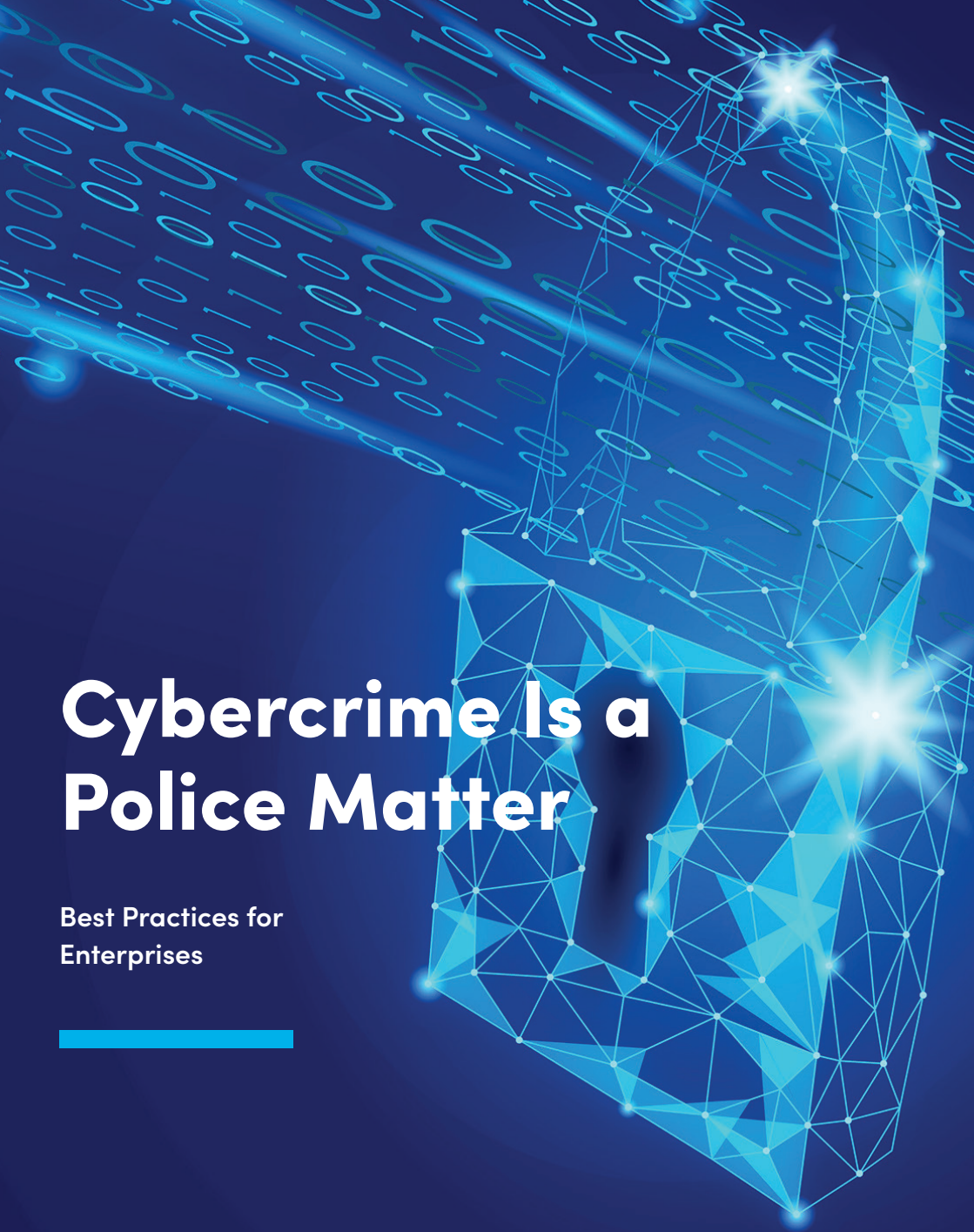


Cybercrime Is a Police Matter

Best Practices for Enterprises

oletietoinen.fi

Ministry of Education and Culture

POLIISI
POLICE UNIVERSITY COLLEGE

JYVSECTEC
by jamk

What kind of information the police may need when investigating a cybercrime in an enterprise?

An Example of the Best Practices

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.

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 analysis?

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?

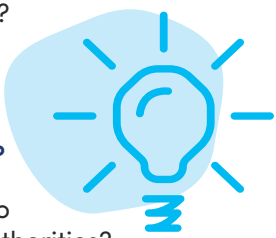
- Do some people have access to computer systems in such ways that it may affect the evidence?
- Who holds administrative privileges?
- Who has access to the information system and security architecture descriptions and documentation?
- Has somebody's user credentials been used for abnormal log-ins?
- 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?

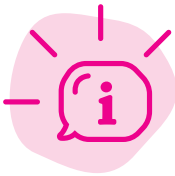
13. Is there a need for external communication?

- External communication should be discussed with the police beforehand, because it may affect the on-going criminal investigation.

The Police University College of Finland and 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 is targeted to key personnel of companies and its purpose is to increase knowledge of cybercrime, encourage the reporting of cybercrime to the police and help to refine procedures used in solving potential crimes.

Companies gain optimal benefit from the guide, if they use it to support discussion and self-assessment.



▶ The guidebook is available only in Finnish. However, download here an English report on the preparation of the guidebook. The report includes for example the best practices.

Contact JAMK University of Applied Sciences:
jyvsectec@jamk.fi | www.jamk.fi

Contact Police University College:
tutkimus.polamk@poliisi.fi | www.polamk.fi

Project CYBERDI

CYBERDI's purpose is to strengthen the competence of JAMK University of Applied Sciences and the Police University College in detecting and investigating cybercrime, as well as to become profiled as cybercrime experts at the European level. The project also increases awareness of cybercrimes in enterprises and among social media users. CYBERDI was carried out between October 2018 and December 2021, and was funded by the Ministry of Education and Culture of Finland.

Author: Anna Leppänen, Polamk | Graphic design: Iina Kolari & Heli Sutinen, JAMK

oletietoinen.fi

Ministry of Education and Culture

POLIISI POLICE UNIVERSITY COLLEGE

JYVSECTEC by jamk