Anna Leppänen

Cybercrime Is a Police Matter – an Introduction to a Finnish Guidebook for Enterprises on Cybercrime Investigation Process

Police University College Reviews 20

CYBERCRIME IS A POLICE MATTER – AN INTRODUCTION TO A FINNISH GUIDEBOOK FOR ENTERPRISES ON CYBERCRIME INVESTIGATION PROCESS

Anna Leppänen

REVIEWS OF THE POLICE UNIVERSITY COLLEGE 20

Police University College
Tampere, 2021

Anna Leppänen
CYBERCRIME IS A POLICE MATTER – AN INTRODUCTION TO A FINNISH GUIDEBOOK FOR ENTERPRISES ON CYBERCRIME INVESTIGATION PROCESS

Reviews of the Police University College 20
ISBN 978-951-815-400-9
ISSN 2341-6394

Grano Oy 2021

ABSTRACT

The Police University College of Finland, in collaboration with JAMK University of Applied Sciences published a Finnish guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta" [Cybercrime Is a Police Matter – A Guidebook for Enterprises on Cybercrime Investigation Process] in March 2021. Over 40 experts from public and private sectors participated in reviewing and developing the contents and best practices presented in the guide. The guidebook's purpose is to increase companies' knowledge of cybercrime, encourage the reporting of cybercrime to the police, and help to refine procedures used in solving potential crimes. Companies will gain optimal benefit from the guide, if they use it to facilitate discussion and support self-assessment.

The guide was well received and led to several requests to translate it into English, too. However, most of its content is directly applicable only in Finland, therefore, a one to one translation would not meet the needs of companies beyond national jurisdiction in Finland. This report is intended for readers interested in raising cybercrime awareness and looking for new initiatives in campaigns targeted at the private sector or organisations. Therefore, it enlightens the process of preparing the guidebook and some of the materials underpinning it. Moreover, the report describes the content of the guidebook without diving into country-specific details and puts forward two sets of best practices: *1) What kind of information the police may need when investigating a cybercrime in an enterprise,* and *2) How to improve the probability of solving such a crime*.

This report, besides being a source of inspiration, provides a starting point or a point of reference for anyone planning practical material for companies or organisations on cybercrime investigation, whether a guidebook or something else. Overall, there is a need to improve co-operation between the police and enterprises as cybercrime victims. Raising awareness of cybercrime investigation might be a potential approach, since it seems that companies seldom report cybercrimes to the police or, if they do, the reporting comes too late and the digital traces have already vanished.

TIIVISTELMÄ

Poliisiammattikorkeakoulu ja Jyväskylän ammattikorkeakoulu julkaisivat suomenkielisen oppaan “Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta” maaliskuussa 2021. Oppaan sisältöjen ja hyvien käytäntöjen kehittämiseen ja arviointiin osallistui yli 40 asiantuntijaa julkiselta ja yksityiseltä sektorilta. Sen tarkoitus on lisätä yritysten tietoisuutta kyberrikoksista, kannustaa ilmoittamaan kyberrikokset poliisille ja auttaa omaksumaan käytänteitä, jotka edesauttavat mahdollisten rikosten selvittämistä. Yritykset saavuttavat parhaimman hyödyn oppaasta, jos he käyttävät sitä keskustelun ja itsearvioinnin tukena.

Opas sai hyvän vastaanoton julkaisunsa jälkeen ja kyselyitä, voisiko sen kääntää myös englanniksi. Käännös ei kuitenkaan palvelisi alkuperäisen kohderyhmänsä, eli yritysten avainhenkilöiden, tarpeita, koska sisältö on suoraan sovellettavissa vain Suomessa. Sen sijaan tämä raportti on laadittu kyberrikostietoisuuden lisäämisestä kiinnostuneille, jotka etsivät uusia avauksia yksityiselle sektorille ja organisaatioille suunnattuihin tietoisuuskampanjoihin.

Tässä raportissa esitellään opaskirjan laatimisprosessi ja osa taustamateriaaleista, joihin opas perustuu. Lisäksi raportissa kuvataan oppaan sisältö menemättä maakohtaisiin yksityiskohtiin ja esitellään kahdenlaiset hyvät käytännöt: 1*) Millaista tietoa poliisi voi tarvita kyberrikostutkinnan aikana* ja 2) *Miten parantaa kyseisen rikoksen selvittämisen todennäköisyyttä*. Raportin tarkoitus on toimia inspiraationa, aloituspisteenä tai viitteenä muille, jotka suunnittelevat laativansa yrityksille tai organisaatioille käytännönläheistä materiaalia kyberrikostutkinnasta – olipa se sitten opas tai jotain muuta. Kaiken kaikkiaan on tarve parantaa poliisin ja kyberrikoksen uhriksi joutuneiden yritysten välisen yhteistyötä. Tietoisuuden lisääminen kyberrikosten tutkinnasta voi olla yksi keino muiden joukossa, sillä vaikuttaa siltä, että yritykset ilmoittavat kyberrikoksista poliisille harvoin tai liian myöhään, jolloin digitaaliset jäljet ovat jo kadonneet.

TABLE OF CONTENTS

ABSTRACT **4**

TIIVISTELMÄ **5**

INTRODUCTION **7**

GUIDEBOOK DEVELOPMENT PROCESS **10**

Framing the need for a guidebook 10
Fictional case examples 11
Feedback from authorities and companies 11
Contents of the guidebook 13
Part one: Companies as victims and factors of reporting cybercrime 15
Part two: Cybercrime investigation 19
Part three: Practical advice 20
Reporting to the police 21
Reporting to all relevant authorities 21
Some of the key authorities and other agencies 22
The kind of information the police may need when investigating a cybercrime in an enterprise 23
How to improve the probability of solving a crime 25

CONCLUSION **28**

REFERENCES **29**

APPENDICES **30**

Appendix I: About the CYBERDI project 30
Appendix II: A fictional example of the pre-trial investigation of a ransomware case 31

INTRODUCTION

Cybercrime is often characterised as a crime targeted at information and communication systems or committed through them. This definition stands out as an informal and encompassing categorisation, and, arguably, many common types of offences may include features of cybercrime. For example, fraud or extortion become cybercrimes if committed in an online environment.

The number and significance of cybercrimes has increased. Enterprises from all sectors and of all sizes should recognise the fact that they may attract such criminals through their business and ICT infrastructure, coincidentally or just by being easy, careless targets.

People and companies often fall victims to cybercrime, but report the incidents to the police less frequently. This fact becomes visible when comparing different authorities' statistics with each other or crime surveys. For example, many clients of CERTs (computer emergency response teams) do not want to involve the police even if they have encountered an obvious crime endangering multiple customers (Leppänen and Kankaanranta 2018). Furthermore, people seem to be less willing to report cybercrime than traditional crime, and they have lower expectations that cybercrime will be solved (Graham, Kulig and Cullen 2020).

In the business environment, preparedness for the threat of cybercrimes is part of risk management. However, the key personnel in charge of the business may not have enough information to draw a conclusion on the risk of cybercrime to the business as whole. Moreover, knowledge of cyber threats may exist in the company or among its contractors but has not dispersed throughout the company. Furthermore, when it comes to criminal investigation, companies may be unaware of the process and efforts it requires of the victim. Misunderstandings, even unwarranted fears, may dominate the decision-making and prevent victims from contacting the police.

To overcome these two obstacles, i.e. non-reporting and potential lack of knowledge, experts from the Police University College of Finland (hereinafter 'Polamk') and JAMK University of Applied Sciences (hereinafter JAMK) have developed a guidebook entitled "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta[1]" (Cybercrime Is a Police Matter – Guidebook on Cybercrime Investigation Process for Enterprises). This guidebook was published in March 2021 as part of project CYBERDI's[2] campaign to increase awareness of cyberthreats. Its purpose is to increase companies' awareness and knowledge of cybercrime, encourage the personnel to report cybercrime to the police, and support the companies in establishing procedures to help to resolve a potential case of cybercrime. Companies are to gain the optimal benefit from the guide, if they use it for as a framework for reflective discussion and self-assessment. For example, management, board members, ICT staff and communications' experts putting their heads together by engaging in a reflective dialogue would pave the way for the emergence of shared understanding from shattered pieces of knowledge.

1 Download the guidebook (in Finnish) from the Police University College's website: https://polamk.fi/en/cyberdi-en

2 Read more about project CYBERDI in Appendix I.

Reporting a crime is simpler when companies have pre-defined operating models.

Illustration 1 The guidebook encourages companies to set a general policy on reporting cybercrime and assess each incident according to the framework.

This report introduces our guidebook to the reader and explicates the way we compiled it. The report originates from the encouraging feedback received from various Finnish authorities and companies, but also from direct requests to have the guide translated into English. Unfortunately, a direct translation is not reasonable as such. Each national jurisdiction represents a unique system, and our guide reflects the criminal justice system in Finland. For example, the sections describing the pre-trial investigation process and practical advice on how to report a crime to the police apply only in Finland. Furthermore, the organisations introduced and the distribution of tasks between them represent the national situation.

A group of Finnish companies and authorities helped us to outline the best practices. However, they have not been evaluated by experts from other countries. Therefore, instead of translating the guide one-to-one into English, it became my task, on behalf of the project CYBERDI team, to make the essential content of the guidebook available in English and to valorise the compilation process behind it too. I decided to include the description of the best practices into this report when it seemed reasonable to do so. The aforementioned are issues, which our team would have appreciated as beneficial in the initial stages of our work for the guide. I hope that our work will serve as an inspiration, starting point or reference to others who wish to write some practical material for companies or organisations on cybercrime investigation, be it a guidebook or something else. Furthermore, I encourage all involved to make suggestions on reviewing and revising the best practices – after all, a best practice is intrinsically something that evolves.

The structure of this report is as follows. First, I introduce the development process of the guidebook. Next, the focus moves onto the composition. I provide an overview on all three parts of it. Then, I present translations of best practices on two themes: 1) information the police may need during a cybercrime investigation, and 2) how victims can improve the likelihood of solving a cybercrime from their part. I conclude the report by discussing the importance of increasing awareness of cybercrime prevention and research. In Appendix I, the reader will find information on CYBERDI project and organisations behind the guidebook, i.e. Polamk and JAMK. Appendix II presents a fictional case example of cybercrime investigation and sheds light on co-operation between the police and crime victims.

GUIDEBOOK DEVELOPMENT PROCESS

Framing the need for a guidebook

Planning of the guidebook began in the summer of 2020 with the idea that co-operation between the police and enterprises might evolve and the number of reported cybercrime increase if enterprises became more familiar with pre-trial investigation work. Experts working at project CYBERDI contacted the National Bureau of Investigation's Cybercrime Centre, the Security Intelligence Service, and the Finnish Transport and Communications Agency Traficom's National Cyber Security Centre to inquire about the potential need for a guidebook for the Finnish companies on the pre-trial investigation. The meetings and information searches confirmed our initial thoughts that companies do indeed need more information on criminal investigation and the police's role in handling cybercrimes.

Furthermore, we received a good number of insightful suggestions for the potential content of the guide. For example, some of the experts remarked that companies, which had learned the hard way and fallen victims to cybercrime, often appeared more able to manage their cyber domain than those with less experience. In addition, increased general competence such as carefully designed log-filing practices and clear distribution of responsibilities between the company and its ICT service providers made the authorities' job easier, too. If no such logs on the incident are available, it may be impossible in practice to detect what has actually happened. Therefore, increased awareness would not only benefit potential victims of cybercrime but also increase authorities' possibilities to help the victims and solve the crimes.

Moreover, it emerged in the meetings with experts that the senior management of enterprises might not be responsible for decisions on information security, so it is possible that management lacks the knowledge to assess the impacts of cybercrime and, thus, underestimates the potential threats. Highlighting management's responsibility for cybersecurity as an essential part of the business could make companies more willing to prepare for the threat of cybercrime throughout the company. Furthermore, there were many other observations such as companies being uncertain of how, when and where to report a crime, and, if the offender was unknown, why too.

Based on the meetings with relevant authorities and discussions within project staff in CYBERDI, we decided to address the guidebook to companies' key personnel, i.e., persons most likely with no specific technical or cybersecurity expertise. Some spesifications resulted from the latter.

The guidebook should address the issue in a general manner that companies of various size and from various fields of business would it find applicable. We agreed that the need of information for computer security experts would have been far too specific. For the police, disclosing instructions derived directly from lessons learned in computer forensics or investigation tactics, if coming into public knowledge, could have hampered their own investigative work in the future. Focusing on non-experts also advances our goal of considering cybersecurity as a matter of whole

company. Directing companies to discuss cybercrime before falling victim to one may increase the likelihood of receiving police reports. In the best-case scenario, companies would include reporting a cybercrime to the police in their incident-handling model, if they have one. When the general policy is set, a company can assess each incident according to its framework.

Fictional case examples

An essential part of the guidebook and its design process were two fictional cybercrime cases, one describing a ransomware attack and another a case of corporate espionage. The ransomware case is presented in the Appendix II. Experts at JAMK formulated the detailed case examples from victims' perspectives. Experts at Polamk continued the work and processed the two cases from the view of criminal investigation. The point was to create two baselines displaying the main phases of pre-trial investigation and plausible interaction between the police and the victim company.

The cases served two purposes: (1) we collected feedback from authorities and companies about whether we had succeeded in 'nailing' the process adequately. Presenting criminal investigation as cases could increase the motivation of participants to review processes from beginning to end. (2) The cases are included in the guidebook. In pedagogical sense, our target audience might enjoy cases more than plain process descriptions. This form encourages readers to step into the victim's shoes and assess how the events might have turned out in their organisation, too.

Feedback from authorities and companies

The feedback process began in October 2020. As face-to-face meetings, such as joint working groups, became impossible due to the COVID-19 pandemic, we employed an online data collection platform designed for Delphi method research, and went into more detail in Teams meetings. The Delphi method is typically applied in future research, for example analysing emerging trends and operating environment, and comparing different options (Kuusi 1999). According to Kuusi (1999), the method has proven its value in situations where a problem needs to be discussed together, but a live meeting is not possible. Characteristics to the Delphi method are, for example, anonymity between the participants, the ability to conduct several feedback rounds focusing on argumentation, and the pursuit for a commonly acceptable solution (Kuusi 1999).

We used our own networks to contact cybersecurity experts such as CISOs (chief information security officers), criminal investigators, and incident responders from the public and private sectors. The purpose was to find a composition of people who would have expertise in assessing the contents and quality of the guidebook, figuring out the best practices, and identifying potential errors or misleading advice. Over 40 experts from various sectors agreed to participate in the process.

The first Delphi round was arranged between 19 October and 2 November 2020. In practice, respondents filled in an online questionnaire based on our two fictional cases of criminal investigation. The emphasis was on open-ended questions where respondents justified their opinions. The questions followed the cases' storylines

from detecting a potential crime to the conclusion. For example, we asked whether the respondents would report the crime in question, to which authorities, how quickly, and what would be their preferred method of reporting (phone call, visit or online platform). Next, we asked the respondents to evaluate our descriptions of the mapping of the crime scene, and enquired what kind of information the police would need from the victim. We also asked how they would feel if the police could not find the suspect, and whether they would still consider it useful to report the respective incident to the police. The respondents also evaluated the necessary incident-related documentation within the victim organisation, the willingness to allow live forensics, and the impact of potential media attention during the criminal process. Finally, we asked them to describe their own expectations of the police.

We received 33 replies. This was an excellent response rate noticing the fact, that several invitation links sent directly from the online platform had ended up in email spam folders and that the questionnaire was a relatively long one. Furthermore, based on wording, it seems that some answers were formulated by a group of people, so the total number of participants could have been even higher. In general, the quality of responses was good because most of the experts had explained their reasoning too.

After the first Delphi round, we spent two weeks reformulating the questionnaire. Based on the received views and comments, we revised the suggested best practices and began drafting the second questionnaire and the contents of the guidebook. For the guidebook, the objective was to respond to the concerns and questions participants had articulated in the first round. Furthermore, the actual cases were removed from the questionnaire since the focus was on presenting generally applicable sets of advice and verifying the usefulness of the content from the view of the participants. Thus, we asked participants to comment on the suggested themes and to review the reformulated best practices.

The second round comprised eight questions and was active from 16 to 29 November. Unlike the first round, participants were able to see and comment on each other's answers anonymously. The second round produced 23 completed replies, which was ten fewer than in the first round. However, the experts who responded were clearly motivated to participate. In a Delphi panel, it is always a challenge to keep participants on board through all the rounds.

The feedback we received on the two surveys was truly helpful due to the the quality of answers. The respondents, it appeared, had a positive attitude to reporting cybercrime to the police. Naturally, the observation applies only in this data since our sample of cybersecurity experts was not statistically representative and it is likely that our invitation attracted experts who perceived co-operation between the police and enterprises beneficial.

The guidebook's draft version was finished in January 2021. It circulated for comments until the end of February. In addition to the Delphi participants, comments were requested from several other experts, most of them working in the public sector. Once the guide was published in late March 2021, it received good feedback e.g. in social media.

Did you know that...

...crime is primarily investigated by the police department within whose area the crime took place? Every police department has the capacity to receive crime reports and provide instructions for securing evidence in cybercrime cases. The investigation of serious or international crime or any crime requiring significant special resources can also be assigned to the Cybercrime Centre of the National Bureau of Investigations, or the local police department may consult it as necessary. The Cybercrime Centre may also request help from the local police departments in collecting digital evidence from different parts of the country or assign cases to police departments, for example, if it has received a report from an international partner regarding a possible crime in a certain police department's area.

Illustration 2 Pink speech bubble asks, "Did you know that... and presents an interesting fact. Source: translated from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta", p. 19.

Contents of the guidebook

The guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta" [Cybercrime Is a Police Matter – A Guidebook for Enterprises on Cybercrime Investigation Process] comprises three main parts and appendices. Each part contains information and questions designed to initiate discussion and self-assessment in a company. The questions aim to lead to the adaptation of the provided information to the particular circumstances of the company. Asking the questions purposely in first person plural form (e.g. *What do we have that might be of interest to a criminal?*) emphasises collective responsibility for cyber security within the company and among its service providers.

The visual layout was also carefully considered with the aim of making the guidebook approachable and easy to browse, and of encouraging discussion on the state of cybersecurity and reporting suspected cybercrimes to the police, within companies[3]. To support that goal, we used two icons, a pink speech bubble indicating a fact box, and a blue light bulb indicating a reflective exercise (Illustrations 2 and 3).

For example, in the Illustration 2, the fact box informs of the division of work within the police. Most crimes are investigated at the local level and each police district has means to receive a police report on cybercrime. However, international crime or serious cases demanding special resources may be transferred to a special unit, the Cybercrime Centre located in the National Bureau of Investigation. Illustration 3 encourages companies to discuss about potential cybercrimes and their effects. The brief examples cover, for instance, extortion, CEO fraud, and website defacement.

3 Heli Sutinen (JAMK) was in charge of the guidebook's visual design. Samples of her work are displayed in this report as examples of the guidebook's layout.

For consideration

How would the following offences affect our company's operations?

A perpetrator finds a well-known, but unpatched, vulnerability in a company's data system, breaks into the database, copies it, and extorts the company.

▶ **What data could be best used to extort us?**

A DoS attack targeted at an online shop prevents customers from shopping and stops sales.

▶ **How would our customers see a DoS attack, and what impact could it have?**

Spyware is installed on an employee's computer to copy and forward everything the employee types, including usernames and passwords.

▶ **What would a perpetrator be able to access in our organisation?**

A country manager sends an email requesting that an urgent account transfer be made to a foreign long-term subcontractor. After making the account transfer, it is realised that the subcontractor's account number was fake and the message was not sent by the country manager.

▶ **Would such a fraud also be possible in our organisation, and how large a financial loss could we withstand?**

The content of a company's external website is defaced without proper authorisation.

▶ **How could defaced pages affect our reputation? Is this all? Could other damage be inflicted through our web pages?**

Illustration 3 Blue light bulb indicates a reflective exercise. Sub-questions help to approach the main question. Source: translated from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta", p. 6.

The appendices comprise a glossary, links to useful instructions, and guides published by the Finnish Transport and Communications Agency Traficom's National Cybersecurity Centre, references to relevant legislation, and a short introduction to project CYBERDI, and information on the process of compiling the guidebook.

Next, I describe each part in more detail.

Part one: Companies as victims and factors of reporting cybercrime

The guidebook's first part briefly describes cybercrimes and the motives behind them. It also argues for reporting cybercrimes to the police and explicates reasons for many companies failing to do so. The chapter's goal is to encourage companies to consider their own risk of falling victim and their policy of reporting cybercrime to the police. Our views derive from criminological research that is briefly introduced next, the views confirmed by our Delphi panellists. In the guidebook itself, we neither refer to the research literature nor present quotes from our cyber security experts', but solely give an overview of the determinators for reporting crime.

Skogan's (1984) exhaustive literature review suggests that reporting a crime is the victim's rational choice where consequences for society and the parties involved are properly weighted. He found out that the seriousness of an offence, potential compensation such as insurance, the probability of identifying the offender, perceiving reporting as a civic duty, preventing others from falling victim, the advice the victim receives from others and, in some cases, fear of revenge, do influence the decision. In addition, the likelihood of reporting decreases if a victim feels that they have partly contributed to the offence, for example having done something illegal or embarrassing. It also decreases if the victim has already come to terms with the issue or reported it to another body.

Three decades later, these observations have not loss their validity and remain applicable to cybercrime (see e.g. Tcherni et al. 2016; Graham, Kulig and Cullen 2020). However, since there is a lack of research related to companies' cybercrime-reporting and because we wanted to ensure that the guidebook meets the needs of its target audience, we asked about reporting from our Delphi panellists. As expected, their responses follow Skogan's (1984) scheme, as I shall point out next.

In the first Delphi round, we requested the participants to evaluate the likelihood and necessity of reporting to the police a ransomware attack, which had paralysed the company's cyber environment (See the case: Appendix II). Overall, the respondents considered reporting to the police necessary and quite likely, even if they presumed that the offender would not be identified by the authorities.

The participants grounded their estimations of likelihood of reporting on the seriousness of the crime: if the company cannot function, its whole business is in danger and the requested ransoms are high. Attempts to protect the company's reputation by concealing the crime was seen frequent but, in this case, also futile, since the partners would have noticed it already. However, some respondents, as illustrated below, considered reporting the incident unlikely. For example, a participant perceived that only known loss of personal data would be a sufficiently serious event from the point of reporting it to the police:

"Likelihood depends on the detected damage. If there is no clear indicator that personal data has been stolen, the police may not be informed."

Several respondents thought that quick recovery is what matters the most:

"It is quite unlikely that the company would ever report the matter to the police. The company is driven by a need to a normal state and, from that point of view, calling the police is unnecessary or even harmful because, instead of dedicating all resources to sorting out the incident, the company must then allocate some of its resources to the co-operation with the police."

"In my experience, companies are not willing to report these cases to the police. They are afraid of bad publicity. Furthermore, companies are not interested in what has happened in their information systems or why. The main interest is to get the business running again as fast as possible."

One participant claimed that the company's management might be worried about becoming scapegoats:

"The management or those in charge may be afraid of ending up being accused themselves."

Table 1 shows participants' justifications for why it would be necessary to report the ransomware case to the police. For this report, I categorised the reasons participants expressed in the questionnaire under two perspectives: societal; and victim-centric arguments. Victim-centric arguments gravitate around potential benefits to the company itself. In eight responses, the police were viewed as helpers, and four responses stated that criminal investigation is the only way to try to get justice. Two respondents also emphasised that the police have the authority to receive information, and an insurance company might require that the incident be reported to the police.

Societal arguments concentrated on the common good. Eight participants mentioned the importance of improving the police's awareness of the current operation environment, whereas seven considered that crimes just need to be reported because that is the way the society works and reporting is a form of social responsibility. Three pointed out that reporting might allow the police to link the reported crime to other crimes, help others to avoid similar crimes, and ultimately, increase the allocation of police resources to cybercrime.

Table 1 Societal and victim-centric arguments for the necessity of reporting the ransomware case to the police.

Societal arguments		**Victim-centric arguments**	
Reporting improves the police's awareness of the current operating environment	8	Police can then help the victim, e.g. instruct and investigate	8
Crimes should be reported	7	Necessary for the materialisation of criminal liability (or the possibility of it)	4
Reporting makes it possible to connect a crime to other cases of crime	3	A precondition for receiving insurance compensation	2
Reporting is necessary for the allocation of police resources to cybercrime investigation	3	Police have the authority to request information	2
Helping others to avoid similar crimes	3	Victim's best interest	1
Deterrence effect	1	Security awareness	1
		Fear	1
In total	**25**	**In total**	**19**

As I mentioned at the beginning of this chapter, the brief introduction to the criminological research on reporting crime above is presented here in more academic style than in the guidebook, where it initiated a reflective exercise. Illustration 4 displays the exercise in its original visual form.

How does our organisation assess the reporting of cybercrime to the police?

- **Is our assessment based on societal or business-driven reasons?**
- **Do we want to allow the police to investigate any crime targeted at us? Does our way of thinking about cybercrime differ from other types of crime? If it does, why?**
- **Do we try to identify potential crime?**
- **Do our procedures involve weaknesses that, when in the wrong hands, would place us in an uncomfortable situation or even lead to sanctions ? Would they prevent us from requesting help from the authorities? How can we fix our practices, and under whose leadership?**
- **Are our decisions affected by the severity of the situation or the damage caused?**
- **Can we be reimbursed by our insurance, and does this require that the crime is reported?**
- **Can we receive compensation from the perpetrator as a result of a criminal process?**
- **Are we afraid of publicity during the criminal process? Can our public image be impacted through our actions?**
- **Can we identify any other benefits from reporting a crime, even if the perpetrator cannot be caught?**
- **Are we afraid of retribution if we contact the police?**
- **Do we know that a single case may need to be reported to several authorities?**
- **How do we assess expected overall benefits in relation to the inconvenience caused by criminal investigations in our company?**

Illustration 4 Example of a reflective exercise "How does our organisation assess the reporting of cybercrime to the police?" Source: translated from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta" p. 11.

Part two: Cybercrime investigation

The guidebook's second part mostly applies nationally, so it is described here superficially. The section focuses on pre-trial investigation as the first stage of the chain for processing criminal matters in Finland (Illustration 5). It demonstrates the main steps of criminal investigation from reporting a crime to the point where the National Prosecution Authority considers the charges if the case proceeds that far. The guide, also, provides references to relevant national legislation and for looking up details, recommendations for further reading and links to instructions provided by the National Prosecution Authority. The pre-trial investigation process is described by using a chart.

Description involves the following themes:

- The purpose of pre-trial investigation
- How the police process a reported crime and communicate to the injured party
- Awareness of two types of offence in the Finnish Criminal Code: complainant offences and offences subject to public prosecution. Knowing the difference is essential because a complainant offence proceeds to pre-trial investigation, with a few exceptions, only after the injured party has issued a penalty demand.
- International co-operation
- Extent of a pre-trial investigation (e.g. grounds to restrict the investigation)
- Co-operation between the police and prosecutor
- Preliminary investigation report
- Consideration of charges
- Publicity during a criminal process

Due to "invisible" harm and digital evidence, detecting and solving a cybercrime differs from traditional crime. The differences are small, but victims need to understand that cybercrime might go unnoticed if nobody is monitoring the cyber domain, and digital evidence can be tampered with as easily as fingerprints.

We introduced two fictional examples of cybercrime cases to address the aforementioned problem. They illustrate that the perpetrators had taken many actions before the victim noticed the incidents. The first case depicts a small company hit by a ransomware attack (Appendix II). The attacker manages to interrupt the company's entire business, but the company recovers from it because it has solid and up-dated back-ups and sought help from the competent authorities quickly. Furthermore, due to the victim's adequate log-filing practices, the police, in co-operation with other bodies, were able to demonstrate the course of events.

Our second case introduces a listed company, which begins to suspect a potential case of industrial espionage. The criminal investigation reveals that the perpetrator received unexpected help from the inside, from e.g., current employee, and got the company to strengthen the connection between cyber- and physical security. When acquainting themselves with these cases, we encourage readers to adopt the positions of the victim organisations.

Illustration 5 The guidebook focuses on the first stage of the chain for processing criminal matters in Finland, i.e. pre-trial investigation. The other stages are consideration of charges, court proceedings and enforcement of penalties. Source: translated from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta", p. 13.

Part three: Practical advice

The Delphi panellists reviewed the guidebook's draft contents, and had a chance to propose new subject matters, too. They considered that the primary focus of the advice section should be on illustrating what kind of information the police may need during a cybercrime investigation (96% of respondents), explaining how companies can improve the probability of solving a crime (74%), and instructing how to report to the police in practice (74%). Therefore, the third part of the guide establishes the following five types of advice:

- The kind of information the police may need during a cybercrime investigation
- How to improve the probability of solving a crime
- Reporting to the police
- Reporting to all relevant authorities
- Some of the key authorities and agencies in the domain of Finnish cybersecurity

In this report, the first two themes will be illustrated, since they are not as country-specific as the rest of the themes. However, only Finnish experts have reviewed the advice so far. Next, I briefly describe the main points of the remaining three topics of advices, before engaging fully with the first two.

Reporting to the police

The guidebook walks the reader through the process of reporting a crime in Finland. The main ways to report a suspected cybercrime to the police are either by filling in an electronic form on the police website or visiting a police station.

The police receive and handle reports on cybercrime like any other crime, so the instructions on the police website[4] are general and applicable to a bicycle theft onwards. However, the police have recently inserted new sections on cybercrime on their website, so there is more information available today than when development of the guidebook began. Anyway, we give instructions on the typical matters and technicalities such as stating that submitting the online form on behalf of a company requires digital authorisation from a person who has the right to represent the company, and that providing direct contact details of the people in charge of the company's cyber domain speeds up the first steps of evidence gathering. The section also recommends the companies to pre-plan the process of reporting a suspected cybercrime and to establish a clear company policy for crime reporting. A reflective exercise with references to the relevant pages of the guidebook leads the reader to reflect their company's policy. The questions include:

- What kind of crimes would we report to the police? Why or why not?
- What would we do if a detected computer security breach seemed to escalate into a potential crime? In our company, who must be informed?
- Who decides on reporting to the police?
- Is it clear to us how to verify the first steps of evidence gathering?
- How do we communicate about a crime inside and outside the organisation?
- If the case is reported to the police, who have the authority to act as contact persons? In addition to a company representative, the police also need a direct contact to the ICT personnel.

Reporting to all relevant authorities

The section about reporting incidents in cyberspace is meant to help companies navigate among four types of public authorities that request reports on incidents or cybercrime in Finland for different purposes. For example, the police conduct pre-trial investigation.

Unfortunately, reporting to all relevant authorities at once is not yet possible. We highlight that some of the reports are voluntary, but there are also mandatory reporting requests drawn originally from EU legislation. For example, the General Data Protection Regulation (GDPR) sets obligations for data protection. Cybercrime,

4 The police website in Finland: https://poliisi.fi/

which involves a breach of personal data security and can endanger the rights and freedoms of natural persons, must be brought to the attention of the supervisory authority – in Finland, the Office of the Data Protection Ombudsman – within 72 hours. Likewise, the EU's Network and Information Security Directive (the NIS Directive) stipulates that critical infrastructure providers must report information security incidents to their sector's supervisory authority.

Reporting to the police and the Finnish Transport and Communications Agency Traficom's National Cybersecurity Centre is voluntary (except in situations where the Cybersecurity Centre is the supervisory authority), but highly recommended at a low threshold. We also encourage companies to discuss and determine whether they are obliged to report elsewhere, too (Illustration 6). For example, contracts or sector-specific legislation may bind them. Sometimes, it may also be preferable to notify partners or clients even if it is not mandatory, especially if there is a risk that the incident can escalate beyond the company.

For consideration

- **Are we obligated or is it preferable to report the case to another party?**
- **What does the governing, e.g., sector-specific, legislation have to say about this?**
- **What do our agreements and commitments obligate us to do?**
- **Is it possible that classified official information has ended up in wrong hands?**
- **Is it possible that our partners or customers are also at risk?**

Illustration 6 A reflective exercise for determining to which other parties a cybercrime could be necessary to report. Source: translated from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta", p. 30.

Some of the key authorities and other agencies

The guidebook briefly covers preparing for cybercrime and, as a part of this, introduces seven bodies, which can help Finnish companies before, during, or after an incident. These bodies are the police, the Finnish Transport and Communications Agency Traficom's National Cybersecurity Centre, the Security Intelligence Service, the Office of the Data Protection Ombudsman, the National Emergency Supply Agency, and support from peers such as other cybercrime victims, and private companies or third-sector entities. This chapter encourages companies to look after their cyber domain, since it is one of the best ways to prevent a crime or mitigate its consequences. An honest (self) evaluation of the status of company's cyber domain serves as a baseline for improvements, and learning the range of public and private services might help companies to decide how and where to turn to with potential problems in their cyber domain.

Furthermore, a reflective exercise (Illustration 7) encourages companies to determine the relevant bodies they find necessary to contact in a cybercrime incident.

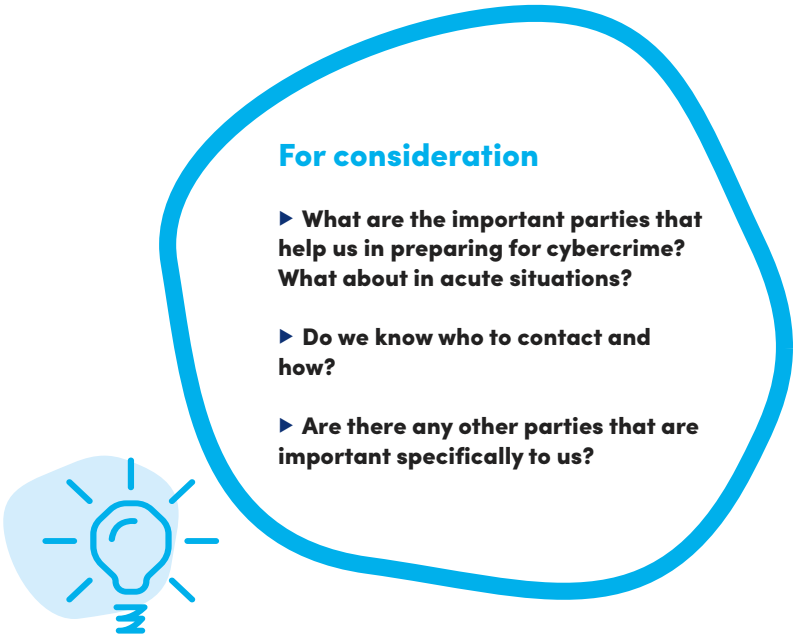

Illustration 7 A brief reflective exercise helping to determine the relevant bodies from where to seek help before, during, or after a cyber incident. Source: translated from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta", p. 37.

The kind of information the police may need when investigating a cybercrime in an enterprise[5]

The pre-trial investigation of a crime targeted at an information or communications system typically requires co-operation between the police and the victim company. Therefore, the victim needs to reserve resources for this co-operation.

Criminal investigation combines traditional police work – such as talking to people who might know about the incident and submitting information requests – with computer forensics. For example, by talking to or interrogating the company's personnel, the police can try to find out what they know about the incident or whether someone has made any observations relevant to the case. Information requests serve as attempts to identify the suspect and link the case to other domestic or foreign incidents.

Computer forensic investigators construct a picture of the company's cyber domain as a crime scene. They also gather and analyse digital evidence related to the course of events or the suspect with court-proof methods. In the best-case scenario, the actions of the company and authorities are mutually supportive, and joining forces results in an outcome none of them could have achieved alone.

The police are often asked for universal advice on how enterprises as victims can obtain evidence from information and communication systems by themselves. However, the relevant evidence, techniques and tactics depend on the case. The police collect evidence – or instruct the victim to do so – and advice on other necessary measures depending on the case. Early contact with the police ensures that the evidence is not destroyed or transformed inadmissible.

1. Is it known whether the injured party has the situation under control or does the attacker still have access to the computer systems? How is this known?
   - Does the injured party have a plan of action? What kind?
2. What kind of damage has the injured party suffered and, according to estimates, how widely?
   - Can the problem escalate beyond the company?
3. What kind of structure, connections and interdependencies do the information systems have?
   - Who owns the information systems? Is it the company itself or service providers and, if service providers, which ones?
   - How are the roles and responsibilities defined? Who are the owners of each type of data and what has been agreed on handling the data?
   - If the information systems have dependencies beyond the company, for example, with other company's systems, are the log files on data traffic available?
   - What kind of information security solutions protect the information systems and data? Have there been any alerts, which could be related to the incident?
   - In addition, maintenance of information systems, version control, update cycles and differences between timestamps are important knowledge.

5 This chapter is a translation of pages 33-34 from the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta."

4. Has anyone gathered or analysed the evidence? Who has documented the measures and how?
    - Have events and measures been put in a timeline, for example?
    - Has any other body such as Traficom's Cybersecurity Centre or a private computer security specialist conducted some analyses?
5. What kind of logging policy has been in the company's information systems and their different parts?
    - Are there some traces available other than those already gathered?
    - Are there some relevant devices left on but in offline mode, waiting for evidence collection?
    - Have some relevant devices been shut down or reinstalled that may have caused a loss of evidence?
    - Is it necessary or possible to temporarily increase the level of logging?
6. What kind of backups are available?
    - Do they cover functions and systems relevant to the case? Do the timespans reach far enough?
7. Are there other devices, which may hold some evidence?
    - During a criminal investigation, the police may request infected device for investigation or capture computer forensic images on site. The aim is to cause as little disruption as possible to business.
8. Is it possible to rule out an insider suspect?
    - Do some people have access to computer systems in such ways that it may affect the evidence?
    - Who holds administrative privileges?
    - Who has access to the information system and security architecture descriptions and documentation?
    - Has somebody's user credentials been used for abnormal log-ins?
    - Do partners have access to company's information systems? Which ones?
    - Have former employees' user credentials been de-activated?
9. Is there any knowledge of what kind of confidential data has been potentially endangered?
    - Who could benefit from the confidential data?
10. What is the nature of the attack?
    - Are there signs of a targeted attack?
    - Can the real target or motive be something other than what it appears to be at first?
11. Has the company previously been a victim of cybercrime?
    - Did it then report to the police or other authorities?
12. Have the staff or CCTV monitoring noticed anything abnormal?
    - Do outsiders have access to the company premises? Have there been observations of abnormal events?
    - Have there been abnormal comments in social media or phishing campaigns?
    - Have the staff participated in external events where their device could have been infected?
13. Is there a need for external communication?
    - External communication should be discussed with the police beforehand, because it may affect the on-going criminal investigation.

How to improve the probability of solving a crime[6]

Answering the following questions illustrates the company's readiness to support the police in the criminal investigation. Many of the sections below may feel challenging, and it is unlikely that all the questions posed in them have direct answers. However, the questions help companies to identify some problem areas. In a wider sense, commitment to working on cybersecurity also improves the capacity to solve potential crime. The latter can be supported by using the self-assessment tools, as mentioned earlier in the guidebook.

1. Are we the best experts of our cyber domain?
   - Have we recently defined and documented the structure of our cyber domain and its interdependences, maintenance, update cycles, information security solutions and connections beyond our own systems?
   - Who is able to recognise our normal network traffic and thus detect anomalies?
   - Who has access to the big picture? It may be an assemblage of several outsourced and internally managed systems or services, in which case understanding the whole is crucial.
2. Have we defined, protected and limited access to data critical to our business?
   - For example, personal data and data on product development may be critical information.
   - It is easier to assess damage, for example in a case of a data system breach, if it is known where the different types of data are kept, how they are protected and how access to them is limited and controlled.
3. What is our (or our contractor's) capacity to monitor and log changes in information systems?
   - How do we recognise and report anomalies?
   - Do we collect widely enough log files and store them long enough keeping them separate from the other systems? Do we limit access to log files and prevent the possibility of their being tampered with?
   - Do we (or our contractors) have the ability to make a copy of a log file and to store it intact, if necessary, for example if a decision on reporting to the police has not yet been made, but a cybercrime seems likely?
4. What do our contracts state about service providers' responsibility to collect and disclose log files?
   - Who owns the log files? Under what conditions are they available and what is available in a case of cybercrime? A company and service provider can agree in advance on an obligation to document a cyber-attack for its potential further investigation.

6 This chapter is a translation of pages 42-43 of the guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta."

5. What is our policy regarding backups?
   - Do we take backups regularly, store them long enough and keep them separate from other information systems? Keeping them separate decreases the risk that a ransomware attack or server failure, for example, would destroy the backups, too.
   - Do we also protect our backups with a password and encryption in order to prevent leakage of plain text data?
6. Are we aware that many digital traces, which could be utilised as evidence of crime, vanish relatively quickly from information systems?
   - Quick contact with the police ensures that the evidence is secured in an admissible way.
7. How do we handle acute, significant cybercrimes, which require rapid decision-making?
   - It is recommended to plan a procedure for acute situations, such as who makes the decisions and what is emphasised in the decisions. Crucial decisions may need to rely on insufficient information.
   - Disconnecting an infected device from the network may be the only way to interrupt the attack and prevent wider damage. On the other hand, it might also be a signal of discovery to the criminal, indicating that is time to start cleaning up the traces. Furthermore, essential evidence may be easily lost if an infected device is disconnected and turned off.
   - In some cases, creating a forensic image takes no more than a moment, so it is unlikely to worsen the overall situation. However, each event is unique so no universal advice applies.
8. Are we aware that there may be a connection between cybercrime and events in the physical world?
   - Do we look after security on the company premises?
   - Do we encourage employees to report abnormal events in the cyber and physical environments?
   - Who in our company has an overall view of all abnormal events?
9. Do we understand the purpose of the pre-trial investigation?
   - In the pre-trial investigation, the police aim to find out about and prove the course of events with appropriate evidence, and to identify the suspect.
   - All victims are encouraged to contact the police immediately. Rapid contact is important in cases where appropriate preliminary measures to secure the digital evidence cannot be taken care of otherwise.
   - What are the capabilities of our company or its service providers in recognising and capturing digital evidence, documenting the process, and storing the copies intact and unaltered?

CONCLUSION

The purpose of this report was to describe the contents and process of compiling the Finnish guidebook "Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta" [Cybercrime Is a Police Matter – A Guidebook for Enterprises on Cybercrime Investigation Process] without going into country-specific details. As I stated at the beginning, project CYBERDI received requests to translate the guidebook into English for foreign stakeholders. However, a direct translation would not have met the needs of the initial target abroad, since most of the content is country-specific. Therefore, this report is for them who are seeking new initiatives to increase organisations' awareness of the role of the police in cybercrime prevention.

Overall, there is a need to improve co-operation between the police and enterprises as actual or potential victims to cybercrime. Increasing knowledge of cybercrime investigation is, we believe, one way to do this. Even today, companies seldom report cybercrimes to the police, or delay it for too long resulting in the disappearance of the digital traces.

Educating companies or other target groups in cyberthreats would benefit from transnational co-operation. Even though some of the materials would need adjusting to a national context, much of it would be shareable. For example, when project CYBERDI began to plan the guidebook for Finnish companies, we were unable to find international exemplars, which would have helped us to determine what the companies would like to know about criminal investigation, or even whether anyone would be interested in such a material. I hope that this publication shows direction and paves a way that others will find useful in their respective pursuits.

Personally, I would be interested to know whether the two translated sets of advice here, i.e. 1) The kind of information the police may need during a cybercrime investigation, and 2) How to improve the probability of solving a cybercrime, would be applicable to other countries, and how other experts could improve them. There is also a need for research into the handling of cybercrime in organisations, such as what kind of support the victim organisations expect from public authorities, what kind of offences organisations would be willing to report and why or why not, and whether campaigns to increase awareness of cybercrime are actually effective. Therefore, I am looking forward to learning more of these issues from experiences in other countries.

REFERENCES

Graham, A., Kulig, T.C. and Cullen, F.T. (2019). "Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice", *Policing: An International Journal*, 43(1), pp. 1-16. https://doi.org/10.1108/PIJPSM-07-2019-0115

Kuusi, O. (1999), Delfoi-menetelmä. [Delphi method] Available at: https://metodix.fi/2014/05/19/kuusi-delfoi-metodi/ Accessed 28.5.2021.

Leppänen, A. & Kankaanranta, T. (2018). Co-production of cybersecurity: a case of reported data system break-ins. *Police Practice and Research*, https://doi.org/10.1080/15614263.2018.1525382

Skogan, W. G. (1984). Reporting crimes to the police: The status of world research. *Journal of Research in Crime and Delinquency*, 21, 113–137.

Tcherni, M., Davies, A., Lopes, G. and Lizotte, A. (2016). The dark figure of online property crime: is cyberspace hiding a crime wave?, *Justice Quarterly*, 33(5), pp. 890-911.

APPENDICES

Appendix I: About the CYBERDI project

Project CYBERDI - Cybercrime prevention, awareness raising and capacity building by RDI on modern cyberattacks
CYBERDI's purpose is to strengthen the competence of JAMK University of Applied Sciences (coordinator) and the Police University College of Finland (consortium partner) in detecting and investigating cybercrime. The project also increases awareness of digital threats and reinforces partnerships. CYBERDI was carried out between October 2018 and December 2021, and was funded by the Ministry of Education and Culture of Finland.

JAMK University of Applied Sciences & JYVSECTEC
JAMK University of Applied Sciences, located in Finland, is an international institute of higher education with expertise in eight different fields of study. JAMK has about 8,000 students and 740 staff members. The basic tasks of JAMK include education leading to degrees, RDI and continuing education and services. Within six focus areas JAMK develops its own competencies and is strongly connected to the development of the region. Its focus areas are education expertise and business, bioeconomy, multidisciplinary rehabilitation, applied cybersecurity, automation and robotics and tourism.

JYVSECTEC - Jyväskylä Security Technology is the leading independent cyber security research, development and training centre in Finland. We operate as a part of JAMK University of Applied Science's Institute of Information Technology, which guarantees us a multidisciplinary network of experts at our disposal. Our areas of expertise include cyber security, incident response, emerging technologies and IT technologies.

https://www.jamk.fi/

Police University College
The Police University College (Polamk) is Finland's only police educational institute – a centre of expertise in police education, research and development. It has a special position in the field of higher education being simultaneously a university of applied sciences and a police unit. Polamk produces research for developing safety in society. It engages in applied research and development, serving police education, planning and the development of policing and internal security.

https://polamk.fi

A fictional example of the investigation of ransomware

How would you feel if you received a message demanding you to pay EUR 350,000 within the next 48 hours or your business secrets would be leaked to the public? The demanded amount would increase by 30% every six hours.

1. Crime is identified

RealSignal is a company with 50 employees, and it takes care of its own cyber domain. In the morning, the CEO receives an email on their mobile phone, saying that the company's data systems have been breached, data has been copied and malware has locked workstations. The message demands the company to pay EUR 350,000 in a cryptocurrency within the next 48 hours or the workstations will remain locked and business secrets will be leaked in public. The demanded amount will increase by 30% every six hours. The same message is also displayed on the CEO's computer screen. The CEO, a two-employee ICT team, unit managers and the communication manager meet to investigate the situation. The Board of Directors is also informed immediately. The situation is seriously threatening the company's business operations. The ransomware has spread extensively in systems, and no workstation has yet been unlocked.

RealSignal has a pre-defined operating model for cybercrime. Following the model, the company management decides that the police should investigate the case and they have a penalty demand against the offender. Furthermore, RealSignal requests help from the National Cyber Security Centre of the Finnish Transport and Communications Agency (NCSC-FI), and allows the authorities to work together to resolve the situation. The company management understands that personal data may be at risk, requiring them to submit a notification to the Office of the Data Protection Ombudsman without any delay, no later than within 72 hours.

2. Reporting the crime

RealSignal's CEO is at a police station explaining what happened. The CEO has an identity card, a copy of the ransom message shown on the screen, the ransom email and the contact details of the ICT manager with them. The police officer writing the report immediately consults the police department's computer forensic investigator. Preliminary offences are registered in the case: aggravated extortion, aggravated unauthorised use, and damage to data. The CEO says that they have asked for help from NCSC-FI and permits the authorities to exchange information. Before reporting the crime to the police, RealSignal decided to have the case investigated. As aggravated extortion is subject to public prosecution, the injured party's opinions on penalty demand has this time no impact on the start of investigations. [Author's note: There are two types of offences in Finland, a complainant offence and an offence subject to public prosecution. The basic principle is that initiating an investigation of a complainant offence requires victim's penalty demand against the offender.]

▶ While the criminal investigation is based on the law, it is always a case-specific process. As a result, the processing of a case may be affected by a number of factors, and the investigation process does not always proceed as described in this fictional example. The purpose of the example is to illustrate what cybercrime and its investigation may look like from a company's perspective without digging deeper into any investigation tactics.

3. Securing the evidence

The police's computer forensic investigator calls RealSignal's ICT manager. They discuss the current state of the case, the structure of the company's cyber domain and consider where evidence might be available. The computer forensic investigator also wants to ensure that the company knows how to prevent the damage from spreading and how to start recovering. As instructed by the police, RealSignal acquires and documents system logs and backups, and hands over an infected workstation to analyse the malware. Once the evidence has been secured, the company no longer needs to be afraid that the re-installation of the system would destroy any evidence.

4. The investigation starts

The local police department appoints a criminal investigator and head of investigation for the case. The prosecutor is notified of the case, and the police and prosecutor are already engaged in cooperation during the investigation. The criminal investigator contacts the computer forensic investigator, who has requested evidence to be secured in data systems, the Cybercrime Centre of the National Bureau of Investigation, and NCSC-FI with RealSignal's permission. The criminal investigator also contacts RealSignal's CEO to notify them of the start of the investigation and the next steps.

5. The investigation proceeds

The police talk to RealSignal's employees and start to identify the course of events using digital evidence. The company's help is required to identify its cyber domain. The police investigate whether similar cases have occurred before in Finland or abroad. The log data shows that an employee opened a malicious email attachment that was sent by SatakuntaVision, a long-term subcontractor. The attachment slipped into a longer message chain in Finnish.

6. The investigation expands to the subcontractor

The police contact SatakuntaVision. The investigation expands, as no-one in the company had noticed the incident. Whether anyone else can access the employee's email account and whether any data systems are at risk need to be identified. SatakuntaVision is an operator critical for societal activities, as laid down in the NIS directive. Therefore, it also submits a statutory report to its supervisory authority through NCSC-FI. As the perpetrator also had access to personal data through an Office 365 account, the Office of the Data Protection Ombudsman must also be notified.

Did you know that...

you may get mixed up with the names of key organisations if you are not paying attention? The Cybercrime Centre operates under the National Bureau of Investigation, while the National Cyber Security Centre is part of the Finnish Transport and Communications Agency. A good rule of thumb is to focus on the scope of activity indicated by the names: the police investigate crime, while NCSC-FI sees to the maintenance of cybersecurity in general.

7. A scam targeted at a partner placed RealSignal at risk

By working together, SatakuntaVision's service provider, NCSC-FI and the police identify that the Office 365 account of the SatakuntaVision employee had already been hacked four months earlier. Messages were forwarded to an email address, which hints at Finnish skills. RealSignal's logs show that the perpetrator was able to navigate in the data system by exploiting the workstation of the employee who opened the attachment, and found a few password hashes, one of which belonged to the system administrator. The perpetrator was able to crack the administrator's **weak password (Real$ignal2018)** and capture the company's domain name (realsignal.fi). The file processing log reveals that the perpetrator had downloaded 45 GB of data from workstations, file servers and email systems, and had transferred it to an Amazon cloud server. The perpetrator was able to spread malware to all workstations and servers connected to the company's network.

8. The police continue to investigate the perpetrator's identity

The police use the digital evidence to look for other clues of the perpetrator's identity and, together with the other parties involved, investigate the use and structure of the malware. The police send requests for information to foreign service providers regarding, for example, the Amazon cloud server, the address to which the SatakuntaVision employee's messages were forwarded, and the address from which RealSignal's CEO received the ransom message. For example, the police are interested to know who logged in to the account and from which IP address, and whether the same elements are connected to other crime.

In conclusion

In this fictional example, the police were able to identify the course of events in cooperation with other parties, and are now continuing to identify the perpetrator's identity. RealSignal's comprehensive logging practices and understanding that the evidence must be protected before the cyber domain can be restored after the crime had a significant impact on identifying the course of events. Contacting the authorities ensured the correct course of action. The separately stored comprehensive backup copies helped RealSignal recover, and therefore its business operations did not suffer any unrecoverable damage, although the crime was a massive blow. RealSignal learned various lessons from the case, and it assessed its operating methods critically and decided to change them. SatakuntaVision deployed multi-factor authentication so that Office 365 accounts cannot be accessed by only using a username and password.

POLIISI
POLICE UNIVERSITY COLLEGE

The Police University College of Finland, in collaboration with JAMK University of Applied Sciences, developed a guidebook entitled “Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta” (Cybercrime Is a Police Matter – Guidebook on Cybercrime Investigation Process for Enterprises). The guidebook was published in March 2021 as part of project CYBERDI’s campaign to increase awareness of cyberthreats. Its purpose is to increase companies’ knowledge of cybercrime, encourage the personnel to report cybercrime to the police, and support the companies in setting up procedures to help resolve a potential crime.

This report introduces our guidebook to readers and explicates the way we compiled it. The report originates from the encouraging feedback received from various Finnish authorities and companies, but also from requests to have the guide translated into English. Unfortunately, a direct translation would not have been reasonable as such. Each national jurisdiction represents a unique system. Our guide opens up the pre-trial investigation of cybercrimes in Finland.

Police University College • Vaajakatu 2, FI-33720 Tampere • tel. +358 295 480 121 • www.polamk.fi