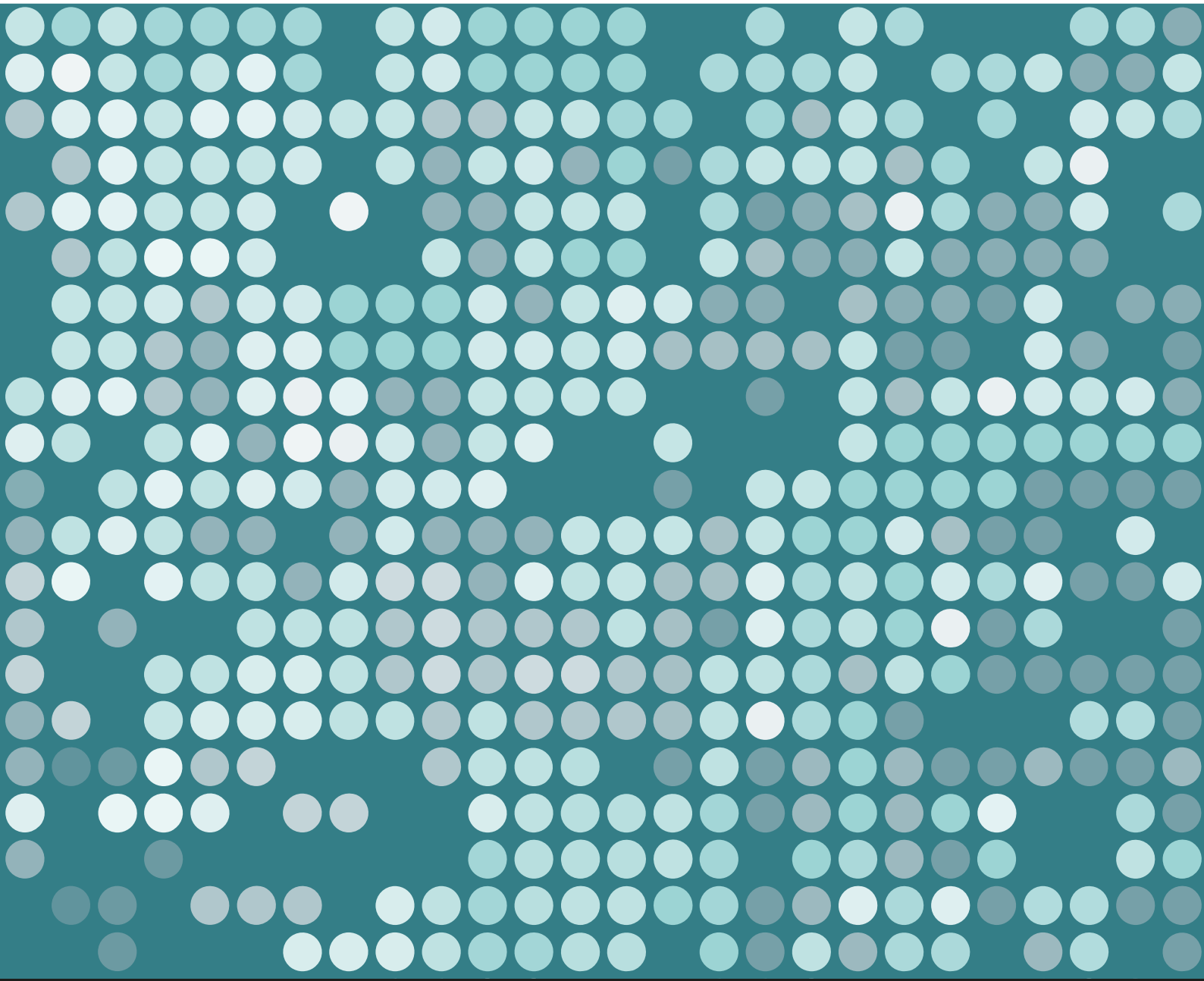
English summary of report 2022:8



Data breaches reported to the police

Offence characteristics, challenges, areas for development

The Swedish National Council for Crime Prevention (Brå) -
centre for knowledge about crime and crime prevention measures

The Swedish National Council for Crime Prevention (Brå) works to reduce crime and improve levels of safety in society. We do this by providing factual information and disseminating knowledge on crime and crime prevention work, primarily for the Government and agencies in the criminal justice system.

This report is a summary of the Swedish report Polisanmälda dataintrång. Karaktär, utmaningar, utvecklingsområden 2022:8
© Brottsförebyggande rådet 2022
urn:nbn:se:bra-1074

Author: Elina Lindskog, Lou Huuva, Sarah Lehtinen, David Shannon

The Swedish National Council for Crime Prevention, Box 1386, 111 93 Stockholm, Sweden
Tel: +46(0)8 527 58 400, E-mail: info@bra.se, www.bra.se

This summary can be downloaded from the Swedish National Council for Crime Prevention's website,
www.bra.se/publikationer

Data breaches reported to the police

Offence characteristics, challenges, areas for development

English summary of Brå report 2022:8

Summary

The Swedish data breach offence involves unlawfully accessing data intended for automated processing or the unlawful alteration, deletion, blocking or entry of such data in a register. The data breach provision thus encompasses offences committed in the context of several different types of crime. These range from the simplest types of breaches, such as unauthorised record searches in the course of one's work or hijacking someone's social media account, to more complex offences in which a perpetrator attempts to gain illegal access to a computer or computer system in order to cause damage by blocking services, stealing or destroying information, or encrypting information for the purpose of extortion.

Although the nature of data breach offences can vary greatly, all are characterised by the fact that they take place in a digital and often international context, which complicates the investigative work of police and prosecutors. The purpose of this report is to describe the types of data breach offence that are currently being reported to the police in Sweden and the difficulties that police and prosecutors face in investigating and prosecuting these offences, with a special focus on the more complex data breach offences. The study is based on the following research questions:

1 What types of data breach and related criminal offences are reported to the police, who are the victims, and who is suspected of committing these offences?
2 What types of data breach offences result in prosecution?
3 What difficulties do police and prosecutors experience in investigating and prosecuting complex data breach offences?

The report also suggests areas in which the investigative work of the justice system could be improved and notes the importance of disseminating information to prevent and thereby reduce the number of data breach offences committed.

A focus on the more complex data breach offences

In Sweden, nearly 9,000 data breach offences were reported to the police in 2020, rising to more than 11,000 in 2021, which is probably only a fraction of the number of offences committed, since the number of unreported data breach offences is considered to be high (Europol 2020). The Swedish police use five different offence codes to distinguish between different types of data breach:

- data breach in the form of denial-of-service attacks
- data breach using malicious code for the purpose of extortion

- data breach involving unauthorised record searches
- data breach in social media or e-services
- other forms of data breach

The police distinguish between data breach offences that are viewed as examples of complex cybercrime, such as data breach in the form of denial-of-service attacks and data breach using malicious code for the purpose of extortion, from data breach offences of a simpler nature, such as data breach in social media or e-services and data breach involving unauthorised record searches. This report focuses primarily on the investigative work related to the more complex data breach offences, which are investigated by the police's expert functions for the investigation of complex cybercrime at the Swedish Police Authority's IT- crime centres.

The report is based on a review of police reports, criminal investigations and interviews

Two data sets were used to elucidate the questions posed by the study. Questions 1 and 2 relate to which types of data breach offences are reported to the police and which types lead to prosecution, which have been examined by means of a sample of 641 police reports made during the period July to December 2020 and, where applicable, material from the criminal investigations linked to these reports.

In order to answer question 3, on the difficulties experienced by police officers and prosecutors in their investigative work, 30 interviews have been conducted with police officers, prosecutors and actors in both the private and public sectors who monitor various aspects of data breach crime as part of their work. These interviews also provide the basis for the report's discussion of areas in which the investigative work of the justice system might be improved.

Overall results

Characteristics of the data breach offences reported to the police

Data breach as an element in other forms of crime

A data breach offence may take the form of an isolated incident or may be initial step towards the subsequent commission of other types of crime. The results of the study show that when the police reports also include references to other types of crime, it was common for the data breach to have been used as a preliminary step in the commission of fraud or extortion offences. With the exception of data breach offences that were limited to unauthorised

record searches, between 20 and almost 27 percent[1] of the police reports examined also included fraud or extortion offences in addition to the data breach.

However, in police reports registered as involving data breach in social media and e-services, it was instead more common for the reports to include descriptions of offences against the person, and in particular the unlawful use of a person's identity. In the case of reports of data breach involving unauthorised records searches, it was common for the report also to also include references to the criminal code provisions on official misconduct or breach of confidentiality.

Data breaches affect both legal entities and private individuals

The study shows that private businesses and organisations in the public and non-profit sectors are slightly more likely to report more complex forms of data breach (denial-of-service attacks and malware-based extortion offences) than private individuals, who are instead more likely to be victims in relation to the other types of data breach examined.

Businesses affected by data breaches range from small firms and the self-employed to large corporations, with some stating that losing access to their servers as a result of malware can lead to a substantial loss of income every day. In addition to denial-of-service attacks and malware-based extortion, the police reports show that data breach is also used to expose businesses to among other things fraud and data theft.

The individuals who report exposure to data breaches include men and women from a wide range of age groups, from schoolchildren to seniors in their eighties. At the same time, there are certain gender and age differences. For example, females were more likely than males to have reported exposure to data breaches in social media and e-services.

There is no age group that appears to be particularly vulnerable to a particular type of data breach, but compared to the other types of data breach examined, it was more common for the victim to be under 18 years of age in reports describing data breaches in social media that had been used as a means of bullying, humiliating or controlling the victim, and females were also more likely to have reported exposure to this type of crime than males. Females were also slightly more likely than males to have reported data breaches that had been used to commit fraud offences via social media and e-services.

---

[1] Depending on the offence code under which the report had been registered.

Few offences result in prosecution

The results of the study show that the clearance rate for data breach offences is low. There is nevertheless a variation in the clearance rate between different types of data breach offences. The vast majority of the offences that had resulted in prosecution involved unlawful record searchers. Of the cases of this kind examined in the study, one-fifth of the reports had resulted in prosecution, while five percent had resulted in a fine imposed by the prosecutor.

With the exception of unlawful record searches, only three of the remaining 542 offence reports examined in the study had resulted in prosecution. One of these was a case of denial-of-service, the other two had been registered as "other forms of data breach".

In many of the other cases, the reports had been filed as closed without initiating a police investigation, and in cases where an investigation had been initiated, the majority were discontinued due to having been unable to identify a suspect or difficulties in securing evidence.

The only type of data breach offence in which a suspect had been linked to the offence in a majority of cases was once again data breach in the form of unlawful record searches. These offences differ from the other types of data breach in that the record searches are often made at the offender's place of work and logged in the organisation's IT system, thus facilitating the identification of a suspect.

In some of the cases involving data breaches in social media and other e-services, however, the victims had given the police the name of a person they suspected of the offence at the same time as they filed the police report. In these cases, the suspect was most often either an acquaintance or a partner or former partner of the victim.

Difficulties and challenges faced by law enforcement

Difficulties at several stages of the investigation

Interviewees reported difficulties at several stages of the investigation process, particularly in the more complex data breach cases. These range from an unwillingness among injured parties to participate in the investigation, particularly among businesses exposed to data breach, to difficulties in accessing data from digital service providers.

A recurring theme in Brå's interviews with actors in the justice system is that overburdened cyber forensic units mean long waits for the results of data analyses, and thus long delays in the investigative process. This jeopardises investigative work because digital evidence is a highly unstable commodity and the longer one has to wait for results from a cyber forensic analysis, the

greater the risk that the evidence needed to make progress in the investigation will no longer be available when the cyber forensic results provide the information needed to retrieve it.

Interviewees also highlighted other challenges. The low reporting rate, combined with the fact that the Police Contact Centres (which register reported offences) sometimes close cases immediately that should instead be forwarded to specialist IT-crime units for investigation, and a lack of coordination in data breach cases, means that those investigating data breach offences lack an overarching picture of the crimes that are committed, which further complicates investigative work.

Specific difficulties linked to the international nature of cybercrime

Many data breaches take place across national borders, particularly complex data breach offences such as denial-of-service and ransomware attacks, with criminal groups in other countries conducting organised attacks against Swedish companies. Investigations focused on these crimes require well-functioning and efficient cooperation between the legal systems of different countries, for example in the form of mutual legal assistance or the implementation of European Investigation Orders. However, interviewees stated that this process is time-consuming, which is counterproductive when rapid access to digital evidence is so important.

An underdeveloped police organisation for investigating complex cybercrime

The interviews conducted by Brå show that the Swedish police today still work in a relatively traditional way in investigations of data breach offences. For example, reports concerning complex data breach offences are primarily investigated at cybercrime centres in different police regions, with little or no coordination of these investigations at the national level. One conclusion from Brå's interviews with both private actors and justice system employees is that the police's working methods are in need of development to facilitate better cybercrime investigations and to allow the Swedish police to make more of a contribution to international collaborations to combat cybercrime.

Brå's assessment

A more developed and effective police cybercrime infrastructure

The interviews conducted by Brå with people in various positions within the police organisation show that the police's infrastructure for investigating complex cybercrime is still under construction, and is also vulnerable. The system of regional cybercrime centres is relatively new, and there is no clear coordinating function at the national level. Brå's study shows that there is a need for more sustained investigative work, where individual investigations are not abandoned too quickly, which would provide better opportunities to identify and coordinate cases originating from the same criminal actor, both

regionally and nationally, for example by working in teams that include representatives from both the regions and the national cybercrime centre. More sustained investigative work would also provide better opportunities to develop investigations to the point at which they become useful to international police operations against organised cybercrime.

An important prerequisite for this work is also that dedicated IT forensic expertise is linked to these investigations. According to the interviewees, dedicated IT forensic expertise is currently linked to the investigative work conducted in some regions but not in others. In cases where there are no dedicated cyber forensic resources, cybercrime investigations have to compete with other types of criminal investigations, including those where a person is being held in pretrial detention (which are automatically given high priority). The importance of rapidly obtaining and analysing cyber forensic evidence means that the lack of a dedicated resource creates a bottleneck in the investigative process that places the entire investigation at risk. There is also a need to improve the level of collaboration between the police and private actors in the cybersecurity field, among other things in order to provide the police with better insights into developments in the field of cybercrime, active criminal groups, malicious digital infrastructure and new cybercrime methods.

At the same time, it is also important to realise that improving the conditions for police investigations is unlikely to lead to a significant increase in the number of prosecutions for data breach in Sweden, since the more complex offences are often committed by actors beyond Sweden's borders. Improved police investigations with a focus on international collaborations with law enforcement agencies in other countries would give the Swedish police a better opportunity to contribute to law enforcement efforts, but to achieve this there is also a need for new performance measures for police cybercrime enforcement that are not based on clearance rates.

Continued modernisation of relevant legislation

The ability of the police to investigate complex cybercrime, including data breach, is dependent on the adequacy of the relevant legislation. A challenge that has been highlighted both in previous Brå reports and in the interviews conducted with police and prosecutors in the current study is that the legislation has not kept pace with developments in the field of cybercrime. In recent years, the Swedish government has appointed a number of legislative committees to review various pieces of legislation related to the ability of law enforcement to access electronic data, and these have resulted in legislation that has improved the opportunities for law enforcement to obtain access to information stored in the cloud. Continued work to modernise the relevant legislation and adapt it to the constantly evolving opportunities for

cybercrime is also necessary to enable law enforcement agencies to work effectively against data breach and other forms of cyber-offending.

Encouragement and support to reduce the risk for exposure to data breach offences

Data breaches constitute an important aspect of cybercrime, which has expanded in line with technology developments and the increasing digitalisation of society at large. These crimes involve large sums of money, are well-organised and are likely to continue to increase. They need to be taken seriously as a significant current and future threat to Swedish businesses and citizens, as well as to the country's digital infrastructure.

Given this threat and the difficulties associated with investigating and prosecuting these offences, it is important to encourage and support businesses, other organisations and individuals to protect themselves against data breaches.

A key conclusion from Brå's discussions with cybersecurity experts is that a central goal for prevention work should be to increase the number of internet users who make use of the existing opportunities to reduce the risk of exposure to data breach. Most data breach offences are committed using simple methods and could be prevented. There are already well-developed security solutions and recommendations to reduce the risk for data breach, and information on these solutions is available from a range of actors, including the Swedish Civil Contingencies Agency (MSB).

The challenge for crime prevention efforts is to effectively communicate these recommendations and ensure that more people implement them. General information campaigns are already being conducted to this end, but research suggests that information efforts are more likely to bring about behavioural change when they are targeted more directly and tailored to specific audiences. It is therefore important that other actors also take the cybercrime prevention information that exists today and adapt and disseminate it to their own target groups, for example in the school and higher education sector, among employer organisations and interest groups from different sectors of the economy, and also in individual companies and public sector agencies.