# A case study of a municipality phishing attack measures - towards a socio-technical incident management framework

Grethe Østby [1], Stewart James Kowalski [1]

[1] *Norwegian University of Science and Technology, Teknologiveien 22, Gjøvik, Innlandet, Norway*

**Abstract**

During the Corona-crisis, the number of data breaches and hacking increased rapidly. For some organizations it was difficult to handle both the Corona-crises and such attacks. A decision made to prevent this overload of crisis, happened in Gjøvik municipality, where they closed their email-system and shut down macros in their applications to prevent an overload situation. In this work-in-progress paper, we have analyzed their decision in a combined socio-technical and crisis management context and suggest such framework to do analysis and make right decisions to prevent data breaches and other organizational cyber-crimes from succeeding, but also to prevent an overload of crisis situations at the same time.

**Keywords** [1]

Incident management, Data breaches prevention, Cyber-attack prevention, Socio-technical analysis, Crisis management analyses, SBC-analyses, NIST-analyses.

## 1. Introduction

Recent studies in Norway show that cyber-attacks on organizations are increasing both in quantity and in scope [1]. The results also suggest a clear shift from attack on machines to attack on humans.

The Norwegian Parliament was subject to such a social engineering attack in August 2020 [2], [3]. A spear phishing attack against several email-accounts took place. In the Parliament several technical measures had been previously implemented, but new social engineering attack approaches circumvented them. Social engineering attacks were also performed against other levels of government in the first period of the Covid19 pandemic (Corona crisis), including a number of Norwegian municipalities [4].

To prevent such attack from succeeding, Gjøvik municipality decided to stop all emails with word, excel and pdf attachments until they could gain control over these type of attacks [5]. By sandboxing these types of attachments, the municipality thereby limited the opportunity-curve as presented by Kowalski in [6] pg. 57 (socio-technical control capabilities over time). However, since the criminal opportunity curve demonstrates that attack methods often out pace control methods it is unclear how this control method will protect Gjøvik municipality, especially if the number of attempts to data breaches will increase in the same rapidly way as it did during the Corona crisis.

In this paper we present the decision made to deal with the social engineering attack method by Gjøvik municipality in a socio-technical context, and further investigate if such controls can lead to a combined crisis management and socio-technical action framework to prevent attacks.

After the introduction we present the background in section 2, before presenting relevant literature in section 3. The research approach is presented in section 4, before presenting the case with interviews and analyzes in section 5. Finally, in section 6, we conclude and suggest future research based on our study.

Proceedings of the 7th International Workshop on Socio-Technical Perspective in IS Development, October 14–15, 2021, Trento, Italia
EMAIL: grethe.ostby@ntnu.no (A. 1); stewart.kowalski@ntnu.no
ORCID: 0000-0002-7541-6233 (A. 1); 0000-0003-3601-8387

## 2. Background

In the Dark numbers survey from 2020 [1], results showed that 28% of the cyberattacks were targeting public administration. The same study found that data breach and hacking still was the most reported attack. In 69% of the incidents, strategic management was involved, and 56% reported that they in the aftermath of the attack had made changes in their policies. However, only 11% reported the attack to the police, despite the police's recommendations to do so [7]. This might be a consequence of the fact that only 44% of the population do not think the police can help them with investigation of such cases [8]. As a number of publicly known cases also are dismissed by the police (e.g. the attack against Helse Sør-Øst [9]), and 40 out of 44 such cases in Oslo in 2016 were dismissed by the Oslo police district [10].

We suggest that since the majority of cases are dismissed by the police there is a need to support competence development for cybersecurity incident management at the municipal level. Additionally, we suggest that the Norwegian laws and regulations on crisis management move the responsibilities away from crime reports and crime handling by the police over to the different organizations (like the municipalities).

> "The Norwegian law concerning the municipality's emergency duty, civilian preparedness and the Civil defense organization outlines the municipality's responsibility to analyze and make emergency preparation based on risk and resilience in their geographical designated area" [11]. "The municipalities would set up prepared societal emergency work that will 1) protect the population and contribute to uphold critical infrastructure, 2) give an overview of knowledge and awareness of societal critical challenges and what effect these challenges would have on the society and communities, 3) reduce risk and vulnerability through preventive work, and 4) ensure good emergency preparedness and crisis contingency" [11].

Moreover, due to the responsibilities outlined above, the municipalities in Norway are mostly self-assurance organizations, that is, they must pay for damages from their own budget. This may also lead to more focus on prevention than if they held normal type of insurance.

For the municipalities to respond to cyber-crime, the understanding of the cyber-attack business is essential. Huang et. al. (2018) outline the cyber-crime business in a value-chain perspective. The primary activities in the mentioned value-chain perspective are 1) vulnerability discovery, 2) exploitation development, 3) exploitation delivery and 4) action, which can be directly translated to the adversary of an incident response process. In this paper we approach the challenges of the cyber-attack business – with an adversary incident response framework combined with a socio-technical analysis framework which take the municipality societal responsibility and challenges into consideration.

## 3. Relevant literature

Crime science has traditionally studied incidents, not persons [13], and has a number of conceptual frameworks like 1) the rational choice perspective, 2) the routine activity approach and 3) the crime patterns theory, which all tries to explain incidents to prevent or control crime and disorder [13]. However, the studies are usually based on target studies, geographical surveys and case studies based on happened incidents, and does not analyze initiated prevention steps with no incident outcome. Additionally, crime science does not often take into consideration how response to crime may minimize the crime outcome. In this paper we therefore suggest to use incident framework like [14] to get a broader approach to crime prevention and crime response and recovery.

Numerous opportunity reducing techniques are suggested in crime science [13]. These opportunities are however systematized to increase effort and risk, to reduce rewards and provocation and to remove excuses [13]. As cyber criminals in addition to targeting private persons also target organizations, several societal, organizational, cultural, methodological, and technical analyses are not taken into consideration in the traditional cyber-crime prevention framework mentioned. In this paper we therefore suggest a socio-technical analysis framework in combination with the an incident framework.

The “objective of socio-technical design has always been the joint optimization of the social and technical system” [15], and the early motivation for developing socio-technical theories was initiated by the desire to improve industry-workers stationary and repetitive job situation [15]. In this paper our motivation is to close the socio-technical gap in crisis management handling, and to create a framework to support those in the situation of making crisis decisions.

We do not try to create a new socio-technical model, instead we will combine a traditional dynamic socio-technical approach, proposed by Leavitt in 1965 and modified by Kowalski in 1994 [6], [16] with the static Security-by-Consensus model as presented by Kowalski [6] to analyze the case mentioned. Leavitt’s model of organizational change comprises four concepts tightly connected to each other – people, task, structure, and technology. The modified Kowalski model also consists of four concepts, culture and structure on the socio site and methods and machines on the technical site. Kowalski’s model is presented in figure 1:

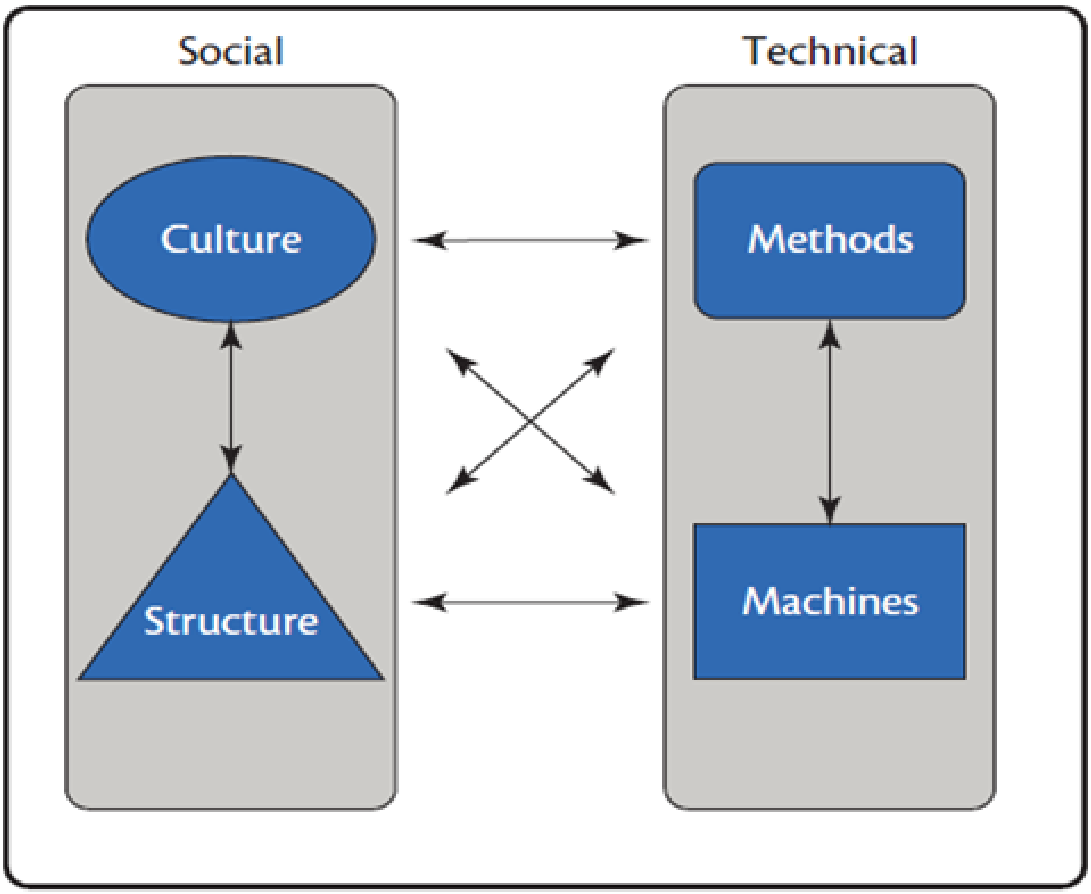


**Fig. 1.** Socio-technical approach [6]

In an organization, there will be several stacks (like in the SBC-model mentioned) to consider when to perform socio-technical analysis. Each of the stacks has it own socio-technical performance [6], and to analyze a case like the one we present in this paper, all stacks would need to be analyzed to find these socio-technical performances. Such a framework was suggested by Kowalski [6], and is presented in figure 2.

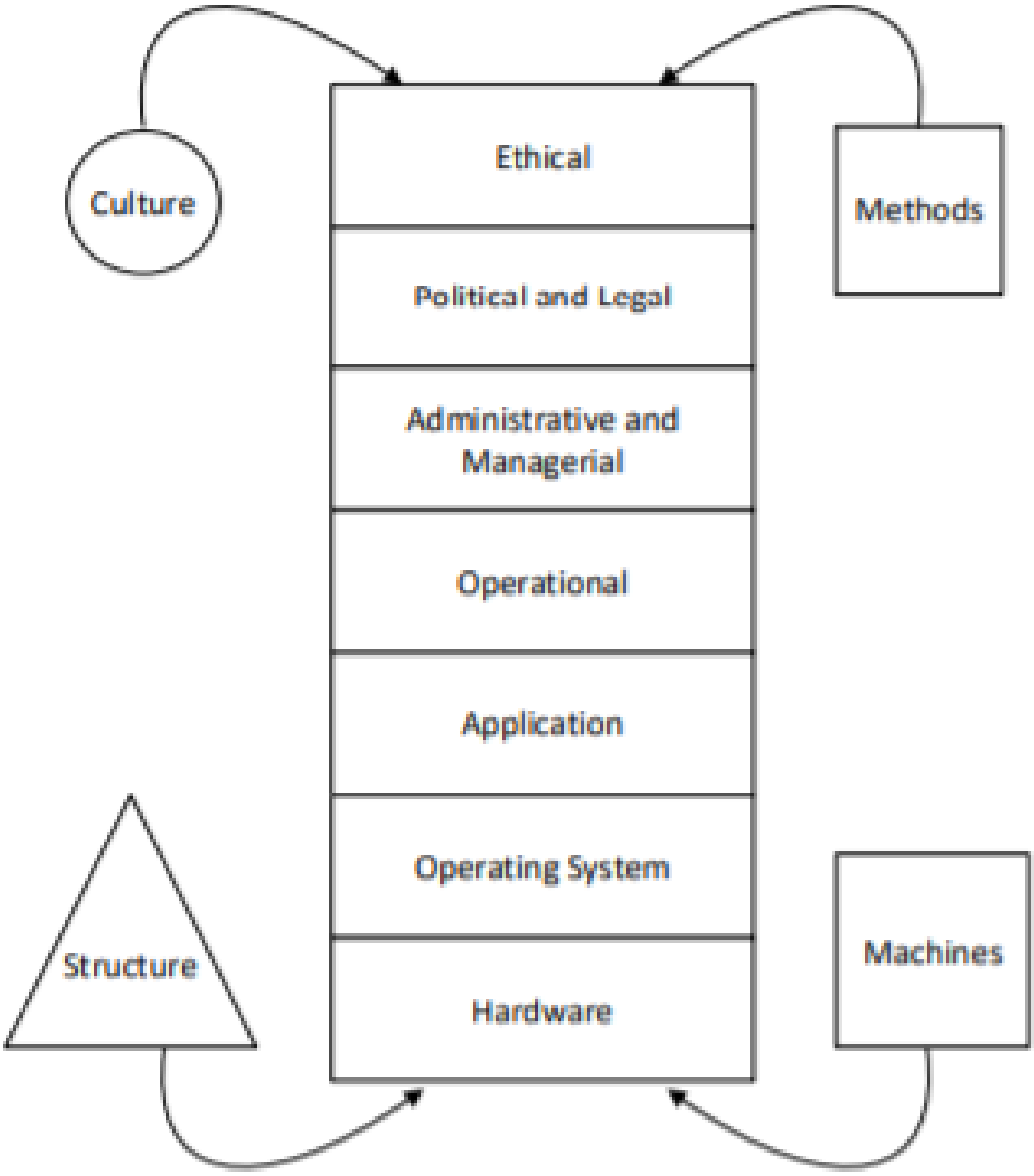


**Fig. 2.** The Security by Consensus model in a socio-technical context [6]

When analyzing the organizations prevention performances in such socio-technical context, we suggest one would need to combine it with the crisis management responsibilities as mentioned in the background. In 1994, Kowalski suggested that this model should be implemented to support a day-to-day emergency response [6]. Kowalski's original suggestion is presented in figure 3.

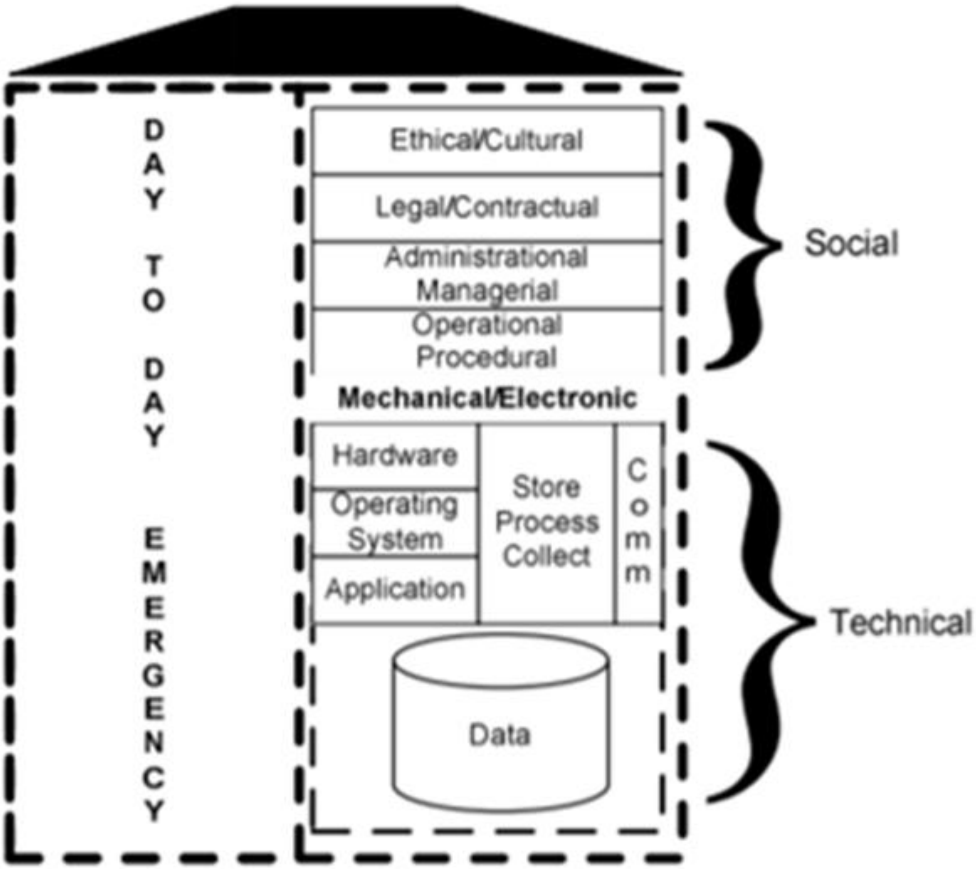


**Fig. 3.** SBC Model suggested to support a day-to-day emergency response [6]

The information shared, escalated, and de-escalated (and adapted) on each layer in this model (figure 3) is in need of being accurate and efficient. Turoff et. al. [17] present a dynamic emergency response management information system to improve information flow. The suggestion is more of a top-down approach, thereby socio-technical semiotics like presented by Piccolo et. al [18] is better for considering information flow in necessary crisis communication. However, Piccolo et. al does not consider the practicalities of what should be considered on which layer in the organizational semiotics. Thereby we suggest using established incident response systems to support information sharing and to have the same information sharing approach on all layers involved in an incident.

In ongoing teaching and research on management at the Norwegian Cyber Range (NCR)/Norwegian University of Science And Technology (NTNU) [19], [20], we are targeting management responsibilities and incident response using the NIST-framework. The American National Institute of Standards and Technology (NIST) provides organizations with a structure for “assessing and improving their ability to prevent, detect and respond to cyber incidents” [14]. The framework consists of 5 stages, 1) Identify, 2) Protect, 3) Detect, 4) Respond and 5) Recover. The framework is presented in figure 4.

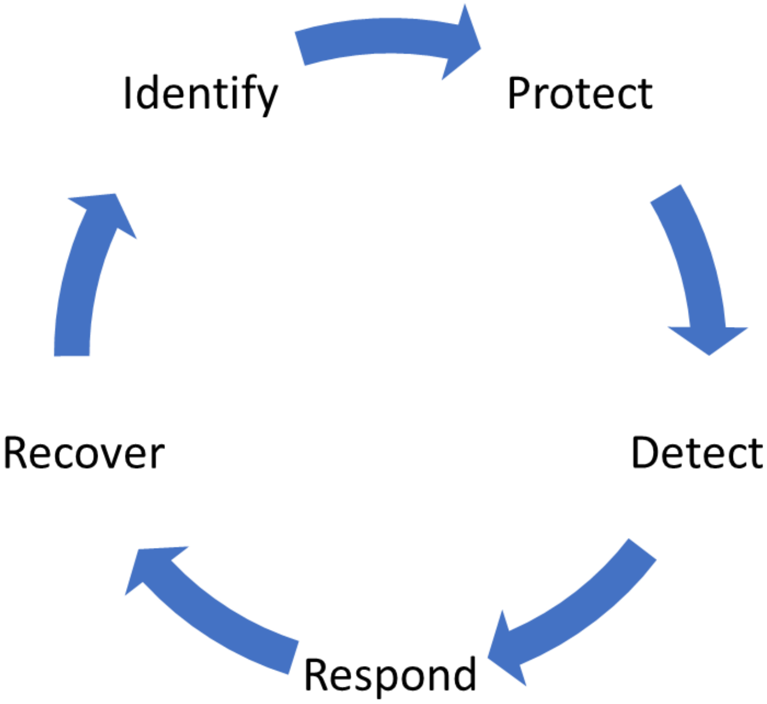


**Fig. 4.** NIST Cyber security framework [14]

By the nature of the case, we present in this paper, we will focus on the identify, the protect and the detect phases of the framework, but also outline the consequences in the respond and the recovery phases.

## 4. Research approach

In this paper, we approach the crime prevention challenge by using the design science research in information systems (DSRIS) [21]. Design science research (DSR) is a methodology which can be conducted when "creating innovations and ideas that define suggestions through the development process of artifacts which can be effectively and efficiently accomplished" [21].

How to work on DSR is presented in a thesis written by G. R. Karokola [22]. He visualized this approach as outlined in figure 5. However, logical formalism in figure 5 is in our research modified with an inductive approach instead of abductive approach used by Karokola.

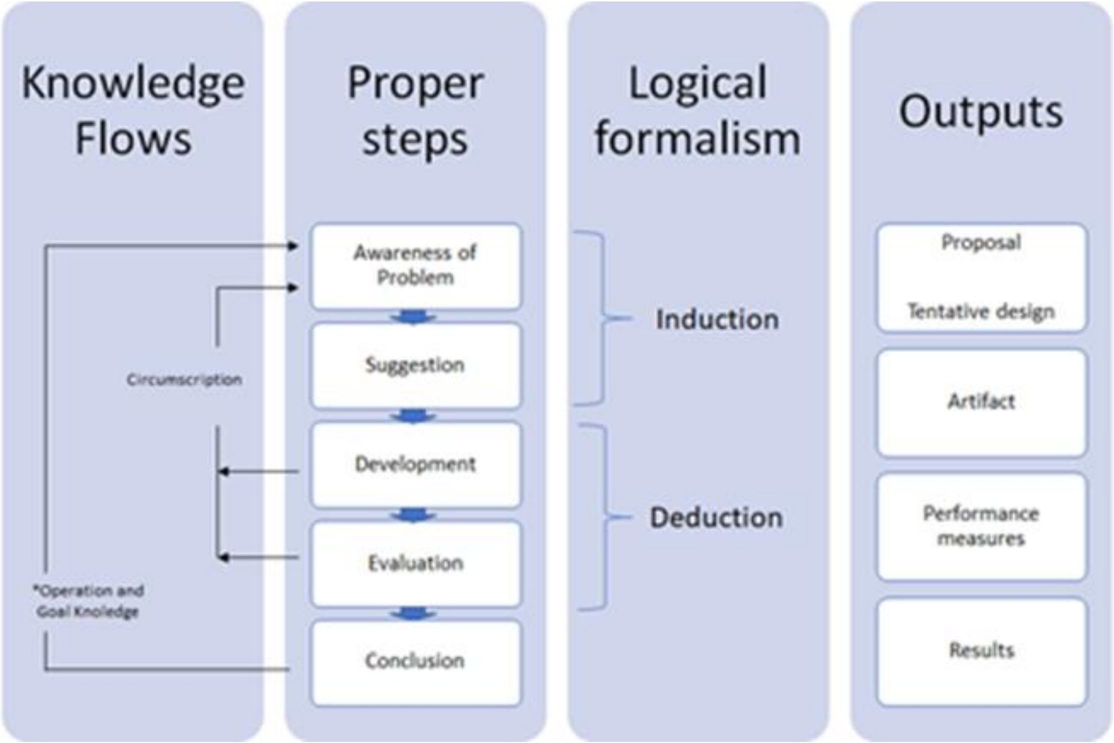


**Fig. 5.** Design research methodology – modified from abduction to induction [22]

As visualized, we have approached the study by what can be referred to as an inductivist approach (instead of abductive or deductive). The inductivist approach starts by first observing a phenomenon and then generalizing about the phenomenon which leads to theories that can be falsified or validated [6]. We have presented the problem by a prevention decision case in Gjøvik Municipality and performed a socio-technical analyze using the SBC model in a socio-technical context (see figure 2) combined with the NIST crisis management framework (see figure 4) to present information from interviews with the decision-makers in Gjøvik municipality. Our suggested combination framework is presented in figure 6.

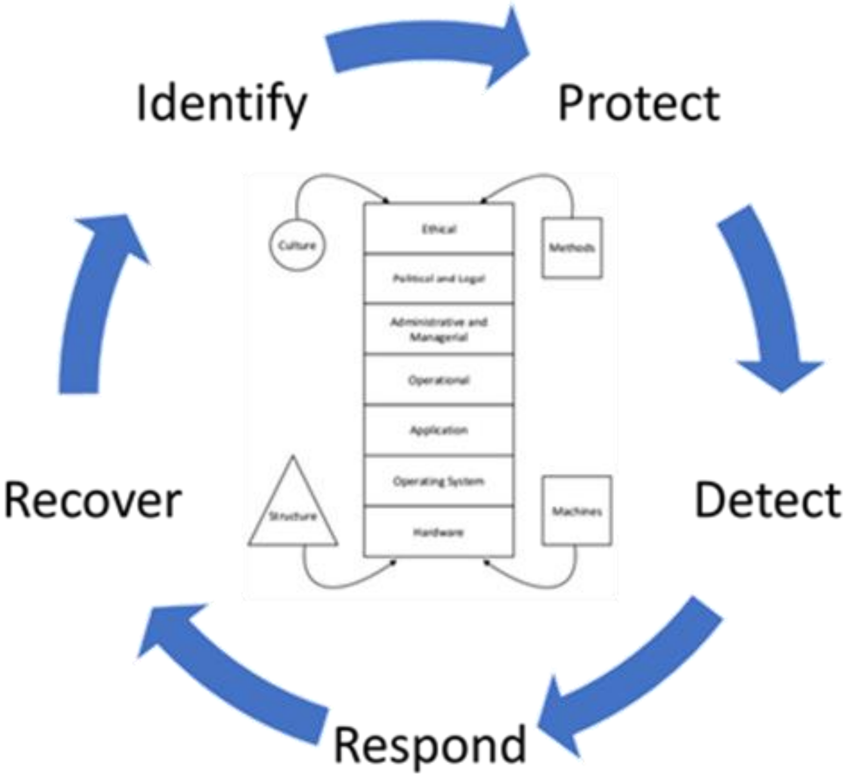


**Fig. 6.** A socio-technical and risk-management root cause analysis framework

We conducted interviews with two of the four people involved in the decision, and the interviews were conducted as open interviews [23] where the participants freely could tell their perception of the situation and decision. We followed up with a few control-questions about crisis management and socio-technical thinking based on what was already told by the participants. Due to integrity issues, no quotes are presented in this paper. The participants were given the possibility of proof-reading the final written case-text to ensure that the content was correct before we started up with our analysis.

As our proposed artifact is a combined risk-management and socio-technical framework to prepare for cyber-attacks, we suggest that this model can be generalized after validation in case-studies in other organizations.

## 5. The case of Gjøvik Municipality prevention decision – a socio-technical and risk-management root cause analysis

After municipalities on the Hedmark-site of the Inland county in Norway was attacked by virus via phishing attack [4], the BAG-group (decision and recommendation group) in the IT-department in Gjøvik Municipality decided to escalate their prevention suggestion to strategic level in the Municipality. The suggestion contained several measures, like 1) to block macros from word, excel and ppt documents, 2) to block internals from sending and receiving emails with word, excel and ppt-files, and 3) to close down all incoming and outgoing emails all together. The suggestion was successfully accepted with immediate effect. The internal blockage lasted for a few days, and the external blockage lasted for proximately 14 days. At this stage no cyber-attacks against the Gjøvik municipality had been discovered.

During the blockade, the municipality implemented sandboxing of word, excel and ppt-files attached to emails, where all the files would be opened and controlled in the sandbox before the email could be passed on.

The IT-department in the municipality participate in a diversity of fora for information security (like Athea[2] and NorCERT[3]) together with amongst others the mentioned municipalities affected by the virus. It was in these fora they were informed about the content of the attacks, and it was the format of the phishing-attack with macros for reuse of internal emails which were analyzed to be the alarming threat. Knowing the internal status on clicking on links the group who decided the measures where confident in their decision (the municipality had already had two phishing attack tests amongst their employees, executed by students from NTNU, where both tests ended up with proximately 10% of the employees clicked on the links in the emails).

The crisis management was not involved in this situation (as the crisis had not yet happened), but the escalation process routine in the municipality was followed: When the IT-department would have to affect the daily routines in the municipality organization, strategic manager in line shall be involved.

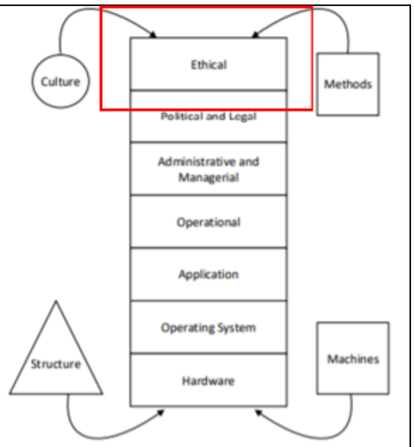
## 5.1. A socio-technical and risk-management root cause analysis framework.

Even though the mitigation measures in Gjøvik municipality first and foremost were executed in the identify and protect phase of a possible data breach, we argue that the consequences in the detect, the respond (e.g. the implementation of the sandbox) and the recover phases were considered. Especially due to the increased number of cyber-attacks during the Corona-crisis. The Corona-crisis itself requires vast crisis management work, and another crisis on top of the ongoing crisis could have affected the organizations capabilities to handle (respond to) the situation, and the recovery could have been very difficult.

In this section we present steps of the combined NIST framework and socio-technical framework presented in figure 6. We have chosen to pesent the Identify-phase of the NIST-framework applied to the socio-technical analyses of the Gjøvik decision in a detailed context (section 5.2) and outline overall importance of similar analyzes for the other NIST-phases in the next sections (section 5.3 – section 5.6).

## 5.2. The socio-technical root-cause analysis to IDENTIFY the situation

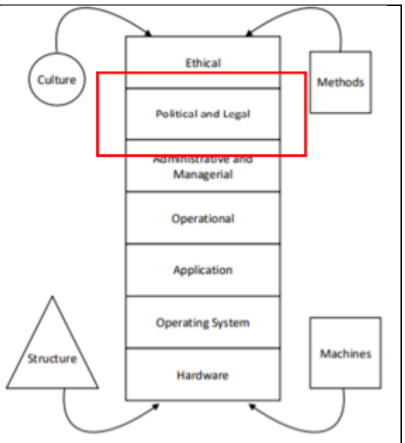
In this section we present the socio-technical analysis (culture, structure, methods, and machines) of each stack in the SBC-framework framework suggested, on how the municipality identified and could identify vulnerabilities in the stacks.

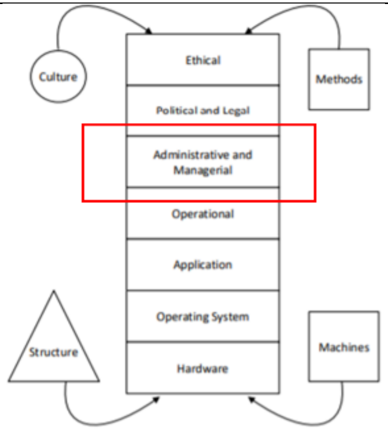
<table>
<tr>
<td>There is a strong culture for considering ethical questions in Gjøvik Municipality. In this case, one could have identified that the cost of closing the email-accounts would be too large to do this job, but the internal culture accepted the beneficial arguments to be more important.<br>It could have been identified ethical concerns on the methodology to execute the cut-off, but there were no hidden agendas, and information about the decision was outlined in public (Facebook), which the local newspaper also put forward.<br>The possible draw-back identified on the ethics of the situation was for how long the systems would-be put-on hold. There was no clear timeline on the implementation-phase of the sandboxing in the machines, and thereby important emails to the municipality could have been blocked.<br>One could also question whether the crisis management group should have been involved all together. The decided structure</td>
<td>
</td>
</tr>
</table>

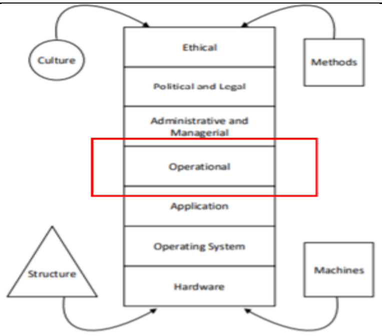
[2] https://www.atea.no/

[3] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

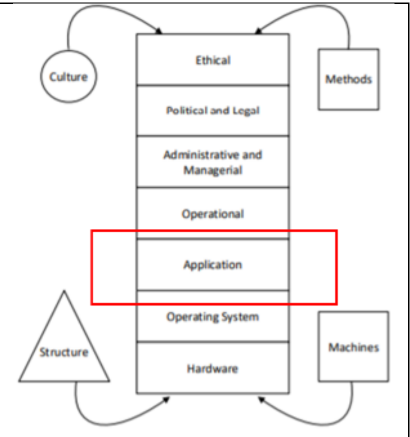
| | |
|---|---|
| for decisions were followed, but due to the high crisis-risk of the decision, one ethical consideration could have been to involve the crisis management. | |

| | |
|---|---|
| The political direction in the Norwegian municipalities is put forward every fourth year, and one political priority in Gjøvik municipality is to be a university city, and as the Information security environment in the University is one of the prioritized areas in the University, so it has also become in the municipality. This is proven by the municipality welcoming students to do tests and write studies in the area. The political culture may therefore influence the culture within the organization, and thereby it might have been easier to take the decision.<br>The legal aspect due to the crisis management responsibility suggests that the decision is owned by the municipality and cannot be argued unless the decision is violating any other laws. One may even argue that not taking the decision could have violated the responsibility [24].<br>To implement the sandboxing system would thereby be according to the law mentioned. |   Culture<br>Ethical<br>Political and Legal<br>Administrative and Managerial<br>Operational<br>Application<br>Operating System<br>Hardware<br>Methods<br>Structure<br>Machines |

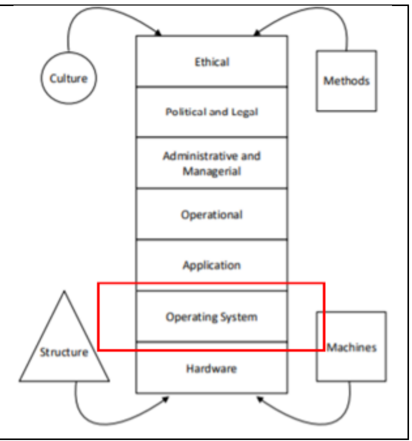
| | |
|---|---|
| The structure of the escalation routine starts normally at helpdesk if abnormalities occur. The on-duty system responsible would, if necessary, gather the BAG-group, which would consider involving the strategic manager. The strategic manager would eventually consider gathering the crisis management group, and necessary decisions would be taken at the proper stage for the case at hand.<br>One has therefore identified that the culture for escalation is a bottom-up approach, where the operational organization outline recommendations to (in this case) prevent the situation. |   Culture<br>Ethical<br>Political and Legal<br>Administrative and Managerial<br>Operational<br>Application<br>Operating System<br>Hardware<br>Methods<br>Structure<br>Machines |

| | |
|---|---|
| With the bottom-up culture described, a great deal of trust is also put on the operational organization to identify the right decision and execute the decision.<br>Their suggested method was to block emails and macros from files, and when doing so, implement sandboxing before opening the systems again. The implementation was finished within two weeks. |   Culture<br>Ethical<br>Political and Legal<br>Administrative and Managerial<br>Operational<br>Application<br>Operating System<br>Hardware<br>Methods<br>Structure<br>Machines |

As much as the municipality is dependent on using their email-system, word, excel and ppt, they still identified that they have an internal culture in the organization to set aside the applications for this period. This is proven right from the fact that there have not been any public critical comments on the decision. If there has been any internal critique, they also had identified the decision to live with such critique to be right. To make the applications unavailable to the organization may have postponed important necessary written work, but they identified the internal and external structure and culture of information would prevent such critique.

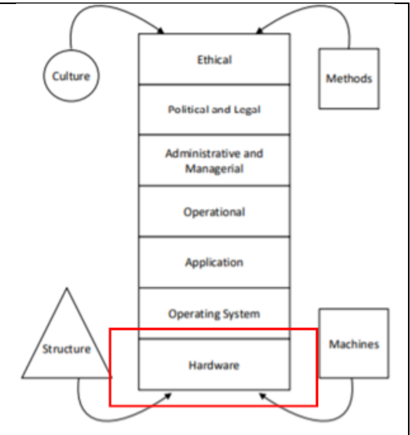


The operative systems in this situation are well known systems, and the decision they identified to close all macros on these systems would make the applications unavailable for a short amount of time (prox 3 days for the internal users). The same identified issues on culture, methods and structure as described for applications was analyzed, and in this case had the same outcome.



To protect the hardware from the virus, the identified implementation of sandboxing was essential. The method chosen was suggested from the information security fora's the municipality is a part of. One may therefore say that there is a good culture for collecting knowledge from external expert groups.

As previously mentioned, the municipality is self-assured, and this could also be an important impact identified for making the decisions they did. A costly investment in hardware would not have been desired in an already pressured financial situation (because of the Corona-situation).



In the following sections we outline how socio-technical findings would be important in the other stages of the NIST-framework, but we do not go through all stacks in the socio-technical SBC framework.

## 5.3. Update on risk-and resilience analysis to PROTECT from data breaches and hacking

A part of the outlined regulations [25] and municipality guidance's [26], is to regularly update risk- and resilience analysis as a baseline for the emergency (contingency)-plans in the organizations. The organizational structure in the municipalities for update is all set, but the methodology is often to do an update every other year, and thereby cases like the one described in this paper might be forgotten. The case would be a sub-issue but would have been a good example to use for deciding what culture, structure, methods, and machines would be necessary to protect the organizations from such attacks, using the SBC-model to explain the risks in the different stacks.

## 5.4. Emergency and contingency plans to DETECT similar data breaches and hacking

In the municipality guidance [27], it is suggested to have emergency and contingency plans on both strategic and sectoral levels in the organization. For the municipality IT-department, it would be wise to do a socio-technical analysis as described on a diversity of Information security issues (like those described in [1]), and make relevant emergency and contingency plans relevant for all issues.

## 5.5. RESPOND to data breaches and hacking

The respond to and escalation in an attack as described would vary by the severity of the attack, but like in the Hedmark-municipalities situation [4], managing the Corona-situation was already heavily burdening the municipalities crisis management team, and they were concerned that the impact of simultaneous crisis was emerging, and also ethical considerations were necessary to consider. Even political priorities were under discussion in the situation mentioned. Information from the Information security fora could also have been relevant to prepare for handling such situations, and in this case, it could be an important foundation for the decision Gjøvik made.

## 5.6. Update on Information security policy in RECOVERY phase data breaches and hacking

In a situation with several ongoing crises at the same time, the recovery phase can take more time than usual. To use time on recovery from such a situation and do the proper socio-technical analyzes as suggested in this paper, could take too much time from other ongoing crises, and could be set aside (and forgotten) before the next crisis occurs. It would therefore be important to establish the framework as part of the deviation report, to be able to collect the analyzes for later recovery [6, chap. 13].

# 6. Conclusion and future research

In this paper we have discussed the Gjøvik Municipality decision case in a combined socio-technical and risk-management root cause analysis framework. We suggest that the combination of the two frameworks (the SBC-model/Kowalski model and the NIST-framework) outline first and foremost a good analysis framework to prevent data breaches and hacking from happening, but also to be able to prepare for the respond and the recovery phases. Our plan is to invite other municipalities in testing the framework, to see what impact such framework could have on incident management in organizations affected by such attacks.

We have only tested the SBC-model combined with the Kowalski-model, as part of the socio-technical analyses. One may suggest that other socio-technical models could be more suitable in combination with the NIST-framework, and such could be tested to validate and possibly figure out the reliability of our suggested framework. Other incident response frameworks than the NIST-framework might also be relevant to test for combination with socio-technical models, and this needs to be further tested in other studies. First however, we need to test if our suggested model in this paper can be applicable in other case-studies.

Organizational semiotics are argued out of this paper but are suggested to have a great impact on emergency responses. Mentioned dynamic emergency response management information system (DERMIS) like presented by [17], and a socio-technical semiotic approach to build community resilience, like presented by [18] will be an important part of the future test and research of combining socio-technical and incident response tools.

## 7. Acknowledgements

We would like to give our special thanks to Gjøvik municipality, which gave us the possibility to do interviews with involved parties in the decision. Our plan was to interview relevant parties on both strategic, tactical, and operational levels in the organization, but the tactical head of the IT-department was disabled from participating. We would, however, give our special thanks to the participant from the strategic management group and the participant from the operational IT-department and member of the BAG-group, for being able to participate in interviews in a hectically period of the Corona-crisis situation.

## 8. References

[1] The Norwegian Business and Industry Security Council, “The dark numbers survey 2020,” 2020.

[2] T. Bie, “Stortinget hacket: – Krise,” *ITAVISEN*, 2020.

[3] J. Gilbrandt and M. Rønning, “Omfattende IT-angrep mot Stortinget,” *dagbladet.no*, 2020.

[4] A. Krantz, M. F. Børresen, T. I. Hagen, and A.-K. Mo, “Dataangrepet: Kan skade korona-beredskapen,” *nrk.no*, 02-Sep-2020.

[5] M. B. Staveli, “Gjøvik stopper e-poster med vedlegg etter hackingskandalen,” *oa.no*, 2020.

[6] S. Kowalski, “IT Insecurity: A Multi-disiplinary Inquiry,” Stockholm University, 1994.

[7] Politiet, “Datakriminalitet,” *www.politiet.no*, 2020. [Online]. Available: https://www.politiet.no/rad/datakriminalitet/. [Accessed: 14-Nov-2020].

[8] NorSIS, “Nordmenn og digital sikkerhetskultur 2019,” 2019.

[9] Digi.no, “Henlegger saken om dataangrepet mot Helse sør-øst,” *digi.no*, 05-Dec-2018.

[10] R. A. Njie, “Kripos advarer: – Stor økning i datakriminalitet,” *nrk.no*, 03-Apr-2017.

[11] G. Østby and B. Katt, “Cyber Crisis Management Roles – A Municipality Responsibility Case Study,” in *Science and Technology in Disaster Risk Reduction in Asia*, 2019, pp. 168–181.

[12] K. Huang, M. Siegel, and S. Madnick, “Systematically Understanding the Cyber Attack Business: A survey,” *ACM Comput. Surv.*, vol. 51, no. 4, p. 36, 2018.

[13] P. Hartel, M. Junger, and R. Wieringa, “Cyber-crime Science = Crime Science + Information Security,” *Inf. Secur.*, pp. 1–55, 2011.

[14] K. Scarfone, T. Grance, and K. Masone, “Computer Security Incident Handling Guide,” 2008.

[15] E. Mumford, “The story of socio-technical design: Reflections on its successes, failures and potential,” *Information Systems Journal*. 2006.

[16] H. Leavitt, “Applying Organizational Change in Industry: Structural, Technological, and Humanistic Approaches.,” in *Handbook of organizations*, J. G. March, Ed. 1965, pp. 1144–1170.

[17] M. Turoff, M. Chumer, B. Van de Walle, and X. Yao, “The design of a Dynamic Emergency Response Management Information System,” *J. Inf. Technol. THEORY Appl.*, vol. 1, no. 1, pp. 253–292, 2012.

[18] L. Piccolo, K. Meesters, and S. Roberts, “Building a Socio-technical Perspective of Community Resilience with a Semiotic Approach,” *Proc. 18th Int. Conf. Informatics Semiot. Organ.*, vol. 527, 2018.

[19] NTNU, “The Norwegian Cyber Range,” 2019. [Online]. Available: https://www.ntnu.no/ncr.

[20] NTNU, “IMT4115 - Introduction to Information Security Management,” 2021. [Online].

Available: https://www.ntnu.edu/studies/courses/IMT4115/2021/1#tab=omEmnet.

[21] W. Kuechler and V. Vaishnavi, “A Framework for Theory Development in Design Science Research: Multiple Perspectives,” 2012.

[22] G. R. Karokola, “A framework for Securing a-Government Services, The case of Tanzania,” Stockholm University, 2012.

[23] D. L. Driscoll, “Introduction to Primary Research: Observations, Surveys, and Interviews,” in *Writing Spaces: Readings on Writing*, 2011, pp. 152–174.

[24] Justis- og beredskapsdepartementet, “Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).” Norwegian Government, 2010.

[25] Norwegian government, *FOR-2011-08-22-894*. Norwegian Government, 2011.

[26] DSB, *Guidance to holistic risk and vulnerability assessment in the municipality*. DSB, 2019.

[27] DSB, *Municipality guidance, emergency duty*. 2017.