Unified Cybercrime Investigations:

Cross-Organizational Investigative Readiness

Odin Heitmann[1,3], Katrin Franke[2,3], Sokratis Katsikas[3], Håvard Aalmo[1]

1. National Criminal Investigation Service, Norway
2. Kongsberg Defence & Aerospace, Norway
3. Norwegian University of Science and Technology, Norway

1. The problem

In today's world of cybersecurity, it is not a question of *whether* an organization will experience a cyber attack, but rather a matter of *when* it will happen. These incidents can cause significant disruption and financial losses to organizations. **Forensic readiness** is becoming increasingly crucial as it can help maximize the use of digital evidence and reduce the investigative cost after an attack [1]. It can also aid law enforcement in identifying and prosecuting cybercrime perpetrators.

Organizations and law enforcement agencies often have **divergent areas of focus**. Unfortunately, this leads to a lack of a comprehensive overview, causing a fragmented approach where each organization and agency works independently. This **siloed approach** can compromise the quality and success of criminal investigations, resulting in **inadmissible evidence** in court and increased costs for the organizations involved.

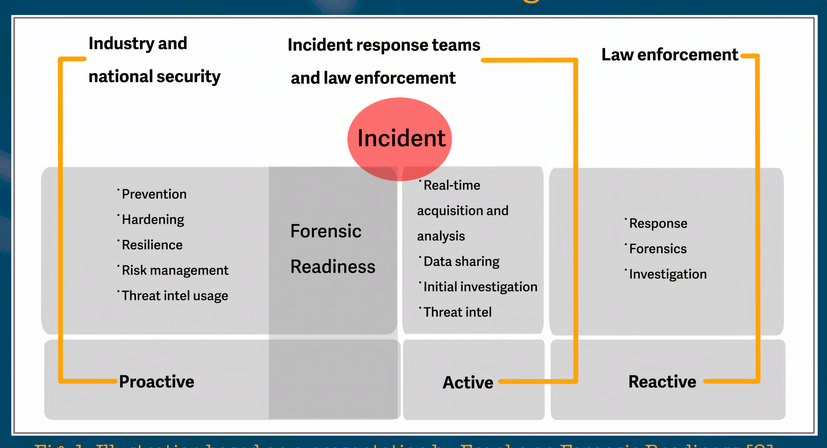

Fig. 1: Illustration based on a presentation by Franke on Forensic Readiness [2]

2. Looking forward

This PhD project aims to bridge the gap between the industry, national security, and law enforcement to **be better prepared** to tackle the challenge of cybercrime. The motivation is that having admissible evidence is crucial for law enforcement when prosecuting cybercrime cases such as the **Hydro case** in a court of law. An organization's forensic readiness level can impact how potential digital evidence is identified and collected. Law enforcement depends on what evidence the industry can provide, and the industry can benefit from law enforcement investigating cybercrime cases.

We aim for **cross-organizational investigative readiness** [3], where all stakeholders share focus areas.

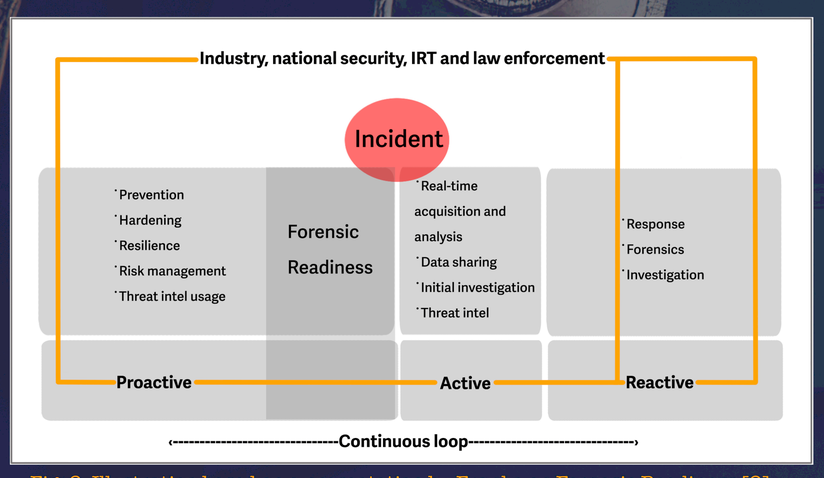

Fig. 2: Illustration based on a presentation by Franke on Forensic Readiness [2]

3. Research question

How can digital forensic readiness for the industry in critical national infrastructure - and information sharing - affect the outcome of a cyber attack and the subsequent investigation and cyber threat intel?

4. Hydro - A real-life example

One instance of successful cybercrime occurred in 2019 when Norsk Hydro fell victim to a major cyber attack [4]. Norsk Hydro is a leading manufacturer of aluminum and one of Norway's largest hydropower producers, with operations in over 50 countries, 34,000 employees, and a turnover of 159 billion NOK in 2018 [5].

The consequences of a successful cyber attack could be devastating, as was the case for Hydro. The cyber attack **affected Hydro globally**, with the Extruded Solutions division facing the most operational challenges and financial losses. The estimated cost for Hydro in 2020 was around **800 MNOK*** [4].

The National Cybercrime Centre in Norway is still investigating this crucial case four years after the attack. Although the Hydro criminal case is not yet concluded, it has **revealed five males** who are suspected of carrying out the actual attack, along with **56 other suspects**. These suspects include individuals involved in money laundering, cryptocurrency activities, and providing various services [6]. The attacks by this group might have affected over **1800 victims** in **71 countries** [7].

**800 MNOK is equivalent to around 70.801.000 EUR.*

5. Methods

Literature review

Expert interviews

Case study

Experiments

6. Preliminary results

One paper exploring the relationship between digital forensic readiness and criminal investigation.
See red QR-code on top.

Exploring Digital Forensic Readiness:
A Preliminary Study from a Law Enforcement Perspective

7. Acknowledgments

This research is funded, in whole or in part, by The Research Council of Norway [338691], and the Norwegian National Criminal Investigation Service.

8. References

1. Rowlingson, R.: A ten step process for forensic readiness. International Journal of Digital Evidence 2(3), 1-28 (2004)

2. Franke, K.: Presentation at Dagstuhl Seminar (February 2014)

3. Heitmann, O., & Franke, K. (2023, November). Exploring Digital Forensic Readiness: A Preliminary Study from a Law Enforcement Perspective. In Norsk IKT-konferanse for forskning og utdanning (No. 3).

4. Norsk Hydro ASA: Cyber-attack on Hydro (2020), *https://www.hydro.com/ en-NO/media/on-the-agenda/cyber-attack/*

5. Bryhn, R., Gram, T.: Norsk Hydro (2023), *https://snl.no/Norsk_Hydro*

6. E24: Kripos mener å ha oppklart løsepenge-angrepet mot Hydro (2023), *https://e24.no/naeringsliv/i/EQ5m6K/ kripos-mener-aa-ha-oppklart-loesepenge-angrepet-mot-hydro*

7. Europol: 12 targeted for involvement in ransomware attacks against critical infrastructure (2023), *https://www.europol.europa.eu/media-press/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure*

odin.heitmann@politiet.no

Images generated with Bing Creator / Dall-E