IJDC | *General Article*

# Secure Data for the Future: A Risk Assessment

Bendik Bryde
Piql

Roberto González
Piql

## Abstract

The guarantee of secure and authentic future access to any digital data is a big worry to those who work with data now and those who are responsible to keep it accessible for the future. There are a wide range of threats to digital data that these people should need to take into consideration. The project PreservIA had the goal to assess the risks of using analogue 35mm film to store and preserve digital information and define its strengths and weaknesses for long-term secure preservation of all kinds of digital data.

The research project was examining the application of the Piql technology to ensure the security, integrity and authenticity of the information stored on a unique storage medium. PiqlFilm has been designed for a life span of 500 years or more and the research tries to assess how well this solution could maintain the authenticity and availability of the information, independently of internal and external changes in the surrounding environment over time.

The research project has been designed using a scenario-based approach and the morphological method of scenario development is used to define a set of scenarios covering the risks to the service.

The scenario classes used were accident, technical error, natural disaster, crime, sabotage, espionage, terrorism, armed conflict and nuclear war. A scenario template has been included for the purpose of describing current and future scenarios. The final scenario analysis identified potential vulnerabilities.

The paper shows briefly how Piql Preservation Services holistic preservation approach perform the work, defines a methodology to select the scenarios for the assessment and then studies the vulnerabilities and security challenges of the solution on those scenarios. The project also includes a comparison of other existing storage media to evaluate their robustness to the addressed scenarios in relation to Piql technology.

*Received* 20 January 2018 ~ *Accepted* 20 January 2018

Correspondence should be addressed to Roberto Gonzalez, Gronland 56 3045 Drammen Norway. Email: roberto.gonzalez@piql.com

An earlier version of this paper was presented at the 13th International Digital Curation Conference.

The *International Journal of Digital Curation* is an international journal committed to scholarly excellence and dedicated to the advancement of digital curation across a wide range of sectors. The IJDC is published by the University of Edinburgh on behalf of the Digital Curation Centre. ISSN: 1746-8256. URL: http://www.ijdc.net/

 doi:10.2218/ijdc.v13i1.665

# Introduction

Digital Preservation is a set of processes and tasks to ensure the access and use in the future of any kind of digital assets created now or in the past (Termens, 2013). We could consider long term from different business perspectives but 25, 50, 100 years or even more is a very realistic need for the conservation of digital data (Academy of Motion Picture Arts and Sciences (2007).

There are many challenges when long term preservation is on the table, and they can be separated into two main areas: physical preservation and logical preservation. The first refers to reliability, affordability, sustainability and efficiency of the physical media used to archive data (storage media). The physical and chemical stability of the recordable medium where data is stored is the core of the problem of long-term digital archiving (Plata and Bjerkestrand, 2012; Spitz Hourcade and Laloë, 2010).

The second, logical preservation, refers to three aspects that must be covered and solved: the ability to recover the bit stream from the physical media regardless of its degradation or hardware obsolescence; the ability to understand and use the digital data despite changes in data formats or software applications that interpret and render the data; and finally, the ability to describe the data to ensure its integrity and authenticity.

The OAIS model (CCSDS, 2002) was created years ago to address this challenge and ensure the availability of the digital data with identical properties and content as the ones who made it originally. One of the prerequisites has been a need for a continuous migration process that involves not only the data but all the information that describes it.

Data migration is now the most frequently used preservation technique and it is based on copying the data and information unlimited number of times from one medium to a new generation medium and from one file format to another. The main risk of this strategy is the danger of data alteration during the process that could lead to inaccuracy, incompleteness or a lack of integrity of the original data to be preserved. An additional issue is the continuous need for funds to achieve preservation goals, as periodic tasks must be performed. This technique serves the two areas, physical and logical.

An alternative approach has become emulation. It is based on the data preservation on the original media, providing tools to avoid the hardware/software obsolescence. With this tool, the old systems could work on new hardware and the user experience would be the same as that of the old hardware. As this technique is mostly focused on the logical area, the existence of a long term stable storage medium would be very helpful.

Finally, a third option emerges as an alternative to migration or emulation: the use of open technologies and standards to mitigate the impact of technology obsolescence. Open technology is the best to be preserved, as full description of formats and code are available and can be archived with the data.[1]

In this context, Piql has worked on different projects (Piql, 2015) in consortium with main technology leaders of different industries to develop a reliable, secure and cost effective long-term preservation solution that was first presented to the market in 2014. Additionally, and included in its continuous improvement vision, Piql launched the PreservIA project together with Norwegian Defence Research Establishment (FFI) to

1 See the Storage Networking Industry Association (SNIA): http://www.snia.org

improve the technology based on piqlFilm, a 35mm nano-film, to ensure the security, immunity and authenticity of the digital data stored on it.

The work presented in this paper was focused on performing a risk assessment of the Piql services, to identify its potential vulnerabilities and security challenges and let Piql solve or decrease them, allowing the users of Piql services to save resources and to avoid the risks of a migration scenario. As a side product of this project, FFI (Norwegian Defence Research Establishment) has developed a whole assessment guide that could help the users of preservation services to verify its own security issues and solve them in a structured manner.

Identified risks will be analysed according to their effect on the confidentiality, integrity and availability of the preserved information. As the time frame for this assessment is 500 years, it is simply impossible from a scientific point of view to predict what changes our world will go through in that time. We have therefore dealt with trends and events we can perceive today. Note that the term 'risk' (rather than 'threat') includes both intentional acts and unintentional events.

## Preservation Services

The Piql Preservation System is a complete end-to-end approach for ultra-secure data storage and long-term preservation of digital data, that ensures data's authenticity, immunity and security for a timespan of more than 500 years (Piql, 2015).

The system includes different components that are shown on the Figure 1 as well as software tools in compliance with the OAIS model.

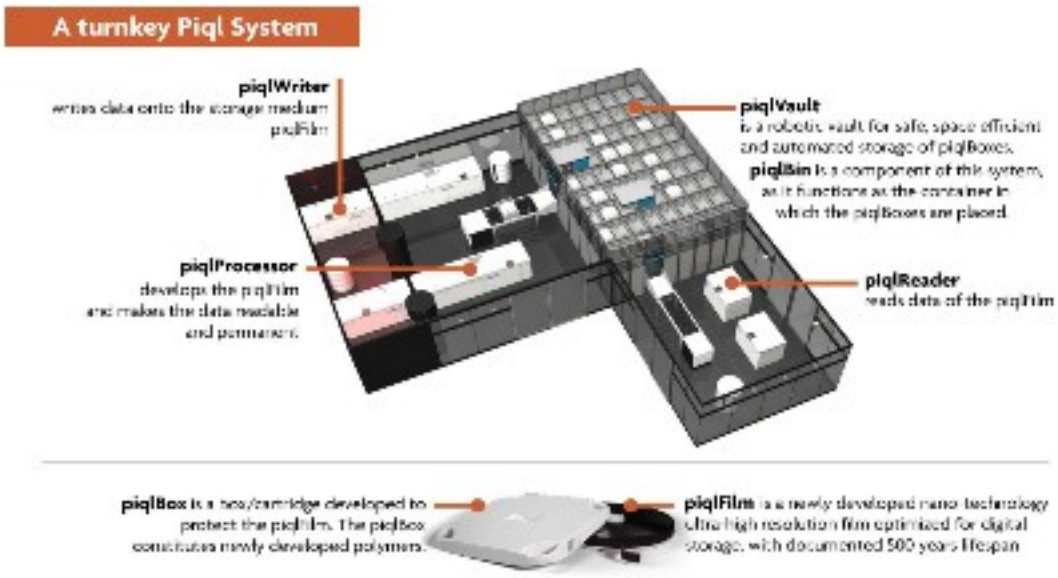


**Figure 1.** Piql system.

The services provided by this system reach the market through selected Piql partners located around the world. Every such partner delivers these services to multiple data-owners in need of either ultra-secure data storage or long-term digital preservation across sectors and industries.

 doi:10.2218/ijdc.v13i1.665

To gain a proper understanding of the Piql services, it is useful to go through the service journey (Figure 2) step by step to understand how digital information ends up on a piqlFilm in a secured storage facility.

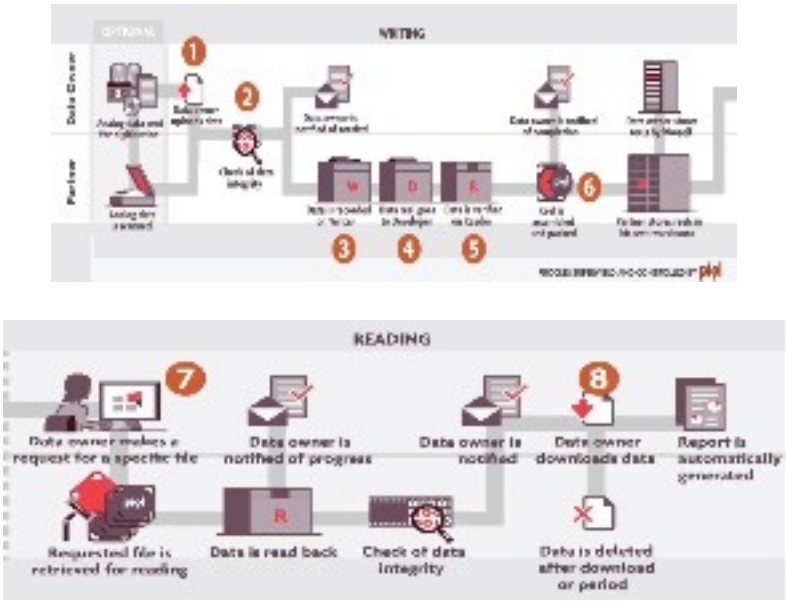


**Figure 2.** Writing and reading workflows.

1. The service journey starts with born-digital or digitized data being sent to Piql by a data owner. This delivery can be done online or through offline transfer with secure methods.

2. When received, integrity checks are performed to make sure that the data was not altered during the reception, and that no viruses are transferred into the Piql system. The received data then goes through a preparation process with two purposes:

    a) to collect relevant metadata to enable future access to the data and to encode both the data and metadata into the Piql system storage format, comprising a single file;

    b) to provide the data owner with three choices: digital, visual or hybrid preservation of the data.

3. The data is then sent to the piqlWriter where it goes through yet another integrity check before being written to the piqlFilm. The piqlFilm is manually loaded into the piqlWriter by an operator who does not access the computer and thus the original file.

4. Once written, the piqlFilm is sent to processing. The content is then verified with the piqlReader.

5. Once verified, the original data is deleted from the computer system, and the piqlFilm is transported to a secure offline storage facility.

**Reading Procedure**

1. Metadata from each individual piqlFilm is stored in an online database, where the data owner can search for any specific file and request retrieval.
2. Upon request through the online client interface, the piqlFilm is sent for retrieval using open-source reading technology,
3. The retrieved data can be delivered to the data owner either electronically (through a client interface, an integrated digital management system or a file transfer service) or in a physical form (e.g. hard drive).

The information stored on piqlFilm is self-contained. This means that regardless of available software or technology in the future, the data can always be retrieved.

Instructions on how to retrieve the data is written in human readable text at both the beginning and the end of every reel of piqlFilm. If the data is written in visual format, all you need, in theory, is a light source and a magnifying lens and you will be able to read it immediately. If the data is written in digital form, you also need a camera (a capturing device) and a computer (to decode the digital frames). Instructions on how to decode the frames back to readable files is included in the retrieval information mentioned earlier. Software to interpret and render digital data is written on the film to ensure the use in the future, if open technologies are used. When proprietary tools are mandatory, all the available information is written on the piqlFilm to ease future users in their interpretation, but when possible the use of public formats, standards or open source software is recommended.

## Scope of Project Report

Risk assessments are a method to better manage risks; to be made aware of the threats and vulnerabilities towards our objectives makes it possible to put appropriate security measures in place. Moreover, the security parameters surrounding the storage site can also be recommended to end users. Value-oriented thinking is essential to this risk assessment and understanding the relationship between value, threat and vulnerability. To implement appropriate security measures, it is necessary to be aware of the multitude of assets that will require protection, i.e. the type of information and the corresponding sensitivity of that information.

This could vary greatly: for instance, military graded information is a lot more sensitive than a company's accounting records. The security level surrounding the preservation services would vary in equal measure. The intrinsic value of the assets will suggest what kind of threats they face and thus what their vulnerabilities are.

This risk assessment consists of three stages:

1. **Risk identification:**
    a) mapping the object of analysis (the Preservation Services)
    b) finding and describing corresponding risks

 doi:10.2218/ijdc.v13i1.665

2. **Risk analysis:**
    a) finding which intentional or unintentional threats/hazards are relevant to the different value-levels of the assets written on the media
    b) the vulnerability of this value against said threat/hazard
3. **Risk evaluation:**
    a) determining the level of risk
    b) identifying security measures to reduce the harmful effect on the Preservation Services.

The processes or objects of study included in this assessment are:

1. The production phase
2. The storage phase
3. The structures surrounding and connecting these objects
    a) transportation between production site and storage facility
    b) the operational processes of running the automated storage facility.

## Scenario Definitions

Due to the scale of the object of analysis – the Piql Preservation Services, with all three components (film, box and vault) and the complexity of the service journey – it became apparent that a simplification of the subject matter was required to enable an adequate scenario development process, which in turn would lead to a meaningful scenario analysis relevant to this study. Accordingly, we were obliged to make certain standardised assumptions about the present and future application of the Preservation Services for this assessment.

We made clearly defined classifications for the categories geography, time-frame and user class, described in the next points.

### Geography

Piql Services is a global organisation, and to divide the geography into more manageable groupings, the three geographical zones operated within this assessment are North, Middle and South. This division is based on the following classifications: climate, development level and political stability. Climate was chosen as the main classifier, as it is deemed to be the most stable indicator over time, even considering climate change. Together these three indicators give an adequate description of the characteristics of a country.

### Time Periods

With a longevity of 500 years, if not more, of the components of the Preservation Services, the time perspective of the risk assessment in this project is a lot longer than normal. In fact, it is too long to be relatable. Consequently, we have created two time periods to use in the scenario development: one short-term and one long-term. The classification is again based on the users' needs, in this case how long we imagine a user would have need of the information which is stored. It was natural, then, to set the short-term period from 0 to 30-50 years. This is the length of a person's career, and thus signifies the amount of time they can imagine needing access to information. We presuppose that the same goes for a business, as things will have evolved and changed quite a bit during this time, perhaps to the point of making the information obsolete. Any need to store information beyond this short-term period we presuppose is for the preservation of the information for future generations. For instance, there is the need to preserve the cultural and historical heritage of a society, or the need to preserve original data for future research with new methods and ways of thinking. This long-term period is set from 50 to 500 years.

### User Class and Asset

As our working-perspective in the report is user-oriented, the user group classification needs to be as accurate as possible, yet it is one of the most challenging ones to define. The Preservation Services are available to any entity in any sector or industry in the world in possession of critical data requiring archiving and long-term preservation. This includes enterprises or bodies functioning in modern society, both private and public. Attempting to make a complete list of all these entities is near impossible. For the purposes of this report, the levels of sensitivity are divided into five groupings, outlined in table below.

**Table 1.** Levels of sensitivity.

| Category | Description |
|---|---|
| Public highly sensitive | Classified or confidential information, as specified by national acts on protective security services (The Security Act, 1998). |
| Public sensitive I | Information exempt for public consumption, as specified by national regulations governing access to documents in the public administration (The Public Procurement Act, 2006). |
| Public sensitive II | Proprietary information, as specified by national regulations governing the management of information in need of protection for other reasons than those mentioned in the national act on protective security services, including regulations (Protection Instructions, 1972). |
| Business sensitive | Business confidential or proprietary information, as specified by the individual enterprise. |
| Public sensitive and business sensitive | Personal data, as specified by national acts regulating the processing of personal data (Personal Data Act, 2000). |

 doi:10.2218/ijdc.v13i1.665

### Location and Description of Storage Facility

Giving a description of the piqlVault and its surrounding environment that is accurate, precise and which reflects the way Piql AS envisions the implementation of the Piql system is an important step of risk identification, which will in turn allow us to give meaningful results in the analysis and evaluation phases. Of course, such a precise and realistic description of a piqlVault and its surroundings would vary greatly between countries and between sectors.

### Safety and Security Requirements

As the design and layout of the storage room used for analysis is described, it is possible to specify which safety and security requirements are built into the storage facility.

## The Scenario Template

The purpose of developing a scenario template to help with the process of scenario description is twofold. First, it will enable thorough analysis of a greater number of scenarios: a risk assessment of this scale necessitates a wide range of scenarios covering a wide range of possible security challenges and vulnerabilities threatening the Preservation Services. Second, it will provide ease of use for interested parties at later stages. As this report is part of a larger project, it is meant to be used by the Consortium partners in later work packages. The template used is described in the Appendix to this paper.

## Presenting the Scenarios

The scenarios analysed in the report cover 12 security situations. These 12 situations include chemical accidents, fire inside of the production plant, natural disasters (floods, forest fire, earthquake), theft with insiders involved or performed by crime organisation, sabotage, espionage, terrorism, armed conflict and nuclear war. These scenarios are fully described in the final report and detailed in the Appendix to this paper.

## Recommendations

General recommendations on security measures are made so that the Preservation Users can keep the piqlFilms they store as protected as possible. However, it is important to remember that there is no “one size fits all” in this matter. Different geographical settings, market areas, sectors and level of sensitivity play important roles, so it is up to the individual users how to prioritize the risks uncovered by this assessment. Additional recommendations are then made for the Consortium partners to consider alterations to the Piql components, which they may decide to implement in future versions.

### Recommendations for General Security

A general rule of information security is to always keep backups. One should therefore request more than one copy of a piqlFilm, and they should preferably be placed in different locations. Another general measure to employ is to preserve the information

using the hybrid method, i.e. both as visual text/images as well as digital. It has previously been stated that the piqlFilms are at their most vulnerable during transportation. Changing the transportation route from day to day would make it more difficult for a threat actor to stage an assault, but having the production site at the storage facility would remove the entire risk altogether.

The insider threat was highlighted as one of the biggest security challenges the Piql Systems faces. To mitigate this risk, one can:

- Have sound procedures like security clearance, check of criminal records, and credit check in place during hiring processes;
- Perform such checks at regular intervals during employment;
- Make sure only a few highly trusted people have access to the most critical parts of the service;
- Implement a control system where a second Piql operator needs to approve that a piqlFilm is withdrawn from the storage system or leaving the storage facility;
- Ensure that a person never works alone, whether they are an operator of the production or a security guard working the night-shift.

**Recommendations for Physical Security**

One event that can cause loss of ideal storage conditions is loss of utilities, most importantly the energy supply, but also water, gas etc. Backup generators and doubling of energy supply from two independent sources, e.g. electricity and diesel, is recommended.

In case of fire inside the building of where the piqlFilms are stored, a vast supply of oxygen restricting gas is important. A sprinkler system can potentially do more harm than the fire it is meant to put out. If the fire is outside of the building, i.e. a forest fire, measures needs to be taken on the construction of the building and its surroundings, such as clearing a safety zone between structures and vegetation, and only using fire-resistant or non-combustible materials on exterior surfaces. It is also a recommendation to add some sort of flame deterrent to the piqlBox itself, to mitigate the risk of damaging the piqlFilm in case of a fire.

Since there is not sufficient information to make a clear statement regarding the effects of water on the piqlFilm and piqlBox, the recommendation to the Consortium partners is to conduct tests of the piqlFilm with both clean, dirty, hot and cold water, with different duration of submersion. Despite this lack of information, it is still recommended to avoid exposure of the piqlFilm to water, to prevent the film layers sticking together, and the swelling and softening of the emulsion. A preventive measure would be to develop an air-tight, waterproof piqlBox.

How the piqlBox and piqlFilm are affected by jolts, drops, and external physical pressure, e.g. falling infrastructure due to an earthquake, is another subject where we lack sufficient information. As with the effects of water damage, we recommend that tests be conducted to better understand the consequences of such events.

In the report it is described how strong oxidative chemicals, like ozone, would cause great damage to the piqlFilm and the piqlBox. A possible solution would be to wrap the piqlBox in sealed aluminium foil to ward off gasses, as well as bacteria and other microorganisms. This type of measure would also mitigate damages to the piqlFilm caused by water.

 doi:10.2218/ijdc.v13i1.665

In terms of nuclear radiation and electromagnetic radiation, the report makes no specific recommendations. The likelihood of nuclear radiation effecting the Piql Preservation System is too low to make radial changes to the safety and security measures. If electromagnetic radiation was ever directed specifically at the Piql Preservation Services, the technology would be negatively affected for a time, but the confidentiality and integrity of the stored information would remain intact. Ultraviolet radiation on the other hand can affect the integrity of the information stored on piqlFilm quite severely. We therefore recommend to never leave the film exposed to sunlight, and to use appropriate lighting inside.

When it comes to physical theft and physical sabotage, the report focuses on ensuring a sophisticated security regime is in place in and around both production and storage facilities in the form of fences, camera surveillance, alarm systems and employed guards both during and outside of office hours.

### Recommendations for Computer Security

The report recommends that the guidelines set forth by the Norwegian National Security Authority to ensure the most impenetrable computer security regime, must be in place. These stipulate: all hardware and software must be state of the art, update security software as fast as possible, never distribute administrator rights to end-user, and block any unauthorized programs. Studies show that these four measures stop 80-90% of all internet related attacks. In addition, the guidelines say to activate code protection against unknown vulnerabilities, harden applications, utilize firewalls on client interfaces, use secure booting and hard disk cryptography, use anti-virus and anti-malware, and never to utilize more applications than strictly necessary.

In addition, the report recommends that Piql AS should offer its users cryptography as part of the front-end service before information is transferred, and implement cryptography for protection of the information after it enters the Piql IT system. This would compromise the vision of being self-contained, so whether this feature should stay intact or not should be up to the individual user to decide.

## Conclusions

The scenario analysis identified several vulnerabilities: some severe, such as fire and the threat of an insider; and some not so severe, like electromagnetic pulses and nuclear radiation, and some that simply require more testing. The main finding in terms of vulnerabilities is that it is the gelatine emulsion layer of the piqlFilm that is the weakest link, and as this is where the information is written, this vulnerability could have grave consequences for the security of the information stored. However, the gelatine silver print method has been used to preserve photos and moving images since 1874, and despite imperfect storage conditions, some of the first examples still exists today.

Nevertheless, Piql Services has many strengths. For example, the choice of materials, disregarding the gelatine emulsion layer, can serve to increase the security of the information stored. The properties of the PP (polypropilene) of the piqlBox and the PET (polyethylene terephthalate) of the piqlFilm seem to withstand a great deal of external influence.

Perhaps the most significant strength is that the piqlFilm is as an offline medium. With 500-year longevity, meaning no need for migration, this sets Piql Services apart

from any other physical storage medium for digital information. The content-data is only connected to online networks once, and only a handful of people must be involved.

When it comes to physical security there are some issues in terms of forces outside of one's control, be it forces of nature or threat actors with malicious intents. Taking necessary precautions and constantly being aware of potential risks should be sufficient. With time, the level of risk may be made even lower if alterations are made following this assessment. Ultimately, the decision to store information in any manner is a matter of risk acceptance. There will always be risks involved with every storage system when valuable information is involved. It simply a matter of placing the risk at a level acceptable to the user.

## References

Academy of Motion Picture Arts and Sciences. (2007). The digital dilemma – strategic issues in archiving and accessing digital motion picture materials. Retrieved from https://www.oscars.org/science-technology/sci-tech-projects/digital-dilemma

Brudeli, B., & Drake, K.M. (2014). A holistic approach to digital preservation. Paper presented at the SMPTE Conference, Hollywood, USA.

CCSDS. (2002). Reference model for an Open Archival Information System (OAIS). CCSDS 650.0-B-1, Blue Book. Retrieved from http://www.ccsds.org

Piql AS. (2015). *PreservIA EUREKA project application form.* Project number BIA 245586-Eureka.

Plata, O., & Bjerkestrand, R. (2012). The ARCHIVATOR: A solution for long-term archiving of digital information. *IS&T Archiving*

Long Term Retention (LTR) Technical Work Group. (2010). Self-contained information retention format (SIRF) – Use cases and functional requirements. Working draft version 0.5A.

Spitz, E., Hourcade, J.C., & Laloë, F. (2010). Lifetime of digital media: Is optics the solution? *Quantum Sensing and Nanophotonic Devices VII, Proc. SPIE*, 7608, 760802. doi:10.1117/12.848948

Termens, M. (2013). Preservación Digital. UOC.

The Security Act. (1998). 20 March 1998, No. 10 on preventive security service. (Actual to Protective Security Services).

The Public Procurement Act. (2006). 19 May 2006, No. 16 on the right of access to documents in public works. (Freedom of Information Act).

The Protection Instructions. (1972). 17 March 1972, No. 3352 instructions on the management of information in need of protection for other reasons than those mentioned in the national act on protective security services, including regulations.

The Personal Data Act. (2000). 14 April 2000, No. 31 on the processing of personal data.

 doi:10.2218/ijdc.v13i1.665

# Appendix 1

**Table 2.** Scenario metadata

| Scenario | Description |
|---|---|
| Scenario Number | |
| Scenario Title | |
| Scenario Justification | *Justification for the choice of scenario* |
| Scenario Outline | *Short description of the context and events leading up to this scenario and the cause of the incident. Short description of the incident, i.e. what happens, and when, how and in what environment does the incident occur.* |
| **Cause** | |
| Type of risk (hazard/threat) | |
| Intentional (Yes/No/Both) | |
| Profile of actor (if intentional) | *Short description of the profile of an actor that is willing and capable to conduct event, including 'modus operandi'* |
| Description of cause | *Threat: Motive, if it is an intentional act. Why is the value that the Piql Preservation Services is protecting valuable to this actor? (Intention).*<br>*Hazard: Type of hazard and brief description of properties. Cause of the accident or natural disaster, if it is an unintentional event.* |
| Competence and resources (if intentional) | *Applicable for intentional events: Necessary level of competence and availability of resources (equipment and economical means). (Capacity).* |
| **User/value** | |
| User class | *Sector* |
| User type | *Market area* |
| Value | *What is the value to be protected? What type of information? How is it valued? Why is it valuable? Is it irreplaceable?* |
| **Location** | |
| Location description | *Geographical zone, with brief description of climate zone (local geographical and typological conditions), developmental level (general standard of infrastructure and work culture) and political stability (stable borders, internal threat actors). City or countryside?* |

| | |
|---|---|
| | *Include what is relevant for the scenario.* |
| Environment description | *Local weather conditions. Time of year (with regards to temperature, etc.) Time of day (with regards to personnel on duty). Year/Time period.*<br>*The same hazard/threat can occur many times from a point onwards. If the hazard/threat presupposes a different setting in future, then the time period would simply start at a later point in the future and onwards.* |
| Vault description | *In mountain or in building. If in building: in basement, lower or upper floor? Inside environment.* |
| Local safety measures | *Fortified walls, seismic resistance, fire protection, water protection, radiation protection, EMP protection, utility backup.* |
| Local security measures | *Physical security measures on access control, camera surveillance, alarm systems and sensors, and number of personnel.* |
| **Consequences** | |
| Outer building | *Damages on physical infrastructure of building or mountain facility.* |
| Vault | *Security challenges/vulnerabilities for vault.* |
| Box | *Security challenges/vulnerabilities for box.* |
| Film | *Security challenges/vulnerabilities for film.* |
| Power/energy supply | *How was the power supply affected?* |
| Divergence from ISO standard | *Specified deviations from ISO standard in the vault concerning temperature and relative humidity, and the time duration of the divergence.* |
| **Security mechanisms** | |
| Integrity | *Brief summary on effects on integrity* |
| Availability | *Brief summary on effects on availability.* |
| Confidentiality | *Brief summary on effects on confidentiality.* |
| Immunity | *Brief summary on effects on immunity (against attacks on CIA).* |
| **Recommendations** | |
| Recommended protective measures | *List the safety or security measures which could alleviate the consequences of the scenario.* |
| References | *Relevant literature* |

 doi:10.2218/ijdc.v13i1.665

# Appendix 2: Detailed Scenarios

### Scenario 1: An accident at a nearby chemical plant caused by a human error

Chlorine gas is released into the humid atmosphere. The piqlBox and piqlFilm are subjected to prolonged exposure. The piqlFilms that the gas reaches are corroded, especially the gelatine emulsion where the information is written. This severely affects integrity and availability, as the data is destroyed and is thus no longer readable or accessible. However, neither is the data readable to anybody else anymore, so at least confidentiality is left intact.

### Scenario 2: A technical error causing sparks to ignite in the electrical system which powers the piqlVault system

This error causes the system to malfunction and shut down, as the faulty wires cannot direct electricity generated by the backup generator either. The sparks cause an electrical fire at the charging stations at the top of the grid which spreads. The fire sets of the sprinkler system in the building, helping to control the flames, but also dousing the piqlBoxes and –Films in water. More water is added once the fire department arrives. The piqlBoxes and piqlFilms near the top of the grid that are touched by the flames are damaged beyond repair because they quickly start to melt. The piqlFilms doused in too much water by the fire hoses and the ones near the bottom of the grid where water starts rising may be damaged because the piqlBoxes are not water-proof. The incident does not affect the confidentiality of the information on the films, yet availability and integrity are compromised temporarily or irrevocably for the piqlFilms too badly damaged either by fire or water. Some may be saved with the proper treatment.

### Scenario 3: A natural disaster in the form of an extreme flood during rainy season made worse by the effects of climate change

Due to the placement of the piqlVault in the basement, the raging waters quickly fill the entire space and completely submerge all the piqlFilms in the vault in extremely filthy water for days. Although the piqlVault system grid remains upright and the piqlFilms are kept in their original position inside the piqlBoxes, the boxes are not waterproof and filthy water can seep in and immerse the piqlFilms. The severity of the flood means that access to the piqlFilms is impossible for several days and they are all destroyed (we assume, but testing is necessary). The confidentiality of the information on the piqlFilms remains intact, as no one without authorized access would be able to read it during the incident. Neither, however, would the data owner. Because the piqlFilms are assumed to be destroyed, the integrity of the information, as well as the availability, is compromised.

### Scenario 4: An alternative natural disaster, e.g. a forest fire, which is made larger and more violent by the effects of climate change

After a period of excessive heat and drought, the piqlVault, which is placed in the lower floors of a building situated in the urban/rural interface, is caught in a fierce forest fire.

The local fire department are unable to get control of the fire for some time and it can rage in the vicinity for a fortnight. Not only are many of the piqlFilms and piqlBoxes irreparably damaged by the fire, but the data owner is also unable to gain access to the building for a very long time due to the dangers of the forest fire reaching the building again. Availability is thus compromised for all the films for a fortnight, and forever for the ones which were destroyed by the fire. The same is true for the integrity of these films, whereas confidentiality is only threatened but not compromised. However, as the piqlVault was equipped with a highly effective fire suppression mechanism, many of the piqlFilms, which would have been destroyed by the fire, were saved.

### Scenario 5: An earthquake measuring 7.5 on the Richter scale hits the city where a piqlVault is located during the middle of an intense heat wave

The skyscraper, in which the piqlVault is situated in one of the top floors, remains standing, but its infrastructure is badly damaged, leaving the piqlFilms in the vault exposed to the elements and allowing warm humid air to flow freely into the vault. The water pipes around the storage room burst, soaking the piqlFilms in water, and the electrical system is also damaged, which means that the ventilation system fails. Pieces of concrete fall from the broken ceiling onto some of the piqlBoxes. The integrity and availability of the piqlFilms which are struck by the pieces of concrete is irrevocably compromised. If the piqlFilms which are exposed to the water from the ruined pipes is not dried and handled correctly, their integrity and availability may be compromised as well. For the remaining PiqlFilms, the integrity and availability may be compromised if they are left too long exposed to high levels of temperature and humidity, as this affects the readability of the information. Confidentiality is threatened, as the security parameters surrounding the piqlVault are no longer in place, but the instability of the building's structure means that no one can enter anyway.

### Scenario 6: The theft of sensitive piqlFilms committed with the help of an insider

In a future setting where tougher market competition necessitates more brutal means of getting ahead, the oil company X bribes a high-level employee with complete access to the EWMS in the piqlVault system, who manages to leave the facility with the relevant piqlFilms without being stopped. The piqlFilms contain information on a new method to do oil well analysis, which can make dry oil wells profitable again. Though the transaction is logged, and the culprit is caught, the damage has already been done because the trade secrets, and thus also market shares, have already been lost. Although the integrity of the information was not tampered with, its availability to the data owner was compromised and, more importantly, so was its confidentiality.

### Scenario 7: The theft of sensitive information committed by an actor in an organized crime syndicate

A threat actor with access to heavy firepower commits a criminal act that takes place while the piqlFilms are transported from the production site to the storage facility. As part of a scheme to expand their revenue, the crime network decides to accept a job from a third party to steal piqlFilms storing personal data which is to be used in large scale identity theft. Although the sensitive information is protected by additional security during transportation, it is not enough to stop a gang of four persons from robbing the truck at gun point, forcing the security personnel accompanying the

 doi:10.2218/ijdc.v13i1.665

piqlFilms to give them up on pain of death. The integrity of the information remains intact, but the availability to the data owner is lost. The confidentiality of the information is most definitely compromised, at the cost of all the people who now stand to have their identities misused.

### Secenario 8: Sabotage

Sabotage is a very relevant threat to the Piql Services. State X hackers can perform logical sabotage on the client information which is being prepared for writing. The hackers place malware in the system which utilizes the interconnection between the Piql computer and the Piql I/O computer to create an open connection between the two. As the hackers now have free access to both computers' CPUs (Central Processing Unit) they can alter the client data undetected because they also change the corresponding checksum on both CPUs. Even though the Piql I/O computer does what it is supposed toand checks the integrity of the data against the designated checksum, it can find no faults and confirms the data ready for writing on the piqlFilm. The integrity of the information is highly compromised, as is the availability of the altered pieces of information. The confidentiality is compromised as well.

### Scenario 9: Espionage

Depending on the level of sensitivity of the information which is stored on the piqlFilm, the Piql System can be a target of espionage. This scenario underlines the risks involved when the digital data is processed during production before it is written onto the piqlFilm. Spyware is installed on this computer when the Piql system is used by the US military. The State X, as we will call them, manages to install spyware on the Piql computer system which the security measures in place are unable to detect. As a result, State X gains access to the designs of a weapon system developed by State Y, the major military power in the world. The spyware does no harm to the information: it simply copies the data that is located on the computer and sends it undetected to State X. Neither the integrity nor the availability of the information is affected, yet the confidentiality of highly sensitive information which can severely affect the relationship between two parties is lost.

### Scenario 10: Terrorism

A piqlVault is in the same building as a major NGO advocating multiculturalism. One day, without warning, a lone right wing extremist places a car bomb in front of the building and offices of said NGO and remote detonates the bomb. The Piql System becomes collateral damage. The bomb is powerful enough to cause severe damage to the structural integrity of the building, but the building does not collapse. Additionally, though the piqlVault is placed on the ground floor, it is placed on the opposite side of the building to where the bomb is placed, meaning that the damage to the vault is not as severe as the front offices. However, the bomb was powerful enough to cause great damage to the piqlVault. The damage to the building was to such an extent that the temperature and humidity regulation in the vault can no longer be upheld and the films are exposed to the elements. The integrity of some of the films is compromised, as they were damaged by the falling infrastructure caused by the bomb. The rest of the films are damaged only insofar as the cold of the outside air has a noteworthy effect on them.

Availability is likewise compromised, whereas confidentiality is only threatened but not compromised.

### Scenario 11: Armed conflict with strategic assault as part of the build-up to a larger confrontation

In a future setting where a state actor has set world domination as its goal, the threat actor executes a strategic assault on Svalbard, as it needs to remove what it believes to be intelligence about the state actor's military capacity. This is a step in a larger scheme to attack Europe, which the state actor believes it cannot do if European powers possess this information about them. Electromagnetic weapons (EMWs) and explosives are used to gain access to the storage facility, which is placed in a mountain repository. The electromagnetic pulses and controlled explosions do no harm to the piqlFilms, but they enable the unauthorized access of the state actor to the information, which is subsequently removed from the piqlVault. For a short period of time, the ideal storage conditions are not present in the piqlVault, but this is quickly rectified. The integrity of all the piqlFilms in the vault remains intact, but the availability and the confidently of the stolen piqlFilms is lost.

### Scenario 12: Nuclear war

In a future setting, the days of Mutually Assured Destruction (MAD) are back, yet the playing field is different than it was during the Cold War. There are a greater number of active nuclear powers, all with deterrence as their main policy, which means that the proliferation of nuclear weapons is higher, and more areas of the world are directly exposed to the threat. Many warheads are directed at various major cities always. One such city is a major metropolis in the Middle East. A glitch in the launch system of a major nuclear power releases a missile on said city by mistake. Even though the piqlVault is not situated within the radius of ground zero where heavily built concrete structures are severely damaged and fatalities approach 100%, it is still within the air blast and thermal radiation radius where most residential houses collapse, and fatalities are widespread. The piqlVault with all its piqlFilms is, in other words, a casualty of war. As all the piqlFilms are annihilated in the explosion, the integrity and availability of the information is forever lost, whereas the confidentiality remains intact.