:

- Leaders cannot rely on their staff being so loyal that they will never pose an internal threat. Anyone can – under certain circumstances – change their ideology, reconsider their loyalty, or become an adversary for personal reasons. We must be wary of the halo effect, assuming that good employees are always reliable (the tendency we all have to positively judge a person based on one positive quality).
- Secondly, leaders must realize that security itself can be part of the internal threat. It is incorrect to assume that hiring more guards automatically leads to more security.
- Finally, Bunn & Sagan emphasize that leaders should not contradict or ignore the judgments and recommendations of security professionals solely for personal or political reasons.

We will reveal some recent results on the prevention of insider threats but will return to this later in the contribution. Ninety percent of respondents agreed that protecting the organization against insider threats is just as important as protecting the organization against external threats. Of all measures currently prescribed in literature, respondents were more drawn to non-disclosure agreements and background checks than to a contact point for employees to report suspicious behavior or conducting exit interviews (Reveraert & Sauer 2021).

2.1 Risk vs. Threat

We prefer to speak of insider *threat* rather than insider *risk*. Every employee is an insider with exclusive access and knowledge; it is only in exceptional and specific circumstances that the insider will pose a threat.

A risk analysis consists of weighing two important criteria: the likelihood that a (potential) risk will occur and the impact if it does occur. Risk management then involves increasing the likelihood and impact of positive situations and decreasing the likelihood and impact of negative situations. A threat analysis, on the other hand, looks at the vulnerable assets in the organization, the profile of potential adversaries, and the modus operandi they might use to attack successfully. We hope you will agree that we should base the preventive approach to insiders on the insights of a threat analysis rather than those of a risk analysis.

Furthermore, it is not easy to learn from previous incidents and the experiences of others. There are substantial organizational and cognitive biases (complacency and overconfidence in one's ability to identify and address potential insider threats) that lead leaders to downplay internal threats. Moreover, they often have limited information about incidents in other countries or sectors and the lessons that can be learned from them. This is further hampered by the secrecy surrounding the security measures organizations take to protect their assets (Bunn & Sagan 2017).

2.2 Art Crime and Zombie Statistics

The EU is a modest art market compared to the three largest markets – the United States, China, and the United Kingdom – which together account for 82 percent of the total global sales of art and cultural heritage objects (Munelly 2021). In its July 2020 report, *"The Art Industry and U.S. Policies that Undermine Sanctions,"* the U.S. Senate's Permanent Subcommittee on Investigations also considers the art industry the largest legal unregulated industry in the United States. In 2019, the U.S. was globally the largest art market, accounting for approximately 283 billion dollars or about 44 percent of global art sales (Grossman, Volkman, Lucas, & Ruiz 2021).

The traditionally secretive and under-regulated nature of the art market allows legal methods and legitimate actors to produce illegal money. The art market is therefore a low-risk, high-reward market for organized criminals, terrorists, and militias (Munelly 2021).

In the EU's 2020 Security Union Strategy, we read:

"The illegal trade in cultural goods has become one of the most lucrative criminal activities and increasingly serves as a source of funding for terrorists and criminal organizations. Steps must be taken to improve the online and offline traceability of cultural goods on the market and to better cooperate with third countries where cultural goods are looted. Active support must also be provided to law enforcement agencies and academic communities" (European Commission 2020).

However, the extent of art crime is unmeasurable. It starts with registration problems and underreporting, resulting in a large dark number that distorts statistics. Furthermore, the extent is almost impossible to express in tangible quantities of objects, currency, or social damage (Oosterman 2023). Statistics on art crime are indeed inconsistent, incomplete, and ineffective. The market is deliberately opaque about the provenance of objects, complicating data collection. The statistics also depend on which data is kept by the data managers and how. Uniformity in data collection is a problem for all national and transnational crime (Albertson 2020).

Erika Bochereau, Secretary-General of the Confédération Internationale des Négociants en Œuvres d'Art (CINOA), put it well: *"It is a trend also known as zombie statistics[2] – that is to say, information often cited by experts and institutions despite having no basis in research or reality"* (supra).

Some examples of zombie statistics:

- At the beginning of the 21st century, the American Federal Bureau of Investigation estimated that 4 to 6 billion dollars' worth of art was stolen worldwide each year.
- *"About 90 percent of art thefts from museums are internal thefts,"* said Special Agent Robert Wittman of the FBI at the Smithsonian Institution's National Conference on Cultural Property Protection in 2008 (Mandel 2008).

[2] Zombie statistics are so named because, although they are not based on official facts, they simply do not die.

- *"I often hear the statistic that 10 percent of all art in museums is fake. I usually respond by saying that 97 percent of all statistics are misleading"* (Charney 2017).

An internal FBI investigation from 1998 found that 83 percent of known museum thefts could be classified as *internal* thefts, committed by staff or persons with access to collections. However, we must take the 83 percent figure with a grain of salt as it refers to any internal involvement, whether direct or indirect, not just the act of theft. Moreover, these are solved art thefts, but we cannot claim that 83 percent of all art thefts were internal thefts (Kerr 2016).

3 Defining Insider Threat and Art Crime

Although we have few hard numbers on the nature and extent of art crime, there are sufficient indications that the insider threat in museums is significant. In this contribution, we limit the discussion of insider threat and art crime to staff members connected to museum institutions and the phenomenon of art theft. This means, however, that we exclude a range of phenomena (vandalism, fraud, forgery, arson, cybercrime, etc.). These may be the subject of a future analysis. A sample of these other phenomena:

- Vandalism: In 2022, a 60-year-old security guard in Russia drew two pairs of eyes with a ballpoint pen on a painting he was supposed to protect. Likely out of boredom. It was the valuable avant-garde painting "Three Figures" by Anna Leporskaya, exhibited at the Boris Yeltsin Presidential Center in Yekaterinburg. Initially, no report was filed as the damage was considered insignificant. Experts believed the damage could be repaired without consequences for the artwork. But when the Ministry of Culture complained to the prosecutor general's office about the lack of action, the police announced they had opened an investigation. The suspect was fired and faced a fine and up to three months in prison (Cain 2022).
- Forgery: The Toporovski case in 2018 revolved around the loan of art objects from the collection of two Russian collectors. These were exhibited in the Museum of Fine Arts in Ghent, after which significant doubt arose about the authenticity of the pieces. The works were seized, and the museum's then-director was temporarily suspended. She was convinced, after laboratory research supplemented by her own art historical research, that the works were real and authentic. After an internal disciplinary procedure and an investigation by Ernst & Young, the City of Ghent decided to terminate the collaboration with her (Peeters 2019).
- Employee Crime: Employee crime is slightly different. The victimization of companies where crimes against corporate assets are committed by employees in (large) companies mainly involves employees stealing money from their employer. The business sector does not provide clear insight into its figures, either, when it falls victim to employee crime, corporate fraud, financial and/or economic crime. Employee crime is a concept that dates back to the 1990s and must be complemented with newer phenomena such as workplace violence, terrorist crimes, and cybercrime (Cools 2016).
- Cybercrime: A global cybersecurity survey in 2022 calculated that internal cyber threats cost organizations $154 million annually, a 34 percent increase compared to 2020. Inattentive employees are responsible for 56 percent of these incidents (Proofpoint 2022). Against the phenomenon of cybercrime, very specific barriers are erected, and it

is best to invest additionally in security awareness among all employees of the organization.

4 Classification of Insiders

When it comes to suspicious disappearances of artworks, those with the most opportunity are the first subject of investigation: the insiders. But unlike employees with access and foreknowledge who commit crimes, staff members can also help prevent crime by successfully managing and supporting internal threat management (Kerr 2016).

4.1 Who are the Insiders in Museums?

There are different types of insiders. We first distinguish between accidental insiders and malicious insiders. Accidental insiders are people who, through a mistake or inattentiveness, unintentionally contribute to the theft of art objects. Think of information leaks, doors left open, or disabled alarm systems. A step further is the accidental insider who consciously (but without malicious intent) poses a threat to the institution by ignoring alarms or security procedures. Accidental insiders can be exploited or manipulated.

The art theft at the Isabella Stewart Gardner Museum in Boston was made possible by the unprofessional security behavior of two young art academy students. They had had only one week of training and were paid $6.85 per hour. On March 18, 1990, two men dressed as police officers showed up at a side door of the museum and called on security through the intercom. There had been a disturbance in the area, they said, and they had orders to check if everything was okay in the building. The guard believed them, ignored official guidelines, and opened the door for the two fake policemen. Within minutes, he and his colleague were tied up and gagged on the floor. The museum's security system didn't have alarms on individual artworks, allowing the two burglars to work at their leisure. For 81 minutes, they had free rein in the museum and were able to steal thirteen masterpieces, including paintings and sketches by Rembrandt, Vermeer, Manet, and Degas. Most experts estimate the value of the stolen works at over $300 million. The collection has still not been recovered (Butler 2000).

Malicious insiders pose an insider threat because they intentionally use their access and knowledge to harm the organization and thus are directly or indirectly responsible for the theft of art or cultural heritage. Malicious insiders can be recruited by external adversaries; they can be forced by adversaries to misuse their privileged access and knowledge against their will; or they can be intrinsically motivated. These insiders operate alone or in groups with other insiders or with outsiders.

We further distinguish between passive and active insiders. Active insiders can be further divided into non-violent and violent.

- A passive insider helps another (internal or external) adversary by providing information that can be used in a theft. A passive insider will not contribute in any other way and will likely end their involvement as soon as they risk being identified.

- An active non-violent insider can also provide information to other adversaries. But they go further: they use cunning and deceit to (help) commit theft. They do this by, for example, lying, falsifying documents, or removing and hiding art. An active non-violent insider will also avoid being identified.
- An active violent insider is also willing to use physical violence against others. Depending on the circumstances, an active insider can switch from non-violent to violent.

4.2 Motivations of Insiders

An insider can hold any position within the organization, from the highest to the lowest level. Insiders at all levels can be sufficiently motivated to pose an internal threat. Possible motivations are money, ideology, ego, collecting, revenge, coercion, or a combination of these reasons.

- The most obvious motivation is financial, where the insider is purely after monetary gain. There may be an underlying reason for this financial motivation, such as substance abuse or a gambling addiction.
- There is the ideological motivation, where the insider acts out of political or principled considerations.
- The ego trip or egocentric motivations are formed from the feeling that the insider is *smart enough* to pull it off.
- Specifically in the world of art and cultural heritage, greed and the desire to collect can be a motivation. The insider wants to keep the stolen objects for themselves rather than sell them.
- The revenge action or motivations formed by resentment or shame mainly occur among dissatisfied and disgruntled employees.
- An insider can be forced to commit an art theft by other (internal or external) adversaries through, for example, bribery, blackmail, extortion, or the threatening of family members.

4.3 Examples of Art Thefts (with Inside Help)

Below, we discuss some high-profile art thefts committed by (or with the help of) insiders. At the end of each example, we discuss which category these insiders belong to and what motives persuaded them to commit crimes.

Vincenzo Peruggia, 1911

Vincenzo Peruggia (October 8, 1881 – October 8, 1925) committed what we may call the greatest art theft of the 20th century. In 1911, Peruggia stole one of the world’s most famous paintings, the Mona Lisa by Leonardo da Vinci, from the Louvre Museum in Paris.

He was a former employee of the museum and knew how to easily enter and exit the building. On Monday, August 21, he entered the museum around seven in the morning through the door used by Louvre employees. The museum was closed to the public that day. According to his account, he wore the white smock that museum employees usually wore and was indistinguishable from other staff. When he was alone in the Salon Carré, where the Mona Lisa was hung, he lifted the painting from the four iron pins that attached it to the wall. He carried the artwork, which with frame and glass weighed about 90 kilograms, to a nearby service staircase. It is unclear if he worked alone or had help. The Mona Lisa was in a glass case that Peruggia, a former house painter and glazier of the museum, may have helped to construct. He removed the painting from the frame and hid the panel in his white smock. Peruggia then left the museum the same way he had entered. The theft was only discovered the next day when the French painter Louis Béroud noticed the bare spot on the wall in the Salon on August 22, 1911.

Peruggia hid the painting in a suitcase in his Paris apartment for two years. He then traveled to Italy and hid the stolen artwork in his apartment in Florence. Peruggia was caught when he contacted the owner of an art gallery, expecting a reward for offering the painting. The gallery owner involved Giovanni Poggi, director of the Galleria degli Uffizi, who authenticated the painting. They then notified the police, and Peruggia was arrested.

He claimed to have stolen the Mona Lisa for patriotic reasons, to return the painting to his homeland after it had been 'stolen by Napoleon.' He may not have known that Leonardo da Vinci had given the painting to Francis I when he moved to France to paint at the French court. This was in the 16th century – 250 years before Napoleon's birth. Experts doubt Peruggia's patriotism because he tried to profit from the sale instead of donating the painting to an Italian museum. The financial motive is also confirmed by letters Peruggia sent to his father.

The court somewhat agreed that Peruggia committed his crime for patriotic reasons and gave a mild sentence. He was sent to prison for a year and fifteen days but served only seven months. Peruggia became a national hero in Italy. Grateful Italians praised him as the Don Quixote of Italy. For months, the Mona Lisa toured triumphantly through Italy. In early 1914, the artwork was returned to the Louvre.

The news of the Mona Lisa's disappearance initially caused national mourning in France. Thousands lined up to see the empty square on the wall; visitors left flowers and notes. But mourning quickly turned to anger. It turned out that the Louvre had flagrantly lax security. Jean Théophile Homolle, the director of the Louvre, was traveling in Mexico when the Mona Lisa was stolen. He mocked the idea that the painting could have been stolen, thinking that at worst it was misplaced. He was dismissed.

Vincenzo Peruggia was an active non-violent insider who acted from an ideological motivation combined with greed. As a former employee, he had knowledge of the building, the practices in the Louvre, and the security. It is even possible that he helped make the glass protection for the Mona Lisa.

David James, 1983

The Chester Beatty Library, housed in the clock tower of Dublin Castle, is known for its rare and beautiful art objects from around the world collected by American mining engineer Sir Alfred Chester Beatty. This prestigious Irish museum mainly holds manuscripts and rare books. Today, the Chester Beatty is a research library for scientists from around the world.

Dr. David Lewis James (1941 – 2012) studied art at the University of Newcastle and did his postgraduate studies at the University of Durham in Arabic language and Islamic art, particularly miniature painting and calligraphy. In 1969, he was appointed curator at the Chester Beatty Library & Gallery of Oriental Art in Dublin, where he quickly gained a solid reputation in Islamic manuscripts and related arts. He wrote several important scholarly publications and some more popular articles in the 1970s and 1980s.

For fourteen years, James managed one of the finest collections of Islamic manuscripts in the world before succumbing to temptation in 1983. During that period, he was solely responsible for cataloging the library. James single-handedly stole hundreds of priceless ancient manuscripts from the Chester Beatty Library, which remains the largest insider theft in a cultural institution in Ireland. In the subsequent years, he meticulously erased his tracks. He used methods such as: loosening the binding of an antique Koran, removing a double page from the manuscript, and rebinding the book. He sold the manuscripts on the international art market in London for what is now worth millions of pounds. In July 1991, James was discovered by a series of coincidences (RTÉ 2011).

In 1992, James was found guilty by the Dublin Circuit Criminal Court of stealing art objects worth nearly £450,000 between 1983 and 1989. Most of this material was recovered by the Irish Garda with James's help, but a portion was reportedly destroyed in a warehouse fire in London. There is an RTE radio documentary about this insider called "The Caretaker," in which curator Charles Horton revealed that about 95 percent of the manuscripts stolen by David James were recovered, but the library is still searching for two missing stolen items (Burns 2011).

David James was an active non-violent insider who acted out of greed. As the only Islamic curator in this Irish cultural institution, he had unique access to valuable manuscripts and leading scholarly expertise on them.

Stefania Viglongo, 1998

On May 19, 1998, just after 10:00 PM, the prestigious Galleria Nazionale d'Arte Moderna in Rome was robbed. Three armed thieves entered the museum just before closing time. They walked barefoot through the galleries, wearing gloves and balaclavas to hide their identities. They stormed the control room, where they tied up and gagged two female guards. A third guard was forced to disable the museum's security system and hand over the corresponding camera footage. The three guards were then locked in a restroom.

The intruders targeted several works in the Impressionist hall. They ignored paintings by Edgar Degas and Gustav Klimt to focus on three specific paintings: "L'Arlésienne" (1889) and "Le Jardinier" (1889) by Vincent Van Gogh, and "Cabanon de Jourdan" (1906) by Paul Cézanne.

Italian investigators from the art crime unit suspected from the beginning of their investigation that the thieves had collaborated with an insider. Someone with first-hand information was familiar with the security system and knew who would be working in the museum that night. The police interviewed all 160 people working at the museum to identify potential suspects. Possible suspects were monitored, and their phones were tapped. Investigators gathered evidence and information for over a month about who might be involved, especially where the paintings were hidden. They learned that some suspects had met while serving time in a Brussels prison, where one was serving a sentence for a violent robbery of a postal truck.

Days passed, and the criminals struggled to find a buyer. Frustrated, they began bickering among themselves. One suspect was so careless that he openly complained during a tapped phone conversation that the police were onto him. The investigation also revealed that the paintings had been split up. “Le Jardinier” and “Cabanon de Jourdan” were in Rome after a failed sale attempt, while “L'Arlésienne” had been left in Turin, possibly as collateral for one of the accomplices (Albertson 2016).

After 48 days, investigators had gathered enough evidence to act. They searched the suspected hideouts for the paintings while simultaneously arresting all suspects to prevent anyone from moving or destroying the artworks to avoid prosecution. In total, eight people were arrested, prosecuted, and convicted. Among them was Stefania Viglongo; she was the insider in the museum and received an eight-year prison sentence.

Stefania Viglongo is a malicious insider. It is not entirely clear from the reports whether she herself committed acts of violence. It is possible that Viglongo was a passive insider who only passed on confidential organizational information. As far as we know, she was financially motivated. Her husband was also a member of the gang that carried out the armed robbery. In the absence of more information, we cannot rule out that she collaborated under some form of coercion.

Denis Wilhelm, 2017

In the early hours of March 27, 2017, a gigantic gold coin was stolen from the Bode Museum in Berlin. The gold coin, nicknamed Big Maple Leaf, weighed about 100 kilograms and had an estimated value of 3.75 million euros. The Canadian coin was stamped with the image of Queen Elizabeth II. There were only five such coins in the world, and it was the second-largest coin in the world.

Insider Denis Wilhelm (1999 –) was hired as a subcontractor for the night security of the Bode Museum a few weeks before the robbery. Between 3:20 and 3:50 AM that night in March 2017, three men dressed in black walked along the tram tracks parallel to the Bode Museum. They entered the building through the staff locker room. Within half an hour, the team managed to break the extremely strong security glass with a special axe. Creatively, using a skateboard and wheelbarrow, they rolled the heavy coin back to the locker room, dropped it on the tracks, and pushed everything to an adjacent park in central Berlin. A getaway car was waiting there.

Shortly after the robbery, Wilhelm suddenly showed interest in buying luxury cars and expensive jewelry. By digging into his past, authorities discovered a connection to Ahmed Remmo, whose family is part of one of Germany's most notorious crime networks. The burglars were quickly caught. The three men had walked their escape route several nights before the robbery, also dressed in black. The expert analysis of the size and posture of the men in security camera footage matched Ahmed and Wissam Remmo. The Remmo cousins had just finished high school but had already been convicted several times for minor crimes in the past.

The police did not expect to find the coin as they found gold dust on seized clothing and in more than one car. Investigators found a history of search queries on a suspect's phone about breaking down gold pieces. This supported the suspicion that the robbers had melted down the coin.

All suspects were tried and convicted under juvenile law based on their age at the time of the crime, according to German authorities. Ahmed and Wissam Remmo each received 54 months in prison. They were also fined for the estimated price of the coin, totaling 3.3 million euros. Their accomplice insider Denis Wilhelm received a 40-month prison sentence and a fine of 100,000 euros.

Denis Wilhelm was an active non-violent insider. As a night watchman at the museum, he had optimal access to the building and knowledge about the target. He acted purely out of financial motives.

5 Preventing Insider Threats

As stated, a threat analysis is the best tool to start insider threat management. The threat analysis provides an overview of the most vulnerable or attractive artworks in the museum and combines this with a detailed classification of possible insiders on the one hand and their modus operandi for a successful attack on the other.

The classification of the main insiders in the museum is a factual (but qualitative) overview of functions in the museum (but not of individual employees), where a value is assigned to their access, their knowledge, and the damage they can cause to the museum institution.

	(Qualitative)		*(Relative qualitative – score out of 5)*		
Function	***Access***	***Knowledge***	***Access***	***Knowledge***	***Ranking***
Head of Security & Facility Mgmt	*High*	*High*	*5*	*4*	***2***
Receptionist	*Low*	*Low*	*1*	*2*	***5***
Head of Collection Mgmt	*Medium*	*High*	*3*	*4*	***3***
Museum Director	*High*	*High*	*5*	*5*	***1***
Security Guard	*High*	*Medium*	*4*	*2*	***4***

Table 1: Classification of Insiders – Fictitious Example

The above fictitious example shows a top five of potential insiders in a museum setting. The most feared person is the museum director, followed by the head of security & facility management, the head of collection management, and then the security guard. Staff responsible for reception and administration, as well as maintenance personnel and subcontractors, rank much lower in this overview.

To obtain an overview of the possible modus operandi the museum should prepare for, scenarios are best used. Scenario development is done by a working group consisting of staff with different perspectives on the museum, the artworks, and current security. Various scenarios identify the specific actions a malicious[3] (passive or active) insider needs to take to commit a theft.

Credible scenarios consider the extent to which and the way opportunities are exploited. Since insiders can prepare actions over an extended period (while at work and having unlimited access to the building) and since actions do not necessarily occur in a predictable sequence, the concept of a path[4] or timeline is not always relevant for analysis.

5.1 Preventive and Repressive Measures

A museum has a range of possible measures to thwart an insider's plan. These measures aim to prevent, detect, delay, and respond to art theft. As with all security measures, it is advisable to implement them in multiple layers (the onion peel principle) and consider proportionality[5]. As the Chinese philosopher Confucius supposedly said: "Do not use a cannon to kill a mosquito."

The measures fall into two main categories: preventive[6] measures and repressive[7] measures.

Preventive Measures are all protective measures the museum provides to reduce the number of potential insiders before they gain privileged access and minimize the windows in which they can proceed to (prepare for) a theft. The possibility of an insider committing theft can be greatly limited by restricting or denying insiders access, knowledge, and information as much as possible.

- Preventive measures include the various actions a museum can take before employment: identity checks; verifying diplomas and references; reliability checks; and possibly extracts from the criminal record or other assessments – if national law allows it.
- During employment, when people have access and knowledge, it involves compartmentalization of tasks, access (keys, badges), and knowledge (need-to-know); logging of information systems and access doors; escorting through no-go zones; the four-eyes principle... These measures are supplemented with clear procedures, training, and awareness.
- Upon termination of employment, physical access to the museum buildings is withdrawn; a non-disclosure agreement can be used to protect sensitive information, and all keys, passwords, and access codes must be changed.

Repressive Measures are measures to detect or delay theft, respond to theft, or limit the consequences of theft. In this category, the theft has already started (beginning of execution). The physical security system deployed by the museum plays a role here. The probability of detection and the timing of response are quantifiable and form the basis of the effectiveness of these repressive measures.

[3] Scenarios for inattentive insiders are generally not developed, but nothing prevents this from being included in the approach.
[4] Path mapping is a security technique that attempts to show the path and timeline taken by external attackers.
[5] Proportionality means that there must be a reasonable relationship between the objective and the means used.
[6] Preventive measures are also called proactive measures.
[7] Repressive measures are also called curative or reactive measures.

- Detection measures: alarms and detectors, systematic analysis of video footage, checking access logs, conducting an unexpected inventory, and possibly deploying devices that indicate sabotage. Suspicious or unauthorized activities must be detected and investigated. They can indicate a reconnaissance or preparation phase. An insider may try to circumvent procedures, gain access to restricted areas, trigger alarms, or obtain sensitive information.
- Access control: must apply to a variety of situations, including control and distribution of key and lock combinations, registration of personal identification numbers... Access control rules must be defined for visitors and their escorts, as well as for abnormal circumstances such as emergencies, failures, and system breakdowns.
- Surveillance: to continuously monitor the activities of persons in areas where theft can occur; so that unauthorized activities are identified, reported, and assessed. Surveillance is useful not only as a detection measure but also for deterring (beforehand) and investigating (afterwards) attacks by an insider.
- Delaying measures: multiple layers of physical protection, including compartmentalization and separation of tasks, can add extra detection time. An example of such separation is making sure that the registration of new items is not done by the same person who labels and stores the item. Another form of compartmentalization is denying museum staff access to storage areas and transport staff to exhibition areas, for example.
- Response measures: compared to external adversaries, an insider is much harder to identify, so the response must be more nuanced. All staff members benefit from security awareness training. They should know how to report suspicious situations or behavior of colleagues. Finally, response procedures must consider the possibility that someone from the security or response staff could be a malicious insider.

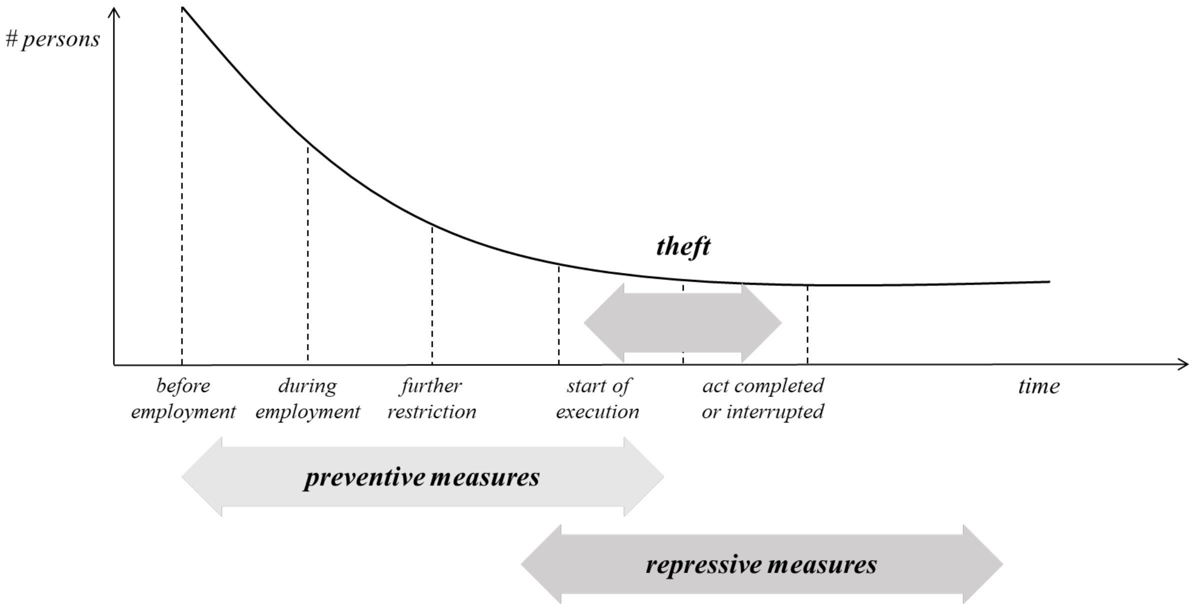

Figure 1: Implementation of Preventive and Repressive Measures Expressed on a Timeline

The timeline shows how the number of people who gain privileged access is limited as much as possible by measures during recruitment and task delineation. When an incident appears on the timeline, preventive measures set up beforehand try to prevent the execution of a theft, and repressive measures ensure that the completion of a theft is prevented or stopped as much as possible.

5.2 Evaluation of Measures

The effectiveness of preventive and repressive measures must be periodically reviewed, especially when changes are made to the threat analysis, the museum's operational functioning, or the measures themselves.

There are various methods to evaluate the effectiveness of security systems specifically designed to address insider threats. These include inspections and system checks, performance testing, quality controls, and scenario analyses. The implementation of preventive measures must be evaluated to ensure they achieve their designed purpose.

Referring back to the study among Belgian security officers (Reveraert & Sauer 2021), some interesting conclusions can be drawn from the respondents' survey. Some protective practices proved more popular than others.

The most popular measures (among more than 75 percent of respondents) include ensuring that employees only have access to the information needed to do their jobs, gauging overall job satisfaction, providing professional assistance to employees with personal problems, conducting exit interviews, and withdrawing access from employees who leave the organization. Semi-popular measures (between 74 and 50 percent) include conducting a threat analysis of internal threats, contacting references listed by future employees on their resumes, checking social media profiles during recruitment, establishing a point of contact where employees can report suspicious behavior of colleagues, and training employees to have the necessary skills to report internal threats. The least popular measures (among less than 50 percent of respondents) include checking social media profiles during employment, simulating internal threats, and applying a reliability check during recruitment and employment (Reveraert & Sauer 2021).

6 Conclusion

In this contribution, we limited the discussion of insider threat and art crime to staff members connected to museum institutions and the phenomenon of art theft. The other phenomena under the umbrella of art crime (fraud, forgery, illegal trade…) can be the subject of a future analysis.

Concrete figures on the proportion of internal thefts in art crime cannot be provided. Numbers are often reduced to zombie statistics, stating that 80 to 90 percent of (known and/or solved) art thefts involve an insider, directly or indirectly. Amounting to an annual loss of 4 to 6 billion dollars. Or not?

Accidental insiders contribute to theft without malicious intent, but because they make mistakes or are manipulated. Malicious insiders operate alone or in groups with other insiders or with outsiders. A passive insider will only pass on information; active insiders, on the other hand, will get hands-on. Depending on the circumstances, an active insider can switch from a non-violent to a violent approach. At every level of the museum organization, insiders can become sufficiently motivated to pose an internal threat. Possible motivations are money, greed, ideology, ego, revenge, coercion, or a combination of these reasons.

Insider threat management starts with a threat analysis. This provides an overview of the most attractive targets in the museum combined with a classification of insiders on one hand and their modus operandi on the other. The museum can then install preventive and repressive measures to prevent, detect, delay, and respond to theft by insiders.

Bibliography

Albertson, L. (2020). Understanding the chiaroscuro context of art crime and statistics. https://www.artcrimeresearch.org/2020/04/18/24813/ Retrieved on 18/03/2023.

Albertson, L. (2016). Museum Theft Galleria Nazionale d'Arte Moderna Rome. https://art-crime.blogspot.com/2016/09/may-19-1998-museum-theft-galleria.html?m=0 Retrieved on 18/03/2023.

Associated Press. (1991). Ex-prof sentenced in art thefts. AP News. https://apnews.com/article/dd0d5f1d1066b6011b55281689e2edf5 Retrieved on 18/03/2023.

Bunn, M., & Sagan, S. (eds.). (2017). Insider Threats. Cornell Studies in Security Affairs. [EPub] Ithaca, NY: Cornell University Press.

Bunn, M., & Sagan, S. (2014). A worst practices guide to insider threats: lessons from past mistakes. https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf Retrieved on 18/03/2023. Cambridge, MA: American Academy of Arts and Sciences, 32 p.

Burns, J. (2011). Atticus: Library puts the word out on its stolen manuscripts. The Sunday Times, 20/02/2011. https://www.thetimes.co.uk/article/atticus-library-puts-the-word-out-on-its-stolen-manuscripts-2sgr8x3gqgx Retrieved on 18/03/2023.

Butler, E. (2000). The art of the heist. The Guardian. https://www.theguardian.com/artanddesign/2000/nov/18/arttheft.art Retrieved on 18/03/2023.

Cain, S. (2022). Russian painting vandalized by ‘bored’ gallery guard who drew eyes on it. The Guardian. https://www.theguardian.com/artanddesign/2022/feb/10/russian-painting-vandalized-by-bored-gallery-guard-who-drew-eyes-on-it Retrieved on 18/03/2023.

Charney, N. (2017). The secret lives of works of art: What percentage of a museum’s holdings are likely to be fakes? Mutual Art | Salon. http://www.mutualart.com/ExternalArticle/The-secret-lives-of-works-of-art--What-p/D7AA63DB3ECF5D64 Retrieved on 18/03/2023.

Cools, M. (2016). Slachtofferschap van ondernemingen: wat leren de cijfers? In E. Devroe, E. De Raedt, H. Elffers, & D. Schaap (eds.) Meten is weten. Cahiers Politiestudies nr. 41 (pp. 169-177). Antwerpen/Apeldoorn: Maklu.

Cybersecurity & infrastructure security agency. Physical security. Insider Threat Mitigation. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation Retrieved on 18/03/2023.

European Commission. (2020, July 24). Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52020DC0605&from=EN Retrieved on 18/03/2023.

Europol. Crime areas. | Cultural goods crime. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/illicit-trafficking-in-cultural-goods-including-antiquities-and-works-of-art Retrieved on 18/03/2023.

Federal Bureau of Investigation. What we investigate. https://www.fbi.gov/investigate/violent-crime/art-theft Retrieved on 18/03/2023.

G4S. (2022). Insider Threat: Wat moet u weten? [Whitepaper] 16 p.

Garner, D. (2009). No smiley faces the day the lady left the Louvre. The New York Times. https://www.nytimes.com/2009/05/01/books/01book.html Retrieved on 18/03/2023.

Grossman, J., Volkman, E., Lucas, K., & Ruiz, G. (2021). New U.S. anti-money laundering laws and sanctions advisory impose compliance obligations on the art market. ARTnews. https://www.artnews.com/art-news/market/new-u-s-anti-money-laundering-laws-and-sanctions-art-market-impact-1234588194/ Retrieved on 18/03/2023.

Hickley, C. (2021). Art crime flourished during pandemic year, Interpol survey shows. The Art Newspaper. https://www.theartnewspaper.com/2021/10/20/art-crime-flourished-during-pandemic-year-interpol-survey-shows Retrieved on 18/03/2023.

Honan, W. (1991). The Trusted Museum Insider Who Turned Out to Be a Thief. The New York Times. https://www.nytimes.com/1991/12/19/arts/the-trusted-museum-insider-who-turned-out-to-be-a-thief.html Retrieved on 18/03/2023.

International Atomic Energy Agency. (2020). Preventive and protective measures against insider threats. IAEA Nuclear Security Series No. 8-G (Rev. 1) 52 p.

Interpol. Cultural heritage crime. https://www.interpol.int/Crimes/Cultural-heritage-crime Retrieved on 18/03/2023.

Kerr, J. (2016). The Securitization and Policing of Art Theft: The Case of London. London, UK: Routledge, 224 p.

Lafleur, J., Purvis, L., & Roesler, A. (2014). The Perfect Heist. Recipes from Around the World. Livermore, CA: Sandia National Laboratories, 107 p.

Maerevoet, E. (2017). Gouden munt van 100 kilo gestolen uit museum in Berlijn. VRT NWS. https://www.vrt.be/vrtnws/nl/2017/03/28/gouden-munt-van-100-kilo-gestolen-uit-museum-in-berlijn-/ Retrieved on 18/03/2023.

Mandel, S. (2008). Insider theft, fires, and vandals top list of museum concerns. ASIS Online. https://www.asisonline.org/security-management-magazine/articles/2008/06/insider-theft-fires-and-vandals-top-list-of-museum-concerns/ Retrieved on 18/03/2023.

Munelly, A. (2021). Compliant or complicit? Security implications of the art market. European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_23_2021.pdf Retrieved on 18/03/2023.

Nussbaum, P. (1991). Professor was a master in art theft. Chicago Tribune. https://www.chicagotribune.com/news/ct-xpm-1991-07-06-9103170215-story.html Retrieved on 18/03/2023.

Proofpoint Inc. (2022). Global Cybersecurity Study: Insider Threats Cost Organizations $15.4 Million Annually, up 34 Percent from 2020. https://www.globenewswire.com/news-release/2022/01/25/2372208/35374/en/Global-Cybersecurity-Study-Insider-Threats-Cost-Organizations-15-4-Million-Annually-up-34-Percent-from-2020.html Retrieved on 18/03/2023.

Oosterman, N. (2023). Wat is kunst- en erfgoedcriminaliteit? GRACE Studiedag. Kunst- en erfgoedcriminaliteit: een caleidoscoop van fenomenen (en hun gefragmenteerde aanpak). https://www.ugent.be/re/cssr/nl/onderzoeksgroepen/grace/watiskunstenerfgoedcriminaliteit.pdf Retrieved on 18/03/2023.

Peeters, T. (2019). Catherine de Zegher is niet langer museumbaas in Gent. De Tijd. https://www.tijd.be/cultuur/algemeen/catherine-de-zegher-is-niet-langer-museumbaas-in-gent/10100801.html Retrieved on 18/03/2023.

Povey, D. (2022). The dangers of money laundering within the art market. International Compliance Association | Insight. https://www.int-comp.org/insight/2022/the-dangers-of-money-laundering-within-the-art-market/ Retrieved on 18/03/2023.

Reveraert, M., & Sauer, T. (2021). Insider threat awareness and behavior: A survey among Belgian security officers. University of Antwerp, 93 p.

Roberts, S. (2022). Happy birthday to the man who stole the Mona Lisa and took it to Italy. The New York Times. https://www.nytimes.com/2022/10/07/arts/design/mona-lisa-vincenzo-peruggia.html Retrieved on 18/03/2023.

Ireland’s National Public Service Media. (2011). The caretaker. RTÉ. https://www.rte.ie/radio/doconone/2011/0217/646638-radio-documentary-chester-beatty-islamic-art-david-james Retrieved on 18/03/2023.

Shaw, E., & Sellers, L. (2015). Internal security and counterintelligence. Application of the critical-path method to evaluate insider risks. Studies in Intelligence, vol 59, no. 2. https://www.cia.gov/resources/csi/studies-in-intelligence/volume-59-no-2/ Retrieved on 18/03/2023.

Thompson, E. (2019). The Old-White-Malest of Crimes. Insider Theft from Libraries and Archives. Eidolon.pub. https://eidolon.pub/the-old-white-malest-of-crimes-e86571325bf3 Retrieved on 18/03/2023.