How do Norwegian enterprises create awareness of cybersecurity?

Ivar Mykkeltvedt[1] & Andreas L Opdahl

Intelligent Information Systems (I2S),
Dept. Information Science and Media Studies,
University of Bergen, Norway

Abstract. The increasing digitisation of society means that Norwegian enterprises experience daily cyberattacks. Most successful attacks today are due to human error, and cybersecurity awareness has never been more important. We therefore ask: *How do Norwegian enterprises create awareness of cybersecurity?* We have interviewed managers from 16 Norwegian enterprises of different sizes and from different sectors and compared them based on size, public versus private sector, and tolerance for cybersecurity breaches. The results show that almost all the enterprises offer some form of course or training, but completion is not always compulsory. Paradoxically, and somewhat worryingly, the informants who reported least security knowledge were the ones who expressed the greatest satisfaction with their security work and were least concerned about attacks. Many small and private enterprises had chosen to outsource cybersecurity, but did not always have detailed knowledge of the cyberdefences that were set up for them. The study indicates that Norwegian enterprises are implementing measures to create awareness around cybersecurity, but that many areas can still be improved, with different challenges facing different enterprise types.

Keywords. Cybersecurity, IT security, Security awareness, Norwegian enterprises, Qualitative study

1 Introduction

Norwegian enterprises are increasingly digitalised across sectors and industries. It makes everyday life more efficient for enterprises, but also opens the doors to new digital dangers. In 2019, the Norwegian government set a strategic goal that Norwegian enterprises should digitise in a safe and trust-inspiring way and be able to protect themselves against cyberincidents (Departementene, 2019), but the National Security Authorities report an increase in the number of attempts to compromise Norwegian businesses: cyberattacks have become commonplace (NSM, 2022). “A wide range of

[1] Contact author: Ivar.Mykkeltvedt@hotmail.com

threat actors exploit various human, technological and organizational vulnerabilities with the aim of affecting the confidentiality, integrity and availability of digital assets" (translated from NSM, 2023).

A successful cyberattack could potentially hit a commercial enterprise so hard financially and operationally that, in the worst case, it could go out of business. In this scenario, an enterprise's employees constitute a large attack surface. Security awareness among employees is therefore a cornerstone for security in any organization that wants to avoid harmful attacks (Dahbur et al., 2017). As much as 85% of security breaches are caused by social manipulation or human error, suggesting that organizations cannot afford to neglect the human side of cybersecurity (KnowBe4, 2022). However, although almost everyone has heard of cybersecurity, neither people's behaviour nor their attitudes reflect a high level of awareness (De Bruijn & Janssen, 2017). Raising cybersecurity awareness has therefore become extremely important for contemporary enterprises. An informant in our study gives an example of this: *"Three employees worked for two and a half hours to manage to open an attachment that everyone should have understood should not be opened. When the first person didn't make it, she brought in another, but they couldn't make it either. They then involved a third person, and finally they encrypted everything in the enterprise."*

This paper therefore presents the results from a qualitative study of a Norwegian enterprises and what they do – or do not do – to create awareness around cybersecurity. Section 2 presents relevant research literature, whereas Section 3 describes our research method. Section 4 then presents the main results, which we discuss in Section 5. Finally, Section 6 concludes the paper and offers paths for further work.

2 Related work

Bendovschi (2015) analyses cyberattacks reported worldwide over three years prior to 2015 to determine patterns and trends in cybercrime and presents countermeasures that enterprises can implement.

Hooper & McKissack (2016) discuss the CISO (Chief Information Security Officer) role, providing information about what is required in this role and how enterprises should organise themselves in an optimal way. They have used data from the United States, Canada and New Zealand.

Dahbur et al. (2017) survey 504 employees in Jordanian enterprises located in Amman in order to assess their level of security awareness and the availability and level of security training and security policies. Their survey contains 31 questions that address physical security, security training, security guidelines, software security, social manipulation, security awareness, and phishing.

Kamiya et al. (2018) investigate which types of enterprises that are targetted by cyberattacks and how they are affected. Cyberattacks cause enterprises to reassess the risks they are exposed to and their consequences, changing the enterprises' choices of measures and countermeasures.

Gordon et al. (2018) examine private-sector enterprises' investments in cybersecurity activities, assessing the extent to which enterprises see investments in cybersecurity as a source of a competitive advantage.

Huang & Pearlson (2019) propose a model that describes organizational cybersecurity culture, focusing on the factors that are important in building it and how it can be measured. Their study aims to helping managers understand and apply recommendations to create a more mature cybersecurity culture in their organization.

Ergen et al. (2021) explore and discuss the role of employees in cybersecurity based on in-depth interviews with eight cybersecurity experts through semi-structured open interviews. They discuss the employees' cybersecurity behaviour, obstacles and how to promote secure behaviour in the cybersphere.

Chowdhury et al. (2022) compare cybersecurity awareness and training practices in selected Norwegian enterprises. They conduct interviews and distribute questionnaires to cybersecurity personnel in enterprises and areas that manage critical infrastructure.

PwC (2023) presents a quantitative Cybercrime Survey with 106 respondents, most of them in management positions, recruited through Finans Norge (Finance Norway), aiming to shed light on how cyberthreats affect Norwegian businesses.

Erdogan et al. (2023) survey 141 small and medium-sized English enterprises quantitatively in order to investigate their level of cybersecurity awareness and which practices they use to mitigate cyberrisks. The study only includes enterprises with 250 or fewer employees. Their survey contains 27 questions, of which 13 are specifically related to cybersecurity awareness and cybersecurity practices.

3 Choice of research method

To answer our research question, *How do Norwegian enterprises create awareness of cybersecurity?*, we chose to perform qualitative interviews (Choy, 2014). Such interviews invite detailed descriptions of the thinking behind the enterprises' various measures. They answer *how and why*, rather than *how many or how much* (Tenny et al., 2017), facilitating more detailed discussions and fine-grained comparisons based on factors such as company size, public versus private enterprises, and tolerance for cybersecurity breaches.

Table 1: Our interview guide.

Main question	Follow-up questions
Q1: Does your enterprise offer courses or training materials to employees to raise cybersecurity awareness?	If yes: What topics does the course cover? Do all employees have to go through this? If not, who must take it?
Q2: Does your enterprise have positions dedicated to cybersecurity?	If yes: How long has the position(s) been in existence? Are they, for example, represented in the management group or other management forums?
Q3: Do you have regular meetings regarding cybersecurity?	If yes: How often do you have these meetings? Who is present at these meetings? Does senior management occasionally participate?
Q4: How would you characterise your own knowledge of cybersecurity?	If yes: Do you have training in cybersecurity? How long, if any, have you worked mainly in cybersecurity?
Q5: To what extent do you fear a cyberattack against your enterprise?	What types of attacks are you concerned about?
Q6: How would you characterise your enterprise when it comes to cybersecurity awareness?	Do you use any kind of maturity model?
Q7: How long do you think their critical applications and systems can be down before it has significant consequences for the enterprise?	Which apps/systems are most critical? Are they particularly protected? What emergency solutions do you have in place?
Q8: Does your enterprise use specific processes or tools to identify cybersecurity vulnerabilities?	
Q9: Have there been any previous cyberattacks on your enterprise that you can mention?	
Q10: What was the impact of the eventual attack(s)?	
Q11: Can the enterprise's employees surf the web freely or are the pages they can access restricted?	
Q12: Do people generally have limited access to the enterprise's office building?	

We interviewed managers in 16 Norwegian enterprises of different sizes and from different sectors about how they viewed their own enterprises regarding cybersecurity awareness. We attempted to recruit informants from both public and private enterprises and from different public domains and business areas. We developed an interview guide with 12 main questions, some of them supplemented by follow-up questions, as shown in Table 1. To make our results comparable to earlier studies, we chose questions inspired by the literature. Questions Q1-Q10 were adapted from Erdogan et al.'s (2023) English survey, whereas questions Q11 and Q12 were based on

Dahbur et al.'s (2017) Jordanian study. The length of the interviews ranged from 15 to 45 minutes.

The interviews were recorded, transcribed and analysed with *NVivo* using a combination of latent and semantic thematic analysis (Braun & Clarke, 2006). Frequently recurring themes were identified in the answers to both main and follow-up questions. The semantic analysis was used to identify themes based on the surface meaning of the data, whereas the latent thematic analysis identified underlying ideas, assumptions, conceptualizations and ideologies (Braun & Clarke, 2006). The central interview themes were then summarised, first for all the enterprises together and, then, comparing the central themes depending on company size, on whether the enterprises were public or private, and on their tolerance for security breaches.

Dinkova et al. (2023) found that the level of cybersecurity maturity tends to increase with company size (Dinkova et al., 2023). Hence, size can influence the security-related awareness and actions of an enterprise. We therefore divided the businesses into the following categories: under 100 employees (*small*); from 100 to 1000 employees (*medium-sized*); and more than 1,000 employees (*large*).

Public organisations tend to have more stable budgets dedicated to cybersecurity, and may be subject to stricter cybersecurity regulations, based on the fact that they often handle sensitive data. Private enterprises may vary more in their available security budgets based on sector and size and depending on commitment from top management. We therefore also divided the enterprises into *public* and private *ones*.

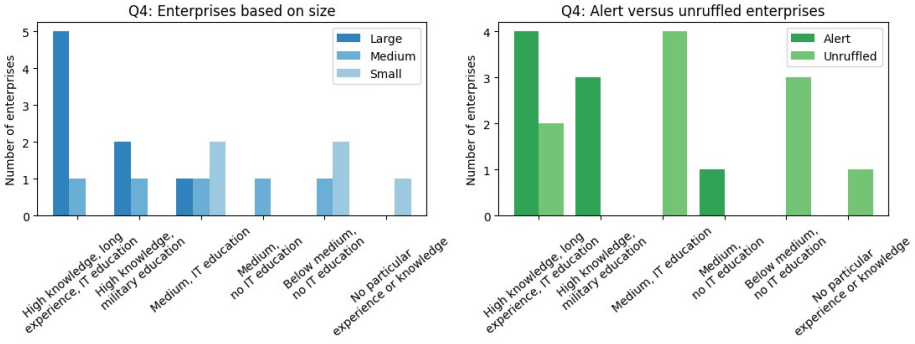
4 Results

This section presents the main results, organised thematically rather than by question order in the interview guide. Detailed results are available in (Mykkeltvedt, 2024).

Enterprises and informants: There were six large, five medium, and five small enterprises in our study. Five of them were public and the remaining 11 private.

In addition, our analysis revealed that a third important factor for the businesses' work with security awareness was tolerance for information security breaches. Enterprises with low tolerance might have both more numerous and more advanced measures in place, with more regular internal communication and more resources spent on employee awareness and cybersecurity in general. The study included six *alert* enterprises that expressed zero-tolerance for security breaches and 10 *unruffled* enterprises whose respondents claimed would not immediately experience major consequences of a successful cyberattack.

The informants played the following roles in their respective enterprises: Chief Information Security Officer (CISO) or Head of Information Security (9); Head of IT or other functional leadership role (5); top-level manager in the enterprise (that did not have an IT department) (2).



(a) (b)

Figure 1. Cybersecurity competence depending on size and tolerance for breaches. (Here and later, the themes are not mutually exclusive.)

Level of competence (Q4): Many informants responded that they had good knowledge, extensive experience and education within IT, in several cases from the armed forces. Larger enterprises and public-sector organisations reported higher competence than smaller and private ones (Figure 1). Note that, in these and later figures, the themes resulting from the qualitative analysis are in general *not exclusive*.

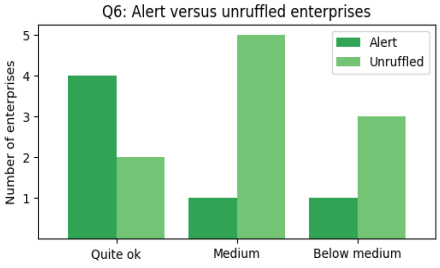


Figure 2. Cybersecurity awareness of alert versus unruffled enterprises.

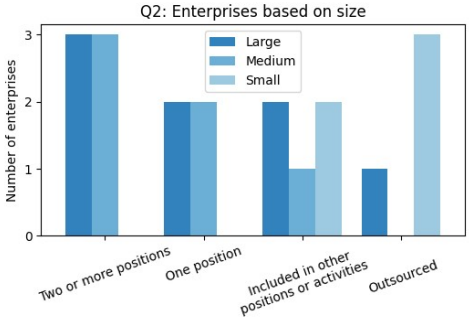


Figure 3. Internal security positions depending on company size.

Level of awareness (Q6): Most informants reported that awareness was quite good within their enterprise, but a quarter of them described it as poor, especially the small ones. Unsurprisingly, awareness is higher in the alert enterprises that report zero-tolerance for security breaches (Figure 2).

Internal positions versus outsourcing (Q2): Most large and medium-sized enterprises had internal positions dealing with cybersecurity, whereas many smaller ones outsourced security to their ICT service suppliers (Figure 3). Those small enterprises tended not to have dedicated security positions and sometimes appeared to trust their security providers blindly without thoroughly comprehending the security measures that were being put in place for them.

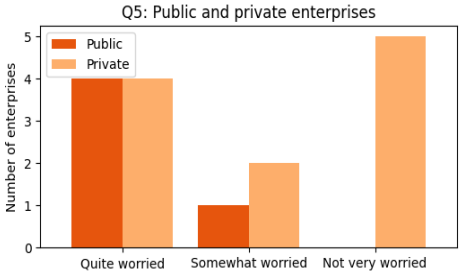
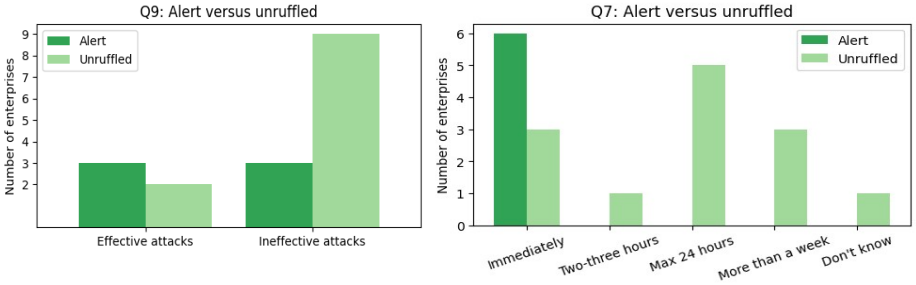


Figure 4. Threat perception in public versus private enterprises.

Perception of threats (Q5): Public enterprises reported fear of cyberattacks more often than private ones (Figure 4). This tendency was less clear when comparing large and small enterprises, although those small enterprises that reported low to medium cybersecurity awareness were also least worried about attacks. The informants who reported lower competence also tended to express the greatest satisfaction with the security work in their enterprises and were least concerned about successful attacks.



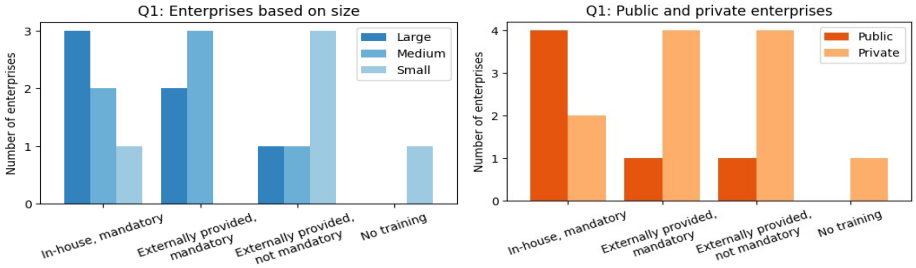
(a) (b)

Figure 5. Past experiences and assessment of impact of alert versus unruffled enterprises.

The enterprises were most concerned about phishing and ransomware attacks, with only a few enterprises mentioning organised and state crime. Among those most worried about phishing attacks, some organisations had either voluntary courses or none at all. These enterprises did not seem to have any effective strategies to stop phishing attacks. Several informants explained that their organisations were working to improve the situation, but relied on their security provider in the meantime. This mostly

applied to those small and medium-sized unruffled private enterprises that reported not being particularly worried about attacks.

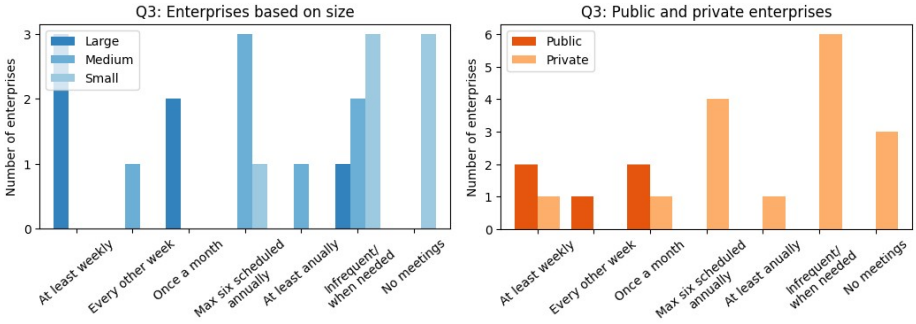
Past experiences (Q9-10): None of the small enterprises in our study had experienced successful cyberattacks in the past. The enterprises that had not been victim of successful attacks tended to worry less that it might happen to them too and were less concerned about consequences (Figure 5). This may explain in part why small businesses were less concerned about cybersecurity in general. Their lack of past experience with successful attacks might have given a false sense of security.



(a) (b)

Figure 6. Training availability depending on company size and sector.

Awareness activities – training (Q1): Almost all of the enterprises offered some form of course or training, in particular the larger enterprises and public organisations (Figure 6). However, in several enterprises the courses were voluntary or only compulsory for parts of the organisation. As a result, a large proportion of employees in the enterprises did not take the voluntary courses. This is a situation that could often be improved by follow-up routines and compulsory testing or training.

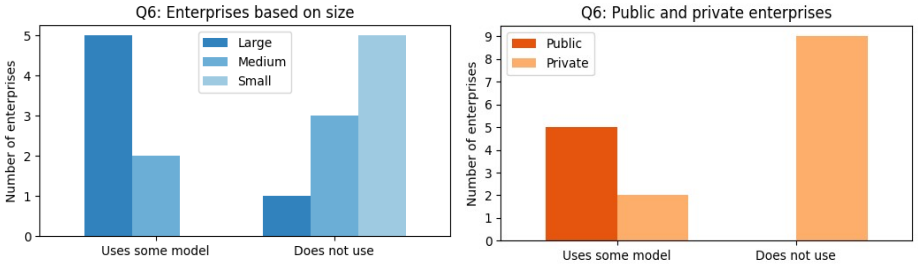


(a) (b)

Figure 7. Meeting activity depending on company size and sector.

Awareness activities – meetings (Q3): The large public enterprises prioritised frequent meetings regarding cybersecurity, as did public organisations (Figure 7). Many

other organisations only called meetings when the situation demanded it or avoided them completely. Routine meetings regarding cybersecurity would undoubtedly create a greater cybersecurity culture, whether only for managers or for everyone.



(a) (b)

Figure 8. Use of maturity models depending on company size and sector.

Awareness activities – assessments (Q8): The large and alert enterprises with zero tolerance for downtime claimed high awareness, and they mostly also had some form of maturity model to back it up (Figure 8). Importantly, all the public enterprises had maturity models in place, but almost none of the private ones. Notably, none of the small enterprises used maturity models to assess cybersecurity awareness (Figure 8).

Online access (Q11): Almost all the small enterprises gave their employees unlimited access to the web, whereas most of the large and medium-sized enterprises had set up in-house limitations or relied on DNS protection from their internet suppliers. Some of the enterprises that provided unlimited internet argued that they trusted their employees' judgments and their company culture, which is contradictory because several of them also reported no mandatory training or regular meetings related to cybersecurity awareness. They also answered that awareness in the enterprise was medium or below.

Physical access (Q12): In general, the enterprises had physical access controls in place. The large and most medium-sized enterprises also had procedures in place for visitors. Only the larger enterprises that were distributed across many buildings had free access to some of their areas.

5 Discussion

The study indicates that, in general, Norwegian enterprises devote attention to cybersecurity awareness. Many enterprises have implemented a diverse set of measures to promote it. However, there are still areas that can be improved, with varying challenges facing different types of enterprises.

Comparison with earlier studies: Of the 12 main questions in interview guide, ten were adapted from a previous study of English enterprises (Erdogan et al. 2023) and two from a study of Jordanian enterprises (Dahbur et al. 2017), both presented earlier. We now compare our responses from Norwegian enterprises with earlier studies.

Level of competence (Q4): In the English survey, the majority of respondents reported moderate to basic knowledge and about half said it was moderate to expert (Erdogan et al., 2023). Among the medium-sized and small Norwegian enterprises in our survey, which can be compared with the English ones based on size, a majority answered that their knowledge was medium or below medium. The English respondents thus tend to claim higher knowledge than our Norwegian informants.

Level of awareness (Q6): In PwC's survey (PwC 2003), 47% of respondents say that awareness training should be prioritised in the coming year. Several respondents in our survey stated that this had been less prioritised. When individuals understand and know how to act, they are more likely to act in a way that improves cybersecurity (Huang & Pearlson, 2019).

Internal positions versus out-sourcing (Q2): A number of small and private enterprises seemed to trust their ICT supplier blindly, but did not always have detailed knowledge of the defensive measures that were being put in place for them. It is important that enterprises and employees are aware of their attack surfaces and understand what their service provider does to bolster their cyberdefences. An IT supplier cannot provide immunity to all types of attacks, so it is essential that the enterprises themselves understand what they themselves can do in addition.

Perception of threats (Q5): The English enterprises had a tendency to trust that cybersecurity was handled in other parts of the enterprise or by other people (for example by third-party service providers) (Erdogan et al., 2023). We observed the same phenomenon in a some of the small and medium-sized enterprises in our survey. The difference was that the English enterprises reported higher internal awareness (Erdogan et al., 2023). The Norwegian enterprises of similar size most often answered that awareness was medium to below medium. Perhaps the Norwegian enterprises had a more realistic view on this particular point based on security assessments and on their own knowledge. A study of Dutch enterprises shows that small and medium-sized enterprises invest less in cybersecurity than large enterprises, but that they do not report more cyberincidents or lower profitability (Dinkova et al., 2023). The reason for this may be that the small and medium-sized enterprises go under the radar of attackers, something several of our informants mention.

Past experiences (Q9-10): In Erdogan et al.'s (2023) survey of English enterprises, 77% responded that they had not experienced any previous cyberattacks against their enterprises. Of those who knew of attacks that had occurred, 12 said the attacks

changed the integrity of information, 11 that the attacks had made their information systems unavailable, while six of the attacks had led to a breach of confidentiality (Erdogan et al., 2023).

Awareness activities – training (Q1): Training was mentioned by almost all our informants and by the literature in general. Compared to Erdogan et al.'s (2023) English enterprises, the biggest difference is that almost all the Norwegian enterprises offer some form of course or training, compared to only 19% of the English ones. However, the Norwegian courses are often voluntary or only compulsory for parts of the enterprise, and many employees do not take them.

Awareness activities – meetings (Q3): The behavioural threat from internal actors is one of the most challenging aspects of security management. Building a culture of cybersecurity in an organization guides employee behaviour and increases resistance to cyberattacks (Huang & Pearlson, 2019). Managers must create multiple formal and informal channels to report cyberincidents and share cybersecurity information dynamically (Huang & Pearlson, 2019). Regular, or at least on-demand, meetings are essential. This must not necessarily be the responsibility of management or of a CISO, but the enterprise must select a leader who is responsible for cultivating a culture of cybersecurity and who has direct power and authority to influence the cultivation process. Without a leader with specific responsibility for building the cybersecurity culture, activities will be carried out haphazardly and sometimes skipped altogether (Huang & Pearlson, 2019).

Awareness activities – assessments (Q8): Almost half of the Norwegian enterprises used cybersecurity maturity models to assess themselves. Large enterprises, public-sector organisations, and alert enterprises with zero tolerance for downtime used them most often. In contrast, those smaller enterprises that were also most satisfied with their security work rarely used any form of maturity models at all. In general, these smaller, unruffled, lower-competence organisations had fewer awareness measures of any kind in place compared to enterprises that had experienced security breaches in the past. Some of the smaller enterprises instead wisely resorted to external evaluators, but there were many that considered their security level to be sufficient without bothering to assess it.

Online access (Q11): Several of the enterprises we interviewed gave their employees unlimited access to online sources. Mostly it sounded like they trusted the employees' judgments. This is contradictory, because several of them also answered that awareness in the enterprise was medium to below medium. Also, several of the same enterprises only had voluntary security courses or offered training to only parts of the enterprise. Dahbur et al. (2017) report that enterprises with unlimited internet access scored the lowest on software security, awareness and policies.

Physical access (Q12): When it comes to online security and physical limitations, the Jordanian enterprises surveyed by Dahbur et al. (2017) and our Norwegian ones were quite similar. Like the Norwegian enterprises, the Jordanian ones were generally good at physical security.

Critique of research method: A qualitative analysis such as ours provide no objectively verifiable result (Choy, 2014). To substantiate our interview responses and make the results more reliable, we would have liked to have more informants representing more enterprises and from other positions than management. We would have liked to have more than five public enterprises to balance the number of private enterprises. The same applies to the alert enterprises with zero tolerance for successful attacks, of which we interviewed only six.

Some informants were more willing to share information than others. Therefore, the length of the various interviews varied a good deal, sometimes making their responses harder to compare.

Our analyses reported in this paper have focussed on those themes were our enterprises differed in seemingly interesting ways. As a consequence, we may have neglected to discuss some of the questions were the answers were similar, but nevertheless interesting. An example could be the responses of the alert and unruffled enterprises to question Q5 regarding fear of cyberattacks: here, the answers were very similar between the two groups, even though the alert enterprises anticipated much greater problems resulting from a successful attack.

6 Conclusion and Further Work

We have investigated how Norwegian enterprises create awareness around cybersecurity based on 16 qualitative interviews with managers in Norwegian enterprises of different sizes and from different sectors, both private and public. The purpose was to take a closer look at the measures Norwegian enterprises use to raise and sustain internal awareness. The responses were analysed thematically and compared based on company size, public/private enterprises and tolerance for cybersecurity breaches. The interview guide comprised 12 main questions, 10 of them adapted from a previous study of English enterprises (Erdogan et al., 2023) and the last two from a study of Jordanian enterprises (Dahbur et al., 2017). In this way, the responses from Norwegian enterprises could be compared to earlier international studies.

The study raises several important issues for future work. For example, very few enterprises refer to artificial intelligence (AI) in general in our interviews. Although it is obviously a very relevant topic, we did not ask direct questions about it, because AI is a technique and techniques were not the focus of our study. Of course, AI can also

be used both to improve cybersecurity and to create more advanced forms of attack. It has the capacity to simulate target-specific scenarios that the security team and organization can train on to prepare for actual cyberattacks (PwC, 2023). It can use large amounts of data about past attacks to simulate and improve, for example, phishing tests. It can also create surveys for employees based on previous attacks. For this reason, AI can be used to enhance awareness in all types of businesses, and it is a central technique to investigate in future studies.

Another issue is our respondents. We exclusively interviewed managers of different types. In addition, we would like to compare the responses of ordinary employees with what their managers have said. We could then compare perspectives and experiences of managers and their employees in the same enterprises. This could potentially be employees who had nothing to do with IT operations. Ordinary employees will always be a potential risk in terms of knowledge and awareness, and their opinions about and views of the awareness and measures taken in the enterprise will always be important.

It would also be interesting to investigate further the differences in security efforts and awareness between enterprises that have been hit by successful cyberattacks and those that have not. Do they prioritise different measures; have they taken more precautions; and do they communicate cyberpolicy more effectively with employees? Further research could also investigate the difference between enterprises that use maturity models or assessments of security measures, and those that do not choose to use them. Are enterprises without measurements more positive about safety and awareness? Our results may suggest this, but a more in-depth study of this topic could provided clearer answers. cybersecurity is constantly evolving and further research on is extremely important.

References

1. Bendovschi, A. (2015). Cyberattacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1
2. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*. Available at: https://doi.org/10.1191/1478088706qp063oa
3. Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering*, 12(3), 299–310. https://doi.org/10.18280/ijsse.120304
4. Choy, L. T. (2014). The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. *Journal of Humanities and Social Science 19(4):99-104.* https://www.researchgate.net/publication/269752866_The_Strengths_and_Weaknesses_of_Research_Methodology_Comparison_and_Complimentary_between_Qualitative_and_Quantitative_Approaches
5. Dahbur, K., Bashabsheh, Z., Bashabsheh, D., (2017). Assessment of Security Awareness : A Qualitative and Quantitative Study. *Scholarly Journal*, Vol.13, 37-58, 101-102. https://

www.proquest.com/openview/ba98a8bc4cf71224c96295ee6eeea0fe/1?pq-origsite=gscholar&cbl=28202
6. De Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007
7. Departementene (2019). Nasjonal strategi for digital sikkerhet. Regjeringen. Available at: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf
8. Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? Small Business Economics. Available at: https://doi.org/10.1007/s11187-023-00803-0
9. Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. (2023). Cybersecurity awareness and capacities of SMEs. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, 296- 304. https://sintef.brage.unit.no/sintef-xmlui/handle/11250/3056514
10. Ergen, A., Ünal, N.A., Saygili, S.M. (2021). Is It Possible to Change the cybersecurity Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies*. Available at: https://www.richtmann.org/journal/index.php/ajis/article/view/12588
11. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*, *09*(02), 133–153. https://doi.org/10.4236/jis.2018.92010
12. Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, 59(6), 585–591. https://doi.org/10.1016/j.bushor.2016.07.004
13. Huang, K., & Pearlson, K. (2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. Available at: https://scholarspace.manoa.hawaii.edu/items/c2f05c8b-a609-4c08-8dea-2d1c4e453b88
14. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. (2018). *What is the impact of successful cyberattacks on target firms?* National Bureau of Economic Research. Available at: https://www.nber.org/system/files/working_papers/w24409/w24409.pdf
15. KnowBe4. (2022). Introducing the Security Culture Maturity Model. Available at: https://www.bu.edu/tech/files/2022/08/Resource_Security-Culture-Maturity-Model-WP_EN-US.pdf
16. Mykkeltvedt, I. (2024). Hvordan skaper norske bedrifter bevissthet rundt cybersikkerhet? Dept. Information Science and Media Studies, University of Bergen.
17. NSM. Cyberangrep har blitt hverdagskost. (2022). Nasjonal sikkerhetsmyndighet. Available at: https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost
18. NSM. (2023). Cybersikkerhet. Nasjonal sikkerhetsmyndighet. Available at: https://nsm.no/regelverk-og-hjelp/rapporter/cybersikkerhet/
19. PwC. (2023). *Cybercrime Survey 2023*. Available at: https://publikasjoner.pwc.no/cybercrime-survey-2023/
20. Tenny, S., Brannan, J. M., & Brannan, G. D. (2017). *Qualitative study*. StatPearls [Internet]. https://pubmed.ncbi.nlm.nih.gov/29262162/