A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic

Annika Andreasson*, Henrik Artman*†, Joel Brynielsson*†, Ulrik Franke*‡
*KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
†FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden
‡RISE Research Institutes of Sweden, SE-164 29 Kista, Sweden
Email: {anniandr, artman, joel, ulrikf}@kth.se

***Abstract*—The COVID-19 pandemic has accelerated the digitalization of the Swedish public sector, and to ensure the success of this ongoing process cybersecurity plays an integral part. While Sweden has come far in digitalization, the maturity of cybersecurity work across entities covers a wide range. One way of improving cybersecurity is through communication, thereby enhancing employee cyber situation awareness. In this paper, we conduct a census of Swedish public sector employee communication on cybersecurity at the beginning of the COVID-19 pandemic using questionnaires. The study shows that public sector entities find the same sources of information useful for their cybersecurity work. We find that nearly two thirds of administrative authorities and almost three quarters of municipalities are not yet at the implemented cybersecurity level. We also find that 71 % of municipalities have less than one dedicated staff for cybersecurity.**

***Index Terms*—Cybersecurity; COVID-19; public sector; situation awareness.**

I. Introduction

The COVID-19 pandemic has taken its toll on society all over the world; first and foremost in terms of human life and suffering in the wake of illness, but also through the secondary effects disrupting everyday life and the economy. Among those secondary effects is the impact on cybersecurity. As people and organizations have struggled to adapt to the "new normal," changing their patterns of work, social interaction, consumption, education, commuting, travel, etc., new cyber risks have emerged. Some risks are non-adversarial: when processes and procedures change rapidly, the risks of human errors, untested software, and improvised processes can easily entail service outages and data being lost or exposed to the wrong eyes. Other risks are adversarial: people working from home under stressful conditions and outside corporate networks offer new attack vectors that cybercriminals can take advantage of.

In this paper, we study such COVID-19 effects on cybersecurity by investigating how the Swedish public sector reacted to the new threat landscape. In particular, we study how government administrative authorities, county councils, and municipalities gathered information to uphold cyber situation awareness [1] and how they chose to communicate to their employees about cybersecurity.

This study was supported by the Swedish Armed Forces.

More precisely, we address three research questions:

1) To what degree did Swedish public sector entities find cybersecurity information resources useful at the beginning of the COVID-19 pandemic?
2) How many Swedish public sector entities have communicated to their employees about specific cybersecurity risks at the beginning of the COVID-19 pandemic?
3) What factors influenced Swedish public sector entities to communicate to their employees about cybersecurity at the beginning of the COVID-19 pandemic?

This paper extends our previous work [2]. Whereas the previous paper covered government administrative authorities only, we now present a fuller picture of the Swedish public sector: government administrative authorities, county councils, and municipalities. This broader material allows us to draw more profound conclusions compared to our previous work. Municipalities and regions are autonomous units as compared to the administrative authorities, which are part of the central government. This makes it interesting to compare how they handled cybersecurity during the pandemic.

Sweden is an interesting case to study, since the country regularly scores high in terms of digitalization. For example, in the European Commission's Digital Economy and Society Index (DESI) 2020 [3], Sweden ranked second among all the EU countries. Indeed, the top four EU countries in the index (Finland, Sweden, Denmark, and the Netherlands) are considered among the global leaders in digitalization. However, Sweden often scores worse in international rankings on cybersecurity. For example, Sweden ranked only 17th in the ITU Global Cybersecurity Index (GCI) in 2017 [4] (and only 32nd in the 2018 edition, but this is a less valid measure since Sweden did not actively participate in the ranking exercise that year). This tension between being a forerunner in digitalization but somewhat lagging behind in cybersecurity makes Sweden an interesting object of study.

The rest of the paper is structured as follows. Section II discusses some related work, followed by a description of the undertaken methodology in Section III. Section IV contains the results obtained. The findings are discussed in Section V, before Section VI concludes.

II. Related Work

Related work can be categorized in two broad areas: 1) studies focusing on cybersecurity in the COVID-19 pandemic context, and 2) studies focusing on cybersecurity in the Swedish public sector context. Regarding the first area, there are still few peer-reviewed empirical studies published with a focus on cybersecurity in the context of the COVID-19 pandemic. A large part of the limited existing literature concerns cybercrime. Analyzing 185 distinguishable COVID-19 scam records, Naidoo [5] notes that the pandemic allowed cybercriminals to utilize specific situational factors brought about by the pandemic for criminal purposes. Lallie et al. [6] analyze UK COVID-19-related data from cyber-attacks suffered between January 6 and March 31, 2020, and find a loose correlation between the attacks and public media communication containing information used in the attacks. Hijji and Alam [7] perform a literature review selecting 52 formal and gray literature sources on cyber-attacks based on social engineering during the pandemic, and find that the most common techniques for social engineering used are phishing, scamming, spamming, smishing, and vishing.

Other studies concern teleworking. Eiza et al. [8] propose a framework for businesses to evolve their current practices to secure the homeworking IT environment. Georgiadou et al. [9] surveyed 264 employees in 13 European countries evaluating the preparedness of individuals and organizations to work from home. One finding was that even though possible, organizations did not all offer employees to work from home. Other papers addressing the dangers associated with pandemic telecommuting are Abukari & Bankas [10] and Ahmad [11], whereas Furnell & Shah [12] discuss UK businesses' preparedness to work from home early in the pandemic.

Regarding the second area, there are pertinent studies covering the public sector entities targeted in this study. Borg et al. [13] study software development in Swedish government agencies through a census of 240 administrative authorities (but not county councils or municipalities). Among the 93 software-developing respondents, security awareness is deemed important throughout the development cycle, and security features prominently in software requirements specifications. However, the full cybersecurity posture of any enterprise encompasses much more than just its development practices. In this respect our study of awareness and employee communication in the face of COVID-19 is quite different from that of Borg et al. [13].

The Swedish Civil Contingencies Agency (MSB) authorized a study of information security at government agencies in 2014 [14] and another study of information security at county councils in 2018 [15]. The Swedish Association of Local Authorities and Regions (SKR) commissioned a study of information security at municipalities in 2019 [16]. While these studies all provide interesting background material, they were conducted before the pandemic, as opposed to our study.

III. Method

To investigate Swedish public sector employee communication on cybersecurity during the COVID-19 pandemic, we conducted censuses of government administrative authorities, county councils, and municipalities. The record of Swedish administrative authorities was downloaded from Statistics Sweden on June 1, 2020, and the records of Swedish county councils and municipalities were received upon request from SKR on September 7 and September 2, respectively. The records listed 250 administrative authorities, 21 county councils, and 290 municipalities.[1] The records of county councils and municipalities provided email addresses for all entities, whereas the administrative authority record only provided email addresses for 236 entities, three of which had email addresses to which emails could not be delivered after repeated attempts.

A three-section questionnaire (see appendix) was created to collect data from the administrative authorities. The questionnaire was subsequently adapted to be suitable for data collection from county councils and municipalities by changing references from *administrative authority* to *county council* or *municipality* where needed. The first section of the questionnaire collected general information about the organization and its cybersecurity work: name of the entity, organization of cybersecurity work, and self-assessed cybersecurity maturity. The second section dealt with questions referring to COVID-19-specific issues: how useful was information from cybersecurity information sources—MSB, CERT-SE, Krisinformation.se,[2] the Swedish Security Service, the National Defence Radio Establishment (FRA), the Swedish Defence Research Agency (FOI), the European Union Agency for Cybersecurity (ENISA), Europol, cybersecurity companies, traditional media, trade press, cybersecurity blogs/podcasts, and informal civil servant contacts—and whether it influenced communication to employees; if the entity had communicated about certain cybersecurity risks—phishing, invoice fraud, video meetings, unsanctioned cloud collaboration, social engineering, telecommuting—and if certain factors influenced the decision to communicate to employees—phishing attempts, attempts at invoice fraud, video-meeting incidents, unsanctioned cloud collaboration, social engineering, noncompliant telecommuting, network traffic changes, and/or previous crisis experience. Finally, the third section queried willingness to participate in future cyber situation awareness research.

A regular web form, without unique links or password protection, was used for the questionnaire. The link to the form was distributed by individual email to the entities with email addresses listed. The email addresses listed mainly pointed to monitored generic mailboxes, and therefore the email requested that the email be forwarded to a staff member knowledgeable about the entity's cybersecurity work.

Data collection was done in two periods during 2020; in the first period data was collected from the administrative authorities and in the second period from the county councils and municipalities. The administrative authorities were invited by email to respond to the questionnaire on June 10. The

[1] Gotland is both a county council and a municipality. The email listed was the same in the records for both county council and municipality, and they were only sent the county council questionnaire.

[2] The official site for emergency information from Swedish authorities.

TABLE I
ORGANIZATION OF CYBERSECURITY AT SWEDISH PUBLIC SECTOR ENTITIES.

Entity type	Organizational form	*N*	%
Administrative authority	Cybersecurity department	18	13
	≥ 1 dedicated staff	38	28
	< 1 dedicated staff	64	48
	Outsourced cybersecurity	14	10
	Total	134	99
County council	Cybersecurity department	2	18
	≥ 1 dedicated staff	7	64
	< 1 dedicated staff	2	18
	Outsourced cybersecurity	0	0
	Total	11	100
Municipality	Cybersecurity department	10	8
	≥ 1 dedicated staff	24	19
	< 1 dedicated staff	92	71
	Outsourced cybersecurity	3	2
	Total	129	100

TABLE II
SELF-ASSESSED CYBERSECURITY MATURITY LEVEL AT SWEDISH PUBLIC SECTOR ENTITIES.

Entity type	Cybersecurity work is ...	*N*	%
Administrative authority	Initiated	54	40
	Documented	32	24
	Implemented systematic	32	24
	Evaluated systematic	12	9
	Optimized systematic	4	3
	Total	134	100
County council	Initiated	1	9
	Documented	2	18
	Implemented systematic	7	64
	Evaluated systematic	1	9
	Optimized systematic	0	0
	Total	11	100
Municipality	Initiated	50	39
	Documented	45	35
	Implemented systematic	27	21
	Evaluated systematic	7	5
	Optimized systematic	0	0
	Total	129	100

administrative authorities that had not responded were sent a first reminder on June 22 and a second reminder on June 30. The data collection concerning administrative authorities closed on August 1. The county councils and municipalities were similarly invited on September 9. The non-responding municipalities were sent a reminder on September 29 and the non-responding county councils on September 30, receiving only one reminder. The second part of the data collection closed on October 27.

Upon data collection closure, the collected data was downloaded into a spreadsheet file and collated. The data was subsequently inspected and treated. For responses representing associations of municipalities, separate data entries were created for each municipality, keeping the same responses. In one case, a municipality belonging to an association provided an individual response. This municipality's input was kept, apart from the response to the question on how the cybersecurity work was organized, where the response of the association was entered. One county council provided two responses; the most recently provided response was kept and the first response was discarded.

IV. RESULTS

From 233 delivered requests to administrative authorities, 174 responses were obtained. 15 administrative authorities declined to participate, 25 referred to their host authority, and 134 completed the questionnaire (130 through the web form and four by email). Among the 25 administrative authorities who referred to host authorities, 11 were represented by responding hosts. The 134 completed questionnaires thus represent 145 administrative authorities, resulting in a 58 % coverage of administrative authorities. From the 21 county councils we received 14 responses, three of which were emails declining participation and 11 that were completed questionnaires, giving a 52 % coverage of county councils. From the 289 contacted municipalities, we received 123 responses; six by email declining participation and 117 in the form of completed questionnaires (115 through the web form, one by email, and one by phone). Accounting for responses representing associations of municipalities, the 117 completed questionnaires represent 129 municipalities, giving a 45 % coverage of municipalities.

The first section of the questionnaire collected background data on 1) how cybersecurity work is organized and 2) self-assessed cybersecurity maturity, as summarized in Tables I and II. Concerning the organization of cybersecurity work at Swedish public sector entities, 58 % of administrative authorities report either having a staff member with cybersecurity as one of several tasks or having outsourced cybersecurity. The corresponding share for municipalities is 74 %. Among the county council respondents, 82 % report having at least one dedicated staff member or a cybersecurity department. As for maturity level, the results show a level of not yet implemented cybersecurity work for 64 % of the administrative authorities, 27 % of the county councils, and 74 % of the municipalities.

In the second section of the questionnaire, COVID-19-specific data was collected. The usefulness of different cybersecurity information sources was assessed by respondents, including whether information from each source influenced communication. Information from MSB was deemed useful by 100 % of county councils, 95 % of municipalities, and 89 % of administrative authorities, thus being the most useful source for all entities. Information from MSB was also reported as most influential on communication by 36 % of county councils and 37 % of municipalities. For administrative authorities, however, 39 % reported that informal contacts with civil servants at other government agencies influenced communication, making it the most influential source for communication. The information source least useful to the entities was Europol, with 99 % of municipalities, 95 % of administrative authorities, and 82 % of county councils rating it as "not useful." An equal share of county councils rated information from FOI as "not useful." Complete results for usefulness of different information sources are displayed

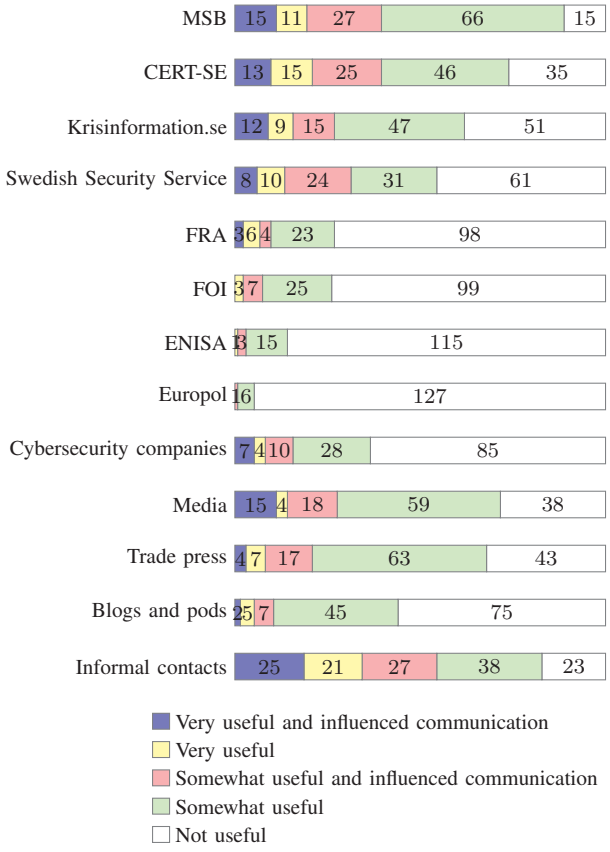

Fig. 1. Usefulness of different information sources for the administrative authorities' work on cybersecurity during the COVID-19 pandemic ($N = 134$).

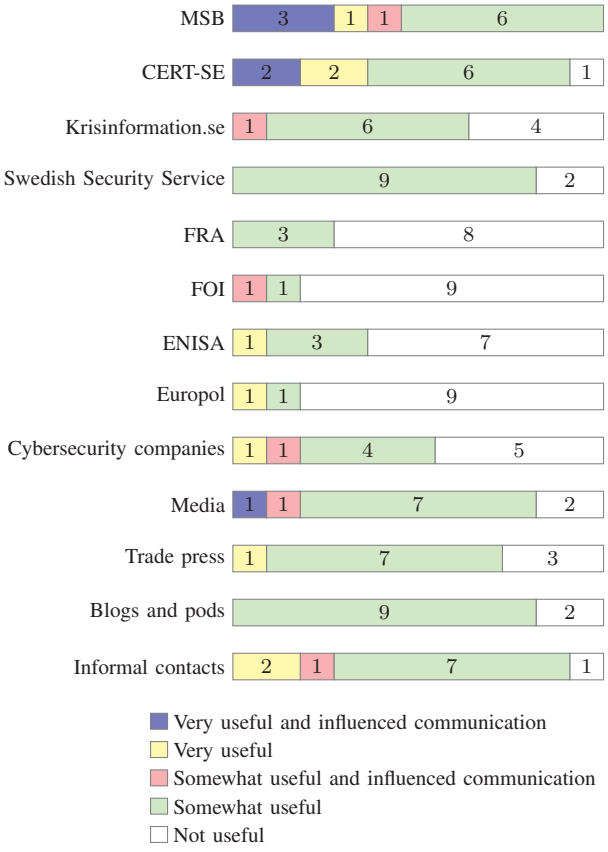

Fig. 2. Usefulness of different information sources for the county councils' work on cybersecurity during the COVID-19 pandemic ($N = 11$).

in Fig. 1 for administrative authorities, Fig. 2 for county councils, and Fig. 3 for municipalities.

The top three risks communicated by Swedish public sector entities were risks related to video meetings, telecommuting, and phishing. Increased vigilance about video meetings was the most common risk communicated to employees by administrative authorities (90 %, Fig. 4) and municipalities (84 %, Fig. 6), whereas risks with phishing was most commonly communicated by county councils (91 %, Fig. 5). Social engineering was the least commonly communicated risk for all entities, with 36 % of municipalities, 45 % of county councils, and 47 % of administrative authorities having communicated about the risk to employees.

Factors influencing Swedish public sector entities to communicate to employees during the COVID-19 pandemic are presented in Fig. 7 for administrative authorities, Fig. 8 for county councils, and Fig. 9 for municipalities. It is interesting to contrast what factors are driven by others' reports and what factors are driven by own observation. For example, 54 % of the administrative authorities reported that video-meeting incidents influenced the decision to communicate to employees, where 38 % of them based this decision solely on others' reports. Looking instead at where own observations (or rather experience) mattered the most, all three categories of respondents identify previous crisis experience, as seen in the bottom bar in the diagrams.

V. Discussion

Looking at the organization of cybersecurity work at the Swedish public sector entities, Table I shows that 74 % of municipalities have either outsourced cybersecurity or have less than one dedicated staff member for these tasks, compared to 58 % of administrative authorities and 18 % of county councils. These results are in line with previous results presented in technical reports. In 2019, while 169 out of 250 municipalities reported they had a Chief Information Security Officer (CISO) (or equivalent), only 50 % of the CISOs had more than 10 hours a week dedicated to information security work [16]. As a contrast, the county councils reported that 10 out of 21 councils had a full-time CISO in 2018 [15]. In 2014, 38 % of information security coordinators at government agencies stated that they could not perform their job satisfactorily due to insufficient resources, mandates, and competencies [14].

74 % of municipalities and 64 % of administrative authorities self-assess as not yet having implemented cybersecurity work, compared to only 27 % of county councils. This difference in maturity could stem from differences in the nature of the entities' operations. One of the main responsibilities of the county councils is healthcare, where they handle large amounts of sensitive personal data. Municipalities' main responsibilities include schools, elderly care and social services. (The administrative authorities are more heterogeneous, both in size and operations.) Thus, it is not unreasonable to

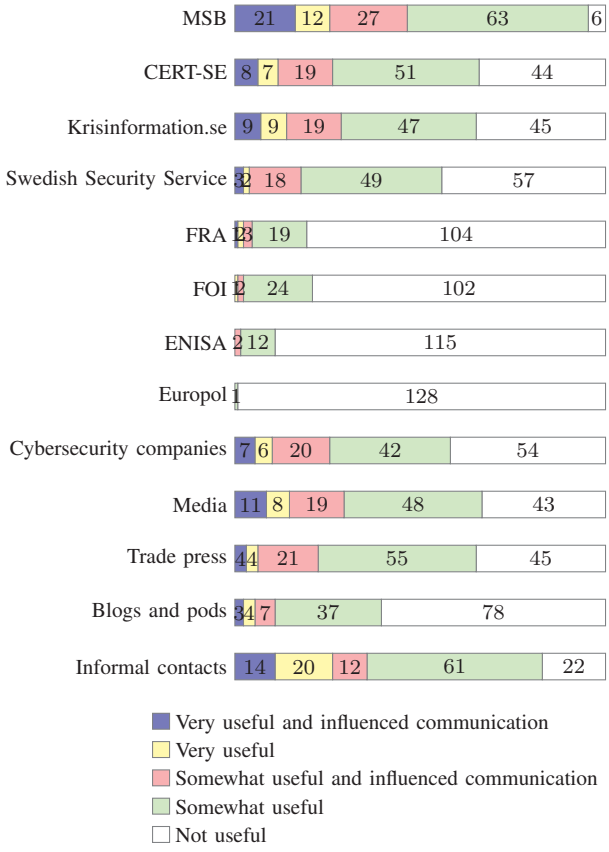

Fig. 3. Usefulness of different information sources for the municipalities' work on cybersecurity during the COVID-19 pandemic ($N = 129$).

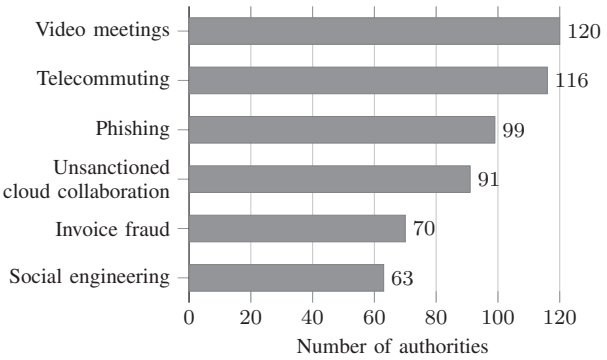

Fig. 4. Swedish administrative authorities' communication to employees about specific cyber risks during the COVID-19 pandemic ($N = 134$).

assume that the healthcare aspect of the county councils has entailed greater cybersecurity efforts, and especially so since healthcare is one of the essential services subject to the EU NIS directive. The NIS requirement to conduct systematic and risk-based information security work is on a par with the level of "implemented systematic cybersecurity work" in the questionnaire (see appendix).

Another factor possibly influencing organization and maturity of cybersecurity work is organizational size. Measuring size as full-time equivalents of personnel, Fig. 10 plots these

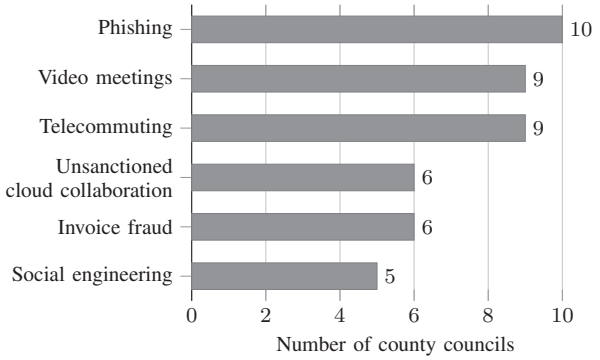

Fig. 5. Swedish county councils' communication to employees about specific cyber risks during the COVID-19 pandemic ($N = 11$).

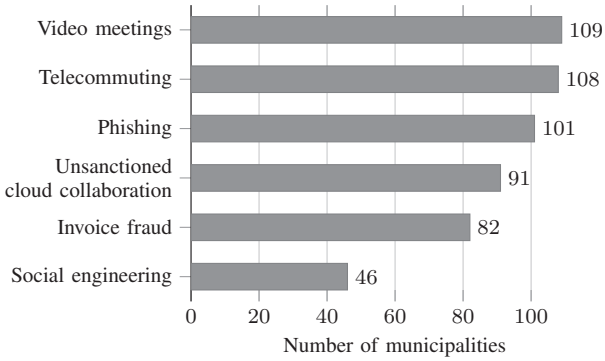

Fig. 6. Swedish municipalities' communication to employees about specific cyber risks during the COVID-19 pandemic ($N = 129$).

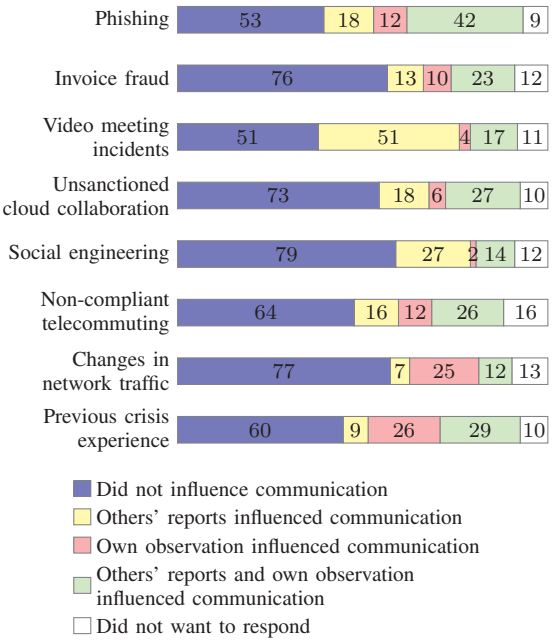

Fig. 7. Factors influencing Swedish administrative authorities' decision to communicate to employees during the COVID-19 pandemic ($N = 134$).

relations.[3] As can be seen in the graphs, there is indeed a

[3]Data on full-time equivalents for 2019 were available and obtained from official statistics: https://skr.se/arbetsgivarekollektivavtal/uppfoljninganalys/personalstatistik/personalenisiffror.850.html (county councils and municipalities), https://www.statskontoret.se/om-oss/om-webbplatsen/oppna-data/ (administrative authorities).

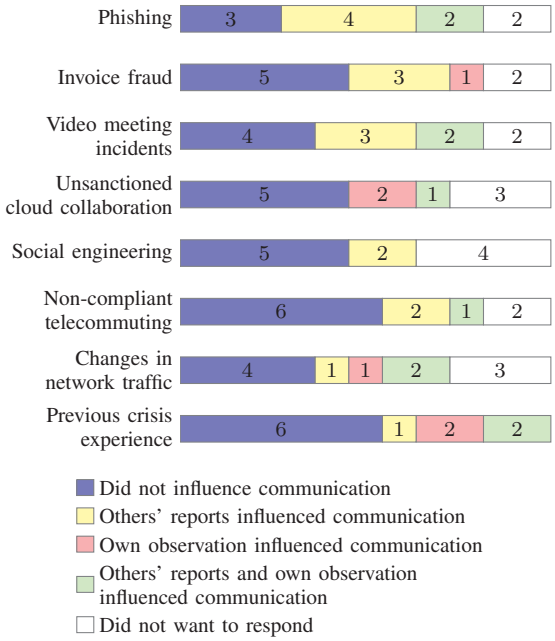

Fig. 8. Factors influencing Swedish county councils' decision to communicate to employees during the COVID-19 pandemic ($N = 11$).

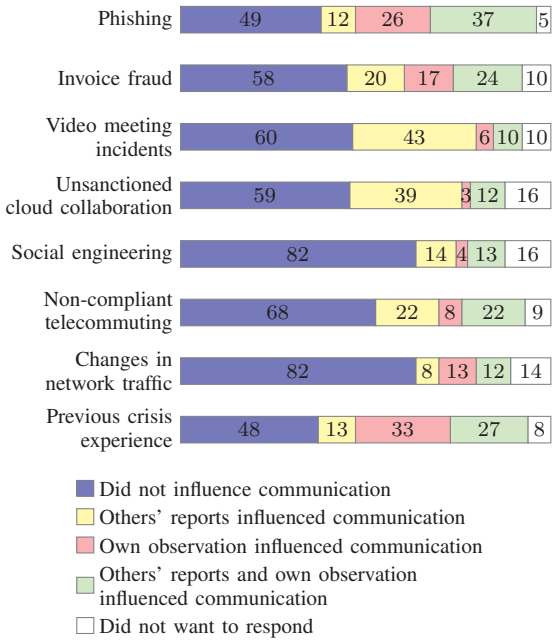

Fig. 9. Factors influencing Swedish municipalities' decision to communicate to employees during the COVID-19 pandemic ($N = 129$).

weak tendency that smaller organizations are somewhat less mature (top graph) and dedicate less resources to cybersecurity (bottom graph). However, the variability is large, and there is a considerable number of larger organizations that are quite immature in their cybersecurity work. Inspecting the empty upper left part of the graphs, it can be concluded that a certain organizational size is a necessary, but far from sufficient, condition to obtain 1) the higher levels of cybersecurity maturity, and 2) a larger cybersecurity organization. (The second conclusion is almost self-evident.)

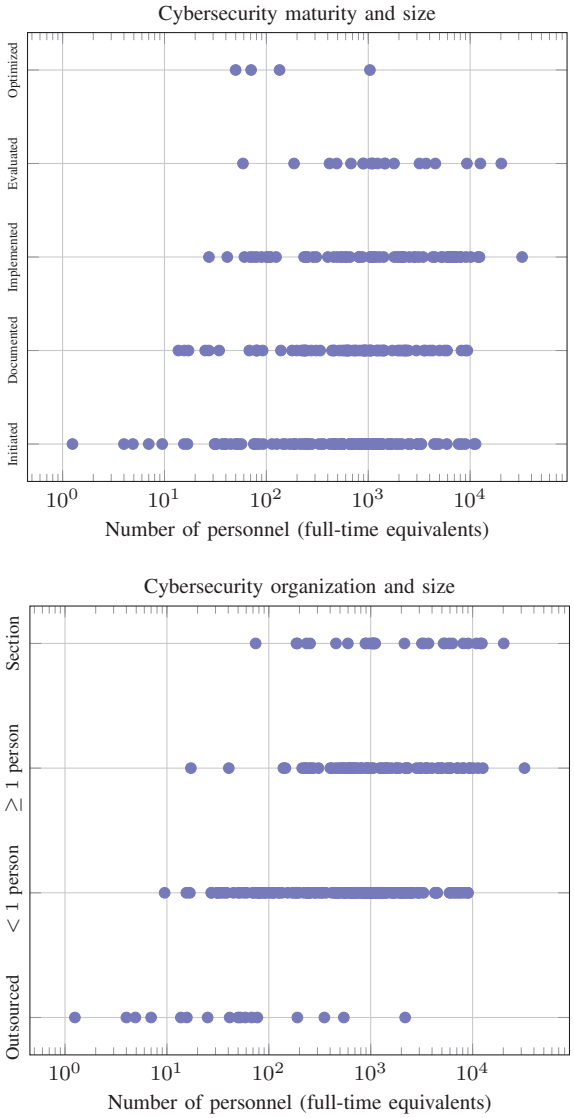

Fig. 10. Cybersecurity maturity and organization related to size (measured as full-time equivalents of personnel, plotted on log-scale). $N = 271$ (compared to the cohorts in Tables I and II, two anonymous entities and one where the official statistics listed zero employees have been removed).

Information from MSB was reported as useful by 100 % of county councils, 95 % of municipalities, and 89 % of administrative authorities, which is hardly surprising given that MSB was tasked by the government to coordinate verified information during the pandemic. A priori, one might assume that different types of entities would turn to different sources of information, but that is not the case here. It is also clear that international organizations, such as ENISA or Europol, are not deemed useful by Swedish public sector entities. Furthermore, national agencies such as FRA and FOI do not receive high ratings; probably since they are not tasked to disseminate their findings directly throughout the public sector or to the public at large, but rather to smaller audiences of decision-makers. The media is rated as useful by about two thirds of municipalities and administrative authorities, and by about four fifths of county councils. This is interesting, as the media usually reports afterwards. Still, such ex post

reporting can serve as cautionary tales for others. It should also be noted that informal contacts between civil servants at different entities are considered useful and influential sources of information by 91 % of county councils, 83 % of municipalities and 83 % of administrative authorities, indicating that there are strong professional networks in place. Some examples (from the free-text responses) include collaborations between municipalities within the same region, between municipalities and county administrative boards (these boards are administrative authorities), and with ITCF, the Swedish higher education CIO-forum network.[4]

Given that the entities' communication is influenced by the same sources, it is not surprising that their resulting risk communication is similar. As can be seen in Fig. 4–6, the most commonly communicated risks were risks related to video meetings, telecommuting, and phishing. While a larger share of the administrative authorities and municipalities communicated about risks directly connected to working from home—video meetings and telecommuting—phishing was the risk communicated by the largest share of county councils. It is helpful to discuss this communication about risk through the lens of *first-order risks* (e.g., data leaking through insufficiently protected video meetings or unsanctioned cloud collaboration) and *second-order risks* (e.g., where an attacker creates purportedly authentic invoice fraud using data leaked from first-order risks). While the risks that are more closely connected to working from home might be the first ones that spring to mind, it would be unwise to downplay second-order risks, which may be closer to attackers' ulterior motives. It is clear from the results that Swedish public sector entities have in general focused more on the first-order risks.

Following the argument that the public sector entities are influenced by the same sources, it is not surprising to see a large part of the entities citing "others' reports of video-meeting incidents" as influencing the decision to communicate about the risk. For all entities, others' reports of video-meeting incidents outweigh own observations as a factor affecting the decision to communicate.

There are some limitations to the study. The municipalities and county councils received the questionnaire at a later date when the infection rates were dropping and some work places were encouraging employees to come back to the office. This may have affected the responses from these entities compared to the administrative authorities which received the questionnaire when infection rates were higher. As the email sent out to the entities was not personally addressed, we rely on the entities ensuring that the link to the questionnaire reached a suitable member of staff. The link was not password protected or unique to each respondent, meaning that anyone with the link could complete the questionnaire. The questionnaire itself did not provide any definitions of maturity levels, which should be kept in mind when interpreting the results. There is also the question of how respondents interpret "own observation," e.g., if they take it to mean a time period when observation occurs, or an actual event being observed.

[4]http://itcf.se/english/.

VI. Conclusions

The COVID-19 pandemic has changed how many organizations operate, and has led to a large number of employees working from home. As a consequence, organizations have less control over the way employees work, and citizens have an increased demand for digitized public sector services. For the first time since 2016, when reporting IT incidents became mandated for Swedish government agencies by law, human error was the most frequently reported incident to MSB, making up 24 % of reported incidents [17]. Under these circumstances, organizations can aid employee situation awareness through communication. In this context, the present study investigated Swedish public sector employee communication on cybersecurity during the COVID-19 pandemic, as well as the maturity and organization of entities' cybersecurity work.

In the beginning of the COVID-19 pandemic, almost the entire Swedish public sector found the cybersecurity information from MSB useful. Different types of entities do not seem to turn to different sources of information, and informal contacts among civil servants are relatively important. The top three risks communicated to employees were risks related to video meetings, telecommuting, and phishing. Such communication was influenced by a combination of own observations, others' reports, and previous crisis experience.

While the study showed cybersecurity maturity levels of a majority of the Swedish public sector entities to be at the not yet implemented level, the county councils show a higher maturity (73 % at the implemented or evaluated systematic level). Looking at the influence of organizational size on cybersecurity organization and cybersecurity maturity, smaller organizations show a weak tendency of being less mature and having fewer employees dedicated to cybersecurity work. Ongoing initiatives to improve the situation include the government having tasked MSB to educate the public sector in cybersecurity in 2019, although this initiative has now been delayed due to the COVID-19 pandemic [18]. A follow-up investigation of public sector cybersecurity maturity after implementation of these education efforts ought to be important in understanding the evolution of Swedish public sector cybersecurity.

Appendix: Questionnaire

(Translated from Swedish. For simplicity, all three respondent designations have been changed into "entity.")

1. About the entity
   - 1.1. Entity
   - 1.2. How is the entity's cybersecurity work organized?
     The following response options were available: the entity has a cybersecurity department / the entity has at least one dedicated staff member responsible for cybersecurity / the entity has one staff member who has cybersecurity as one of their tasks / the entity has outsourced cybersecurity.
   - 1.3. The entity's cybersecurity maturity is considered to be:
     The following response options were available: initiated cybersecurity work / documented cybersecurity work / implemented systematic cybersecurity work /

evaluated systematic cybersecurity work / optimized systematic cybersecurity work.

2. COVID-19 and cybersecurity

2.1. Has information from the following sources been useful for the entity's work on cybersecurity issues during the COVID-19 pandemic?

- MSB
- CERT-SE
- Krisinformation.se
- Swedish Security Service
- FRA
- FOI
- ENISA
- Europol
- Cybersecurity companies
- Traditional news media (press/TV/radio)
- Trade press (IDG / Computer Sweden / Ny Teknik)
- Cybersecurity blogs/podcasts
- Informal contacts with colleagues at other entities at the civil servant level
- Other source [free text]

For each source, the following response options were available: yes, the entity found the information very useful and it influenced communication / yes, the entity found the information very useful / yes, the entity found the information somewhat useful and it influenced communication / yes, the entity found the information somewhat useful / no, the entity did not find the information useful.

2.2. Has the entity communicated to its employees that they should be more vigilant about the following cybersecurity risks during the COVID-19 pandemic?

- Phishing attempts
- Invoice fraud
- Cybersecurity at video meetings
- Collaboration using unsanctioned cloud services
- Social engineering
- Cybersecurity when telecommuting
- Other risk [free text]

For each risk, the following response options were available: yes/no.

2.3. Has the decision on communication to the entity's staff been affected by the following factors?

- Phishing attempts
- Attempts at invoice fraud
- Incidents at video meetings
- Cooperation using unsanctioned cloud services
- Social engineering
- Telecommuting that does not comply with the entity's policy
- Changes in network traffic
- Previous experience of a crisis
- Other [free text]

For each factor, the following response options were available: no, [the factor] did not influence the decision to communicate / yes, others' reports [about the factor] influenced the decision to communicate / yes, own observation [of the factor] influenced the decision to communicate / others' reports and own observation [of the factor] influenced the decision to communicate / do not want to respond.

3. Next steps

3.1. Can we contact the entity for a follow-up interview?

References

[1] U. Franke and J. Brynielsson, "Cyber situational awareness: A systematic review of the literature," *Computers & Security*, vol. 46, pp. 18–31, 2014.

[2] A. Andreasson, H. Artman, J. Brynielsson, and U. Franke, "A census of Swedish government administrative authority employee communications on cybersecurity during the COVID-19 pandemic," in *Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2020)*. Piscataway, NJ: IEEE, 2020, pp. 727–733.

[3] European Commission, "Digital Economy and Society Index (DESI) 2020," 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020

[4] ITU, *Global Cybersecurity Index (GCI) 2017*. Geneva, Switzerland: International Telecommunication Union, 2017. [Online]. Available: http://handle.itu.int/11.1002/pub/80f875fa-en

[5] R. Naidoo, "A multi-level influence model of COVID-19 themed cybercrime," *European Journal of Information Systems*, vol. 29, no. 3, pp. 306–321, 2020.

[6] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," 2020. [Online]. Available: https://arxiv.org/abs/2006.11929

[7] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions," *IEEE Access*, vol. 9, pp. 7152–7169, 2021.

[8] M. H. Eiza, R. I. Okeke, J. Dempsey, and V.-T. Ta, "Keep calm and carry on with cybersecurity @home: A framework for securing home-working IT environment," *International Journal on Cyber Situational Awareness*, vol. 5, no. 1, pp. 1–25, 2020.

[9] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Working from home during COVID-19 crisis: A cyber security culture assessment survey," *Security Journal*, 2021.

[10] A. M. Abukari and E. K. Bankas, "Some cyber security hygienic protocols for teleworkers in Covid-19 pandemic period and beyond," *International Journal of Scientific & Engineering Research*, vol. 11, no. 4, pp. 1401–1407, 2020.

[11] T. Ahmad, "Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity," 2020. [Online]. Available: https://doi.org/10.2139/ssrn.3568830

[12] S. Furnell and J. N. Shah, "Home working and cyber security: An outbreak of unpreparedness?" *Computer Fraud & Security*, vol. 2020, no. 8, pp. 6–12, 2020.

[13] M. Borg, T. Olsson, U. Franke, and S. Assar, "Digitalization of Swedish government agencies: A perspective through the lens of a software development census," in *Proceedings of the 2018 ACM/IEEE 40th International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS 2018)*. New York, NY: ACM, 2018, pp. 37–46.

[14] MSB, "En bild av myndigheternas informationssäkerhetsarbete 2014 [A view of government agency information security work 2014]," Swedish Civil Contingencies Agency, Karlstad, Sweden, Publ. MSB740, 2014.

[15] MSB, "En bild av landstingens informationssäkerhetsarbete 2018 [A view of county council information security work 2018]," Swedish Civil Contingencies Agency, Karlstad, Sweden, Publ. MSB1254, 2018.

[16] SKR, "Kommunernas informationssäkerhetsarbete [Municipalities' information security work]," Swedish Association of Local Authorities and Regions, Stockholm, Sweden, Tech. Rep., 2019.

[17] MSB, "Statliga myndigheters it-incidentrapportering 2020 [Government agencies' IT incident reporting 2020]," Swedish Civil Contingencies Agency, Karlstad, Sweden, Publ. MSB1692, 2021.

[18] MSB, "Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 [Comprehensive information and cybersecurity action plan for the years 2019–2022]," Swedish Civil Contingencies Agency, Karlstad, Sweden, Publ. MSB1635, 2021.