Nationaal Archief
Ministerie van Onderwijs, Cultuur en Wetenschap

CERL Security Summer School
4-5-6 September
University Library Tartú
Angela Dellebeke
National Archives of the Netherlands

Dealing with disaster: a network approach to collection security and salvage

When I first started working in the field of emergency preparedness with a focus on collection security I had yet to learn to look at the bigger picture. I thought it was obvious that the safety of the collection was equally important to all within the organisation. And although colleagues have a connection to the collection and know and feel it is important, we all approach it from different angels, for different reasons and we want different things from it.

Network within your organisation

Understanding which activities in the organisation (can) influence each other.

It is important to understand how departments/ colleagues are related in our daily work. Are there co-dependencies or opposing interest that involve the collection. For example: interests from the point of view of collection security might differ from colleagues working in exhibitions. Identify the internal stakeholders and hold regular meetings to discuss:

- Wants and needs assessment
- Options for cooperation
- Where needs meet / are the same and where to mitigate differences.

Also important is to connect your work to the mission/goals of your organisation. It is easier to get management support and interest if there is a connection between what you want/do and where the organisation is heading or wants to be. Look at your work in collection security in the bigger framework.
And... nothing is as helpful as an incident so make the most of them (although we all do everything in our power to prevent them from happening ☺)

External network based on the location of your organisation: the Governance zone

Integral cooperation in the field of safety and security within a specific geographical area (aka the governance zone)

Participating organisations share information on events that might influence measures of others within the zone. Think about important visitors that draw a lot of attention and/or a large crowd, events like concerts and exhibitions and demonstrations.

We invest in optimizing communication between all partners and in sharing best practices and doing table top exercises.
The National Archives of the Netherlands wanted to be part of this network because it is situated next to a large and busy train station in the vicinity of several government buildings and it will be the neighbour of Parliament for a couple of years as there is a huge renovation planned for their current facility.

Table top Exercise 2019
Method

- Explanation of the issue / scenario to the whole group
- Each group discusses within its own group their course of action
- Short presentation per group to all others present

Topics to address when discussing each issue/scenario:

- What is the effect of the issue on the partners in the group
- What are the responsibilities of the parties in the group
- In what way is the issue managed by each partner (coordination)
- How is information managed by each partner and amongst group members (information management)
- What are key moments and decisions for each partner and amongst group members (decision making).

Learning points

- ✓ Practice restraint: think before you act.
  Who or what will be influences by the incident but also by the actions you take?
- ✓ Are emergency services involved?
  This might affect your actions: e.g. in case of fire the fire department might have vehicles parked in front of your building
- ✓ Is Is there a chance of "follow-up danger" or problems expanding to other areas/organisations
- ✓ Identify what the critical moments are for your organisation and what you consider key- decisions.
- ✓ Are you aware of the critical moments of others and their key-decisions
- ✓ Situational awareness: are we all part of the same scenario?
  e.g. do we all know what is happening, why that is, what we need and can do

External network for heritage institutions in the city of The Hague: The Hague Prevention Network

To stimulate emergency preparedness, hazard mitigation and collection security ant to promote research into related areas.
To share experiences: do's and don'ts
To give support and lend a helping hand in case of emergencies (big or small)

What do we do within the network
Starting point of this collaboration was the development of disaster management plan.
Chair rotates every 2 years / 2 meetings per year

Projects
* Fire damage (with fire dept. and a research component)
* Water damage (due to heavy rainfall)
* Guideline: Theft in Archives
* First aid to collections: large scale exercises

Workshops/lectures
*Events and Collections
* Cultural emergency app
* Illicit traffic
* Packing objects for transport and security protocol during transport
* Water damage to paper collections with Van Gogh museum
* First aid to collections: small scale exercises
Best practices /experiences
* How do you react to.....

New: app group for alerts (deviant behaviour, theft etc.)
eg. girl with the pearl earring

Actual aid in case of an emergency : packing material, conservation advice, quick risk assessment

General support for policy making , awareness and funding within own organisation!

Guideline *Theft in Archives*
integral text

Preserving archives and collections is one of the primary roles of any archive institution. Theft and misappropriation represent important threats in this context. How can you prevent these? And what can you do when they happen?

The illegal trade in cultural heritage involves large amounts of money. Large-scale art theft, illegal excavations and looting all receive plenty of coverage in the media. Thefts from archive institutions and libraries are also frequent occurrences, but very little is published about them. In most cases, they only come to light much later. A significant portion of these thefts are committed by internal employees.

Archives and collections are increasingly becoming digitized. This means that your institution's digital security also needs to be up to standard. The information in this document is limited to the theft of physical items.

The information in this document provides general guidance for security measures and security policy, a prevention checklist and an action plan to apply in the event of theft and misappropriation. It offers a broad overview of the issues that you must or should consider but is in no way exhaustive. Much will depend on the individual situation. For most of the measures included, a limited budget should not be seen as an obstacle. Many issues can be solved by means of organizational interventions. The time and energy you invest in this will be more than worth the effort.

In brief: an integrated security policy

In protecting against theft, it is essential that all staff, in all layers of the organization, is aware of situations that involve risk. Equally, the institution itself must have developed strategies for dealing with these risks. The first major step in this process is to establish an integrated security policy. A policy of this kind not only makes theft less likely, it also reduces other security risks.

What is integrated security? In a nutshell, it means that there is a cohesive focus on security in the building, the people who work in it or visit it, the collection and the information systems. By way of example: protecting archives and collections against theft cannot be organized by the manager of the collector alone, but also depends on the building's security against burglary, something for which the collection manager is not usually responsible. This is what makes a cohesive and coordinated approach so important. It involves a collection of measures relating to the organization, the building and its electronic systems that raise security to the highest possible level.

So who is involved in an integrated security policy? Much depends on the size and internal organization of the institution. In any case, it will involve the management, the building management, collection management in all its forms, security, public services, HR and ICT – although in smaller institutions these positions and roles may possibly be combined. It is important for the integrated security policy to be formally established in a plan that has the support of the management. They have ultimate responsibility for the policy but its implementation is a job for the entire team. If the building itself is managed by another organization, this is a complicating factor. In that case, effective agreements need to be made with the department responsible for managing the building.

Whatever the case, the security policy plan must contain the following components.

- *General policy principles*

For example: we place great value on the safety and security of the people and collection in our building. We aim to offer our staff and visitors a safe and secure environment in which to work and study and strive to manage and make available our collection, physical or digital, in as secure a manner as possible.

- *Responsibilities and organizational aspects*

Responsibilities and organizational aspects not only focus on the security of the collection, but also the organization of such areas as the in-house emergency response, occupational health and safety and privacy.

- *Procedures and regulations*

Here are just a few examples, specifically focusing on the security of archives and collections.
◦ General access policy: who is allowed to enter and when? Is a distinction drawn between public and office zones?
◦ Access regulations on repositories: who is allowed access and when? Experience shows that there will always be a risk of internal theft. The fewer staff allowed access to repositories, the lower the risk.
◦ Procedures on security in the reading room: is there supervision? How many items is a visitor allowed to access at one time? What checks can be carried out to verify this? Bear in mind that regular visitors are just as great a risk as occasional ones.
◦ Procedures for access to materials in the collection during evacuations: what should reading room supervisory staff do in this situation?

- *Risk management and risk assessment*

◦ Do you have an accurate picture of the risks that your institution is running? What kind of incidents have you experienced? Keep a record of minor and more major issues (incident registration) and use it to provide a better assessment of the risks. This will enable you to take specific measures.

◦ Which archives, collections and individual items are at greater risk than others? Adjust the reading room regulations accordingly. Keep an eye on what is available in the antiques market, so that you are aware of changes in what the public is interested in and the associated risks of theft.

- *Collaboration and knowledge-sharing*

Do not base your decisions on your own experiences alone, but also share ideas with colleagues. Seek out contact with other heritage institutions that are willing and able to give advice on security policy. Actively share your experiences about incidents with fellow institutions so that they too can learn from them.

Checklist for preventing theft

This checklist is intended to prevent theft and takes the form of a questionnaire. Most of the questions are accompanied by guidance on prevention measures and notes to make answering the questions easier.

It is not possible to provide 100% protection against theft. However, if you can answer 'yes' to all the questions in the checklist, you can safely assume that everything possible has been done to make theft from the archives and collections more difficult. If a theft has taken place, the checklist can help you to identify it quickly. For the purposes of evidence, it is important to discover as quickly as possible if a document is missing in order to draw a direct connection between the document being consulted and the person who consulted it.
If you cannot answer 'yes' to all of the questions in the checklist, the 'no's will form a list of opportunities for improvements. In this, it is up to you to decide which measures you will take. The result will be a customized plan of approach based on a risk analysis that takes account of the value of the items, the existing system of security measures and the service philosophy of your institution.

CHECKLIST

Have all components in the archives and collections managed by your institution been described?

A comprehensive description of the archives and collections facilitates accessibility and provides proof that these documents are actually being managed by your institution.

If not, do you restrict access in the reading room to archives or collections that are not described or only in very global terms?

If the content of archives or collections is not known or only in very global terms, it is not possible to determine if documents are missing. If the maximum number of items that can be consulted is limited, supervision is more effective.

Are you aware of which archive items and objects from the collections are at particular risk of theft because of their value?

This may relate to the proceeds made from a sale, but also the value to a collector or private individual. Find out what antiquarians and auction houses have to offer and at what price.

If so, do you restrict access to risky items/objects?

If risky items are consulted in the reading room, designate a very visible location for this. If possible, make copies available rather than originals.

Do you register visitor information?

You can use this to demonstrate which visitor was in the reading room. When registering visitor information, make sure you take account of the rules on personal data protection.

Do you register which items each visitor consults?

A register of this kind is useful if something is missing in order to check when and by whom the item was most recently consulted. This enables you to determine more effectively the time and circumstances of the item going missing.

Do you have regulations for the reading room?

If you have clearly-defined rules, it also makes it possible to enlist the help of the police at an early stage. Rules could include a ban on bringing in coats, bags, notebooks, etc.

Do you apply a maximum for the number of items that can be consulted simultaneously?

A maximum limit makes it easier to manage supervision of the items.

Do you check archive items and collection objects before they are consulted and after return?

Use a set of scales in the case of collections of several items. Numbering (with a pencil) of items liable to theft makes it easier to check for completeness.

Is there permanent supervision in the reading room?

Supervision can be interrupted if the reading room employee also has to collect items from the repository and answer visitors' questions. If there is no permanent supervision, consider limiting the number of items that can be viewed each time.

Are reading room staff trained to identify unusual behaviour?

This concerns behaviour that is different from what you would expect from someone visiting a reading room. For example, you can have staff take a course in predictive profiling, enabling them to learn to recognize unusual behaviour and call visitors to account for it.

Are visitors' writing equipment and laptops checked when they leave?

Include in the reading room regulations the power to inspect people's personal property. This could include checking documents, notebooks, files, pencil cases etc.

Is access to the repository restricted?
Ensure that only staff whose duties require it have access to the repository.

Do you have a procedure regulating how staff take items from the repository?
Do you also have a procedure for dealing with items at the staff workstations?

Have you had a background check run on the staff you employ?
Examples of this include a Certificate of Good Character. Do not forget volunteers and interns.

Have the staff completed integrity training?
Make sure that the integrity training focuses on the situation in your institution and is part of a wider security policy. Integrity is all about standards and values that, together with customs and habits, form the culture of an organization. The culture is also often set out in a code of conduct.

Do you record incidents in a (central) database?

Do you have contact with the police officer in your local area?
If your local police officer is familiar with your organization, this might make cooperation with the police in the event of theft easier.

Have you drawn up a list of missing items and is this kept up-to-date?
The fact that items are missing can be discovered when they are requested and consulted. This may not necessarily involve theft. The items may simply have been incorrectly stored away or replaced.

Do you conduct (location) checks in the repository?
You can also identify missing items by conducting a regular random check in the repository to verify that all items liable to theft are present and complete.

Theft and misappropriation in your organization: what should you do?

It is important to determine in advance who in your organization is responsible for what if an incident occurs. Make sure you know if and when you are permitted to apprehend someone if you suspect this person of theft or another illegal act (e.g. misappropriation or vandalism). Ensure that all staff are prepared and know what is and is not permitted when apprehending a suspected thief. A protocol for theft provides staff with the necessary guidance in a tense situation of this kind. Make sure you are aware of the rights that you have when apprehending a person. The applicable legislation in your country will be the decisive factor in this.

When apprehending someone, what factors should you consider?
If you detain or apprehend someone, you are depriving them of their liberty. That

person is unlikely to be happy about it, whether guilty or not. It is therefore important that you agree on following a procedure for this. Please take the following points into account.

1a. Caught in the act

◦ Always consider your own safety and that of staff and visitors.
◦ Apprehend a suspect only if you intend to report the matter.
◦ Be polite at all times: it could be a mistake.
◦ The person being apprehended can suddenly start panicking. Remain calm but convincing.
◦ Do not use violence and avoid physical contact.
◦ Allow just one person to tackle the suspect but ensure that a colleague is nearby to help if necessary.
◦ Introduce yourself to the suspect, citing your name and position.
◦ Tell the suspect what you have seen – without mentioning theft – and ask them to accompany you voluntarily to another room to discuss the issue.
◦ Clearly and calmly explain the procedure you are following. Explain that more detailed discussions about guilt or the particular circumstances will need to be conducted with the police.
◦ If the suspect refuses to accompany you, you can apprehend him or her there and then.
◦ Make sure that the police are then called immediately.
◦ Avoid removing any evidence that may be useful for the investigation: for example, do not return any confiscated items to the repository before the case has been dealt with.
◦ Make sure any witnesses are available/stay in the building for the police and note down contact details.
◦ Consider in which room you intend to wait with the suspect for the police (visible/not visible to the public).
◦ Keep the suspect in sight at all times (do not let him/her go to the toilet) in order to prevent them from concealing stolen items.
◦ Keep a close eye on the suspect's behaviour (aggression, fear).
◦ Hand the suspect over to the police when they arrive.

1b. Reporting incidents to the police

◦ Always report incidents to the police, even after an event has already occurred.
◦ Always complete a form to report theft/misappropriation at the address of your institution and not at your personal address. Issue a verbal report (at the police station), especially if it appears to be a major case.
◦ Go through the report form with the police to check if it is complete and accurate.
◦ Always keep a copy of the report form.

1c. If you made a mistake...

◦ Offer your sincere apologies.

◦ Explain the reason for the misunderstanding.
◦ Think of how you would like to be treated.

2. Theft/misappropriation after the event ...
◦ Always report incidents to the police, even after an event has already occurred.
◦ See 1b and the points following it.

3. Collecting information
◦ Document all activities and the chronology (sequence in time) of the actions taken: write everything down.
◦ If possible, take photographs or make video recordings.
◦ Ensure security camera footage is secure.
◦ Collect relevant information about the missing objects; such as lending details, photographs, scans, distinctive characteristics, stamps, photocopies.
◦ Decide whether to hire someone to conduct an investigation (private detective, investigation team).

4. Communication
◦ Make sure you have a designated spokesperson.
◦ Notify the management, the board, etc. and if the item was on loan, immediately inform the lender.
◦ Do not deny any information that is already known (e.g. people have seen someone being escorted away by the police).
◦ Notify the staff.
◦ Think about instructions/rules for staff use of social media.
◦ Inform the media if desirable or necessary.
◦ Consult with the police on how to present the news.
◦ Do not make any statements on the security of heritage within your organization. Keep to the facts. Do not be tempted to jump to conclusions and instead refer to the police investigation.
◦ Be prepared for further questions about the financial value of the stolen archive items/objects. It is recommended that you focus on the cultural and historic value, the importance of the items for the collection and their importance for society. Do not be enticed into making statements: consider in advance what message you wish to convey.
◦ Consider also notifying institutions that have similar collections.
◦ Consider also notifying institutions in the trade (antiquarians).

5. Impact and after-care
◦ Discuss the incident with everyone involved:
  - build up a picture of the actual impact of the event;
  - take stock of what went well and what needs to be improved;
  - investigate whether this is a one-off incident or a structural problem;
  - check if you need to modify agreements or procedures.
◦ Provide after-care to anyone involved who might need it.
◦ Also think of after-care for the organization as a whole: e.g. implementation of the code of conduct/house rules, awareness-raising

activities, integrity training.
◦ Think about such issues as buying back materials, looking through the catalogues of antiquarians and auction houses, contacting the local trade.

Who might you have to deal with?
When an organization faces an incident, it is worth bearing in mind that more people or institutions may be involved then you realised before dealing with the incident. The list below contains examples of parties that can play a role in an incident, voluntarily or otherwise.

- Antiquarians and art dealers
- Auction houses
- Enforcement agencies:
  - Cultural Heritage Inspectorate
  - Public prosecutor
  - Government organizations
  - Police/investigation team
- Executive Board
- Government organizations
- Lenders and depositor:
- Local municipal executive
- Management and staff of the organization
- Media (newspapers, radio and television)
- Private detective agency
- The thief's associates (family members, friends)
- Social media (Twitter, Facebook, Instagram, LinkedIn)

Practical examples

Who did it?

In the event of internal thefts, it is easy to conclude 'that the cleaners or security staff must have done it'. In many controversial cases, the culprits turn out to be colleagues who have worked at the institution for more than a decade and often hold key positions. They know the collection and have easy access to it. They know what the special items are and what value they have. They also know the channels for selling them.
Private circumstances can play a role, including relationship problems or debts. But there have also been cases where employees have stolen collection materials after a conflict at work or because of frustrated ambitions.

The reliable visitor

In one of the European national libraries, an English-speaking visitor approaches the staff in the reading room with a banknote worth around € 25 that he claims to have found in the reading room. Several days later, it turns out that this friendly man has stolen several valuable maps from atlases.
Never judge on first impressions: this nice, honest-looking visitor is actually just as likely to be a thief as anyone else. The same applies to regular researchers in the archive. There is no reason to apply different rules to them than to occasional visitors.

Theft of maps from atlases

A visitor in the reading room in the National Library of the Netherlands spends days requesting 16th to 18th century atlases. After a few days, his unusual behaviour starts to attract attention (looking around a lot, less focused on study, regularly walking out of the room, somewhat nervous). Supervision is intensified, after which he disappears. When checks are carried out, it appears that dozens of maps are missing. In most cases, it is not possible to determine whether they were stolen now or were already missing. Enquiries reveal that this visitor has also stolen maps from other libraries.
Theft of maps from atlases is an international problem. Map theft continues to be reported regularly in large and small institutions.

Personal property?

A visitor in the reading room at the National Archives of the Netherlands finds letters and photographs from deceased family members in a government archive and decides to take them with him. At the exit check, the material is discovered by the supervisor/security officer. When confronted with the find, the visitor

admits realizing this is a crime, but feels that the letters and photographs are private property that belong in the family home.

Misappropriation
On the shelves of an antiquarian, an employee from the University of Amsterdam's Special Collections Department discovers a series of interesting wedding poems. On his return to work, he googles the names of the families in the poems. He finds the poems in the inventory of a family archive that is kept in the Amsterdam City Archives collection. He calls the City Archives and they discover that the poems are no longer located where they should be in the repository. Because the antiquarian has the details of the person who sold the poems, it quickly becomes clear that it was a City Archives employee. Personal circumstances have led him to resort to this way of gaining extra money.

Inadequate registration details
It is believed that a member of staff who worked on a topographical historical atlas in a medium-sized city archive regularly returned after work in order to steal valuable prints and maps. It is believed he had been doing that for years on end because of frustration about his position at the archives and because of greed. The stolen goods were sold to an Amsterdam antiquarian. The archives reported the incident and a court case followed. Because the suspect denied guilt and there was no conclusive evidence of theft, the case was dismissed. The registration of the missing items was inadequate.