CONFERENCE OF EUROPEAN STATISTICIANS

Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality Session 5

29-31 October 2019, the Hague, the Netherlands 17 September 2019

Crisis management – training, practising and testing

Janika Tarkoma and Harri Koskinen (Statistics Finland)

janika.tarkoma@stat.fi, harri.koskinen@stat.fi

Abstract and Paper

Crisis management is becoming more and more important for statistical offices because the general awareness on privacy has increased by discussions over the general data protection regulation (2016/679). Statistics Finland has in recent years actively worked to improve the documentation and processes for crisis management. The basic training of personnel in crisis management is naturally essential as well as the encouragement to inform all suspicious events, possible mistakes and errors as soon as possible. The procedures should be simple and clear and the responsibilities well designed. Information handling and dissemination should be efficient and timely; however, the dissemination should be carefully planned.

It is important to accept that a confidentiality breach is more often detected by someone outside the organisation than inside the organisation. This usually means that the media has learned about the incident at the same moment if not earlier than the organisation itself. Crisis management in case of confidentiality breach would mean that there are constant requests for more information and several rumours to confirm or reject. Only one representative should communicate to media to avoid conflicting comments. Therefore, quick and up to date communication to all the members of the organisation is also important. The quality of the crisis plans needs to be tested in simulations to obtain comprehensive feedback. Scenario testing in Statistics Finland demonstrate that even if the process is on a good level in general there can be some weaker points that should be improved. For example, the updated guidelines of Statistics Finland for crisis communication have been found to be good and thorough but too long to refer to when there is an actual crisis. Original guidelines are recommended for training, but a short list of main points is needed for actual use.

This paper will examine the crisis management guidelines and procedures of Statistics Finland and discusses certain aspects of the procedures based on simulation results. Based on the results we identify a number of concrete recommendations and refined guidelines.

Crisis management – training, practising and testing

Janika Tarkoma* and Harri Koskinen**

* Statistics Finland, janika.tarkoma@stat.fi
** Statistics Finland, harri.koskinen@stat.fi

Abstract: Statistical offices are facing new challenges as the general data protection regulation (2016/679) has been applied for more than a year now. In general, the general awareness regarding privacy has increased and at the same time more open source data is becoming available for everyone. Social media is an additional aspect because it changes the way information is distributed – it is faster but also more unreliable as false news are shared through the medium. The changing environment requires more emphasis for crisis management and especially crisis communication.
It is important to accept that a confidentiality breach is more often detected by someone outside the organisation than inside the organisation. This usually means that the media has learned about the incident at the same moment if not earlier than the organisation itself. Crisis management in case of confidentiality breach would mean that there are constant requests for more information and several rumours to confirm or reject. The high quality of the crisis management guidelines is essential. This quality needs to be tested by training and the guidelines need constant updates.
In this paper we will give general information on crisis management on the crisis communication point of view. We give examples on the situations when crisis communication has been needed in Finland pertaining to government agencies. The lessons learned from the actual incidents and the internal training will be described as concrete recommendations.

1 Introduction to the issues of crisis management

Statistical offices have come far from the time when statistics were published in printed versions. This change has been quite fast. Internet and webpages, advances in database technologies, public use files and now also social media have been shaping the environment. Each step has brought new advances in the form of easier access to data. But the changing environment also creates risks. If we compare the disclosure risks back when statistical tables were printed on paper to the situation now the risks are much higher. In the past, merging background and external information to the paper printed values took more than reasonable amount of resources. When the first statistics were published on the web the users still had limited computational power even if they had suitable software to use. Now there are more and more databases available and it is easy to merge different data sets with easy to access software. This helps to serve the users but it also means that undirect identifying takes no longer unreasonable resources if the data is not carefully protected.

Many national statistical institutes (NSI) are only learning to communicate via social media. Usually statistical offices do not publish more than key figures and some

advertisement in social media. Social media influences communication – how fast news are distributed. If any kind of disturbance would occur, the information would be available for many people faster than ever. This holds for false information as well. The new challenge is that corrections for the false information are more difficult to get distributed and the false news will live long after they have been corrected.

Crisis management covers not only confidentiality issues, but also other risks that can occur in statistics production and at the office in general. In this paper we will focus on the confidentiality issues and crisis communication when a confidentiality breach or other potentially harmful event has occurred. We give examples on events that are harmful to statistical office's reputation and on training for data breach situation.

1.1 General guidelines in Finland

The government has its own bodies for data security in Finland. The Public Administration Digital Security Steering Group (VAHTI), which is working for the Public Administration Information Management Advisory Board (JUHTA), provides guidelines and education on data security and disclosure control. VAHTI provides general guidelines from implementing legislation to practical guidelines on ICT, encryption, logging or cyber-attacks for central government authorities.

VAHTI guideline for Effective data security (Vahti 2009) describes continuity and emergency preparedness plan in detail. The emphasis should be on identifying and preventing threats. There should be plans how the operations and processes can continue in exceptional situation. The planning should specify key functions and services and the processing they need. This way it is possible to identify the threats, impacts of emergency conditions in systems, their effect on the key functions and specify back up plans. Emergency preparedness plan should always include up-to-date scenarios which means it must have an update plan.

One option to be sure that whole personnel is aware of their responsibilities in emergency situations is to include this information in their job descriptions. It would be easier for the personnel to understand their responsibilities, information security management, authorisations and monitoring and reporting obligations if they are described at early point. (Vahti 2009)

1.2 Guidelines at Statistics Finland

Statistics Finland has their own guidelines with specifications suitable for statistics production. An extensive document including all the subtopics of crisis management would be impractical in actual use. If a comprehensive document is needed it would be better to include a summary of all different topics with a reference to more extensive guidelines. Statistics Finland finds it better to have several guidelines for different parts of the production – from collection to production and publication.

Statistics Finland's communication guidelines for crisis and exceptional situations contain examples of situations when the guidelines are applied. Most common case is

when statistics will be published late, but also more severe cases are covered in the document. It contains details on the management and organisation for the communication. The responsibilities and the working groups are defined in the document. This helps to get organised when these groups are needed. The objectives and the principles for the communication is also defined in detail. The communication guidelines have several short attachments that are easy to use when anything exceptional happens. It is important to remember that the guidelines once written are continuously updated and reminded especially by the key personnel as the actual use of these guidelines will quite certainly come unexpected.

2 Personnel education

At many NSIs new employees are trained during the first days at the office. This seems to be the common way of educating personnel on the security and disclosure control. However, the work environment and especially the information technology is changing fast. Software are featured with new handy features that one must be aware. This means that continuous education is needed.

2.1 An example on human error in the use of confidential data

A data leak occurred in the National Institute for Health and Welfare (THL) in 2017 (THL 2017). It was a chain of unfortunate mistakes that lead to the publishing of confidential information of 6 000 persons. The first mistake was the use of use non-pseudonymised data set. This was allowed by the institute as this data was used for research by their own personnel. Another mistake was incomplete understanding of the software when preparing a presentation and accidentally including the data with a diagram. Then the presentation was downloaded from a slide sharing database to another and after that search engines were able to find the data behind the diagram. (Turun sanomat 2017)

THL worked hard to prevent further damage. This confidential information was noticed by a random citizen and he informed the Data Protection Ombudsman who informed THL. THL took time to investigate the situation and make sure that all the leaked information was removed from web before making a public announcement to prevent more people trying to find and download the confidential information. Also other precautions, like instructions for the persons included the leaked data set to follow their invoicing and credit and debit card information, were provided. Luckily there is still no evidence on misuse of the data. (Turun sanomat 2017)

2.2 Lessons learned

This described THL case works as a warning to all governmental authorities. Even if processes seem to be very well prepared there is a possibility for a human error. This data leak occurred before GDPR was applied. Now the legislation is stricter and all information is pseudonymised when received in an organisation. So, there should be no

personal identification numbers available in a data set that is given for research. Careful privacy measures may still fall short due to human error. It might still be unclear how diagrams are produced, and which software include the data with the diagram. Providing unnecessary and potentially harmful information can be prevented in different ways but people should know the features of the software used.

Times change as already described earlier. This also means that the procedures and rules that worked earlier might not be good enough anymore. This is among the most challenging topics for education. People tend to feel accused for doing something wrong when they are told that they need to add disclosure measures. The optimal way would be to audit all procedures when there is a change in legislation, but it is very hard in practise because production cannot stop for audits.

2.3 Educating the personnel at Statistics Finland

Statistics Finland has taken personnel training seriously. At Statistics Finland there are several courses covering data security and disclosure control. These courses are given on a regular basis and all personnel can participate on these courses. New recruits are attending orientation courses that include these topics as well, but they are encouraged to participate on the more comprehensive ones after the orientation.

Statistics Finland organizes general presentations and training when the legislation changes or if there are other changes in the working environment. There are also obligatory short courses for new or updated software at our office. This means that no one can install a new software version without attending the relevant course. During these courses personnel learn about security risks; however, the main focus is educating on the optimal use of the software. This helps to avoid possible mistakes that happen when the software is not familiar enough.

In addition to the in-house education of Statistics Finland, there are general courses for government personnel. VAHTI has organised projects as a part of the data security education when preparing for the general data protection regulation (GDPR). These projects have produced data security and disclosure control videos for the government personnel. Everyone should watch the videos and then pass the related test. This education is considered as a part of the training for accountability of the GDPR. (Rousku 2018)

3 Training for crisis

Statistics Finland has emphasized the preparation of the guidelines and procedures, but it is also important to see how they work in practise. This could be learned from a true experience, but it is much better to have a safe training environment to check the status. It is quite clear from the experience of others that it is more matter of when than if a publicity crisis will occur.

3.1 Congratulations, you're a winner!

On 1 August 2018 Statistics Finland started to receive emails and phone calls from concerned citizens. They wanted to know if an email that they had received was real. The email told them that they had won a latest model iPhone. The email had a link to a webpage that contained the instructions on how to claim the promised iPhone and how to pay for the one euro postage fee. The webpage looked just like a genuine Statistics Finland webpage.

To remedy this scam campaign, we posted warnings to social media channels, our own website, and news media also ran stories about the scam. Despite the efforts, we still received well over 300 emails and phone calls about this incident in just a few weeks. It was also unfortunate that some persons lost money to the scammers.

The basic idea of the scam was simple: ask people to pay one euro using a credit card for a new expensive phone and then charge them a much larger sum instead.

3.1.1 What we found out and learned from this (TOP 5)

1. People still don't pay enough attention to the address of the website they are visiting

The scammers used several different URLs/domains for the fake webpage, but none of them were even close to the real address. People are used to the fact that most of the websites they visit have urls that are complete gibberish, so they are easily fooled if the website just looks genuine.

2. People still don't pay enough attention to the sender's email address

The emails were sent using free email services like Google and Hotmail. The scammers didn't make any effort to fake the sender address. There are multiple ways to prevent email's sender address forgery, but as this case shows, they offer no protection if the scammers are not even trying to forge the address. It should be common knowledge that a government agency is not going to send you email from an address like andrew77777@gmail.com.

3. International scammers speak your language too

It used to be that the emails scammers would send were written in English. So, if the sender claimed to represent a Finnish government agency, it was easy to dismiss the email as a fake. But now, the fake emails and the fake webpage were written in Finnish. Not in perfect Finnish, but it was good enough to fool people. The rise of easy-to-use translation tools has made scammers life much easier.

4. Scammers use HTTPS too

It is not that many years ago when people were instructed that safe websites use traffic encryption and bad websites don't. This was mainly because the certificates, required to encrypt the traffic, were expensive. Today you can get a certificate that is trusted by all major browsers for free.

5. You cannot practice communication too much

> When people, who normally are not your clients and have no idea how to contact you "properly", have an issue they want to discuss with you, they will use whatever contact info they will find using a search engine. This means that they may end up contacting directly a worker who has no knowledge of the issue or no idea about who could know something about it. Thus it is important to instruct staff members to handle these contact requests following a unified policy. It is also important that there is sufficient training for the staff regarding the policy.

From a risk management perspective these kinds of incidents may pose a real threat to organizations reputation if not handled correctly. Communications received from clients, users, etc., should always be answered properly and always in a unified way.

3.2 In Finland we have this thing called TAISTO

The Population Register Center of Finland organized a security and data protection management training (TAISTO18) in 2018. TAISTO18 training was a simulation of data security breach and it was designed for government organisations. This was a voluntary based practise and some 235 organisations including Statistics Finland participated in this exercise. The twofold aim of the training was to develop organisation's data security management in case of a data security breach and to develop the processes needed to minimise the harm in these unfortunate events. These processes include for example the ability to evaluate the risk at hand realistically and to work based on that evaluation so that the information needed is provided to other government offices and the situation is communicated to the larger audience. (Rousku 2018)

TAISTO18-practise is an excellent method for assessing how well the personnel have prepared and how well crisis communication guidelines work.

Content of Taisto18 training (Rousku 2018):

1. Finnish Transport and Communications Agency informs that there is a severe zero-day vulnerability that effects all organisations and requires actions immediately.
2. An activist group has informed a data breach. This data breach affects a high number of Finnish online services.
3. The activist group has published information on the personnel of Finnish organisations.
4. *First reporting point.*
5. The activist group has published more information on the personnel of Finnish organisations.
6. Media wants to know the situation in your organisation.
7. Taisto-TV reporter is asking more information on the events of the day.

8. *Second reporting point.*
9. *Exercise is almost finished. Make a short report on the main points from the exercise for your own organisation.*
10. *Exercise has finished. Fill in the feedback and write down the lesson learned, and possible changes needed based on this exercise.*

TAISTO19 training will be organised in November 2019 (VRK 2019). Statistics Finland will participate in the event. An advance assignment was sent to the organisations so that the organisations will be prepared for the training. In the previous TAISTO18-training there was information available in advance, but no advance assignment.

3.3 Tailored training for Statistics Finland

There were two separate training sessions organised in 2018 with a consulting company. This company provides a specific training platform that simulates the information on media and government connections. They also had a tv-group to have an authentic simulation of communication for media. The aim of these training sessions was to test the documentation and increase the capability of the keypersons to manage crisis situations. One important point was to ensure that deputies for the key persons are assigned and they are prepared to step in when needed.

The first training was more focused on the crisis communication to media and the second one was focusing on internal and governmental coordination and communication. Both training sessions were found very useful. The second training had an additional challenge level when some of the key personnel had unplanned absence from work and the deputies had to step in with a larger responsibility.

It is one thing to write and formalise documentation for crisis management and another thing to work with these guidelines and make decisions when a crisis occurs. Training with a simulation platform makes the training situation feel more realistic and helps personnel to get more natural reactions during the training.

Training provided information on the parts of documentation that could be improved. For example, the documentation describes how different crisis management groups should work but still some of the issues were discussed in many groups. Division of tasks should be more precise. Also some other points were noted during the training, like more focus should be put to status of the situation. The status of situation and steps taken should be logged in a platform that is available for all key personnel and also easy to follow.

These TAISTO and tailored trainings helped the planning of the personnel education. Some education was planned for everyone but also specified training courses were planned.

4 Lessons to share

Crisis management training and the unfortunate event of data breach in THL raised up some key points that need to be addressed:

- The environment in the organisation must be such that the possible errors/accidents can be informed immediately and not covered if noticed by an employee. It is also important to make sure that the information on the incident has been received.
- Stay calm. The situation – what has happened and the role of your organisation – must be clear enough before communicating or acting.
- When data breach is discovered, the guidelines must be sort and clear.
- List of persons to contact in the organisation must be clear and updated.
- Organisation's own personnel must be informed as fast as possible to prevent unofficial comments and confusion in the organisation.
- The list of organisations to contact with precise contact names and contact information should be updated and easy to find.
- Press release should be formulated in a form that you only need to fill in parts as there is probably no time to start to formulate one from the scratch.
- The minimal information rule should be applied until whole situation is clear.
- Keep precise log on the actions taken as they might be needed for the reference during the situation and will be useful when refining procedures and guidelines afterwards.
- Summaries that give overview on the situation and its status are mandatory when several people work together. An up to date flip chart or similar would be useful to give a quick overview.

References

The Government Information Security Management Board (VAHTI) (2009). *Effective Information Security*. Helsinki.

The National Institute for Health and Welfare (THL) (2017). *Press release: Confidential personal information was publicly available online*. https://thl.fi/en/web/thlfi-en/-/confidential-personal-information-was-publicly-available-online [6.8.2019]

Population Register Centre (VRK) (2019). *Taisto-harjoitus*. https://vrk.fi/taisto [2.8.2019]

Rousku (2018). *Miten Suomen julkisen hallinnon organisaatiot pärjäisivät tietoturvan ja tietosuojan ollessa uhattuna? TAISTO18-harjoitus*. https://vrk.fi/documents/2252790/9592142/TAISTO+tiiviisti+-esitys/72eaedff-

4498-d66f-fbc8-588c3973170e/TAISTO+tiiviisti+-esitys.pdf?version=1.1 [2.8.2019]

Turun sanomat (2017). *Virkamies tietovuodosta: Miksi THL ei käyttänyt anonyymia tietokantaa?* https://www.ts.fi/uutiset/kotimaa/3668604/Virkamies+tietovuodosta+Miksi+THL+ei+kayttanyt+anonyymia+tietokantaa [6.8.2019]