2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) | 978-1-7281-1056-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/ASONAM49781.2020.9381324

A Census of Swedish Government Administrative Authority Employee Communications 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*—Cybersecurity is the backbone of a successful digitalization of society, and cyber situation awareness is an essential aspect of managing it. The COVID-19 pandemic has sped up an already ongoing digitalization of Swedish government agencies, but the cybersecurity maturity level varies across agencies. In this study, we conduct a census of Swedish government administrative authority communications on cybersecurity to employees at the beginning of the COVID-19 pandemic. The census shows that the employee communications in the beginning of the pandemic to a greater extent have focused on first-order risks, such as video meetings and telecommuting, rather than on second-order risks, such as invoice fraud or social engineering. We also find that almost two thirds of the administrative authorities have not yet implemented, but only initiated or documented, their cybersecurity policies.**

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

I. Introduction

Cybersecurity has become one of the most important and urgent areas for many organizations as society is undergoing rapid digitalization. Thus, an increasing number of countries have adopted national cybersecurity strategies, and international organizations like the OECD make recommendations on digital security risk management to ensure economic and social prosperity [1]. Organizations are vulnerable to attacks not only on their public websites, but also on their increasingly web-facing cloud-based administrative systems [2], and to different forms of user-oriented attacks like phishing [3].

Cyber situation awareness is one essential aspect of managing cybersecurity. *Situation awareness* was coined by Endsley [4] within the domain of aircraft pilots and their understanding of the current and future situation. The definition of situation awareness is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [4, p. 792]. Endsley later develops the definition into a three-level situation awareness framework model for dynamic systems, where the situation awareness levels are: 1) perception, 2) comprehension, and 3) projection [5]. Cyber situation awareness is defined by Franke and Brynielsson as "a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the 'cyber' environment" [6, p. 20].

A specific organization might have cybersecurity experts who are monitoring network activities and thus gain cyber situation awareness about ongoing threats, but this awareness must also be communicated to employees more widely. Much of cybersecurity happens at the fingertips of the employee when interacting over digital systems—and deceiving that employee is often the easiest way to gain unauthorized access [7].

During the 2020 COVID-19 pandemic, much office oriented work has been relocated to home offices through telecommuting. When working from home by digital means (video-mediated meetings, increasing amount of emails, etc.) on a home internet connection, vulnerability increases as the employer organization might not have full control over router settings [8], use of unsanctioned cloud-computing tools [9], etc. Furthermore, with fewer informal contacts with colleagues, the employee might not get relevant security information as quickly as when meeting colleagues in the break room, thus missing out on contextual information pertinent to forming cyber situation awareness.

It is against this background that the current study investigates how a subset of Swedish government agencies, the administrative authorities, communicated about cybersecurity with their employees during the beginning of the pandemic. More precisely, the following research questions have been addressed:

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

The rest of this paper is organized as follows. The next section surveys the literature and situates the present work within it. Section III describes the method used to conduct the census. Section IV describes the results obtained, before

2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)

they are discussed in Section V. Finally, Section VI concludes the paper.

II. Related Work

Two main areas of related work can be identified: studies of cybersecurity in the context of the COVID-19 pandemic, and studies of cybersecurity within the Swedish public sector. These are covered in turn.

As for the first area, empirical studies of the COVID-19 impact on cybersecurity that have made their way through peer review to final publication are still rare. However, there are some preprints dealing specifically with COVID-19 cybersecurity themes. Naidoo [10] analyzes COVID-19-specific cybercrime data from FraudWatch International, finding that the pandemic begot specific situational factors that were quickly exploited by cybercriminals, such as 1) employees being ordered to telecommute, 2) increased rate of unemployment, 3) more available government funding, and 4) a switch to digital diversions instead of in situ experiences.

Using UK data on COVID-19-related attacks, Lallie et al. [11] find a loose correlation between media communications on events concerning the COVID-19 pandemic and attacks using information relating to these communications. Both Lallie et al. [11] and Naidoo [10] emphasize phishing as the predominant point of entry for cybercriminals. There are also some studies highlighting the specific challenges that organizations with employees working from home face, and how to enable the employees to become more resilient towards COVID-19-related cybercrime [12], [13]. Finally, there are also technical reports highlighting sector-specific issues, e.g., one report from the Swedish Defence Research Agency (FOI) focusing on attacks in the healthcare sector, pointing out different ways the healthcare sector is both targeted by cybercriminals and used as a guise by cybercriminals in targeting others [14].

As for the second area, several relevant studies exist. Borg et al. [15] study software development in Swedish government agencies through a census of 240 agencies, 93 of which confirmed that they develop software. While the scope of their investigation is much broader, it contains some specifically security-related findings, e.g., 1) that a high proportion of contractors correlates with less focus on security, 2) that a substantial majority of software-developing agencies agree that security awareness permeates their entire development processes, and 3) that compared to the other software qualities defined by ISO/IEC 25010, security is the most frequently mentioned quality in the software requirements specifications obtained and analyzed. Though related to our work through the focus on Swedish government agencies, Borg et al. differ considerably in their focus on software development, compared to our focus on cybersecurity awareness and employee communications. Furthermore, there are also a few relevant (though not peer-reviewed) studies of Swedish public sector information security commissioned by the Swedish Civil Contingencies Agency (MSB): one investigating government agencies [16] and a later one investigating county councils [17]. Obviously, they differ from our investigation by predating the COVID-19 pandemic, but the study of government agencies offers a useful background. One key finding is that 26 % of the responding government agencies did not verify employee compliance with information security policies (in 2014).

To conclude, we have not found any previous study of cybersecurity in Swedish government administrative authorities in the context of the COVID-19 pandemic. Thus, our study makes a novel contribution.

III. Method

In this study we conduct a census of a subset of Swedish government agencies, the administrative authorities, and their cybersecurity in the context of the COVID-19 pandemic. Statistics Sweden[1] are tasked to keep a record of all Swedish government agencies and the record of our target population, the Swedish administrative authorities, was downloaded from Statistics Sweden's website[2] on June 1, 2020. The record contained 250 administrative authorities.

A questionnaire (see appendix) was developed to collect data from the population. The questionnaire consisted of three parts with predominantly predetermined response options along with a possibility to add a free-text comment. The first part asked for background information: name of the authority, how cybersecurity work is organized, and how the respondent rated the cybersecurity maturity.

The second part asked COVID-19-specific questions, starting with usefulness of information from specific cybersecurity sources and whether it affected communication to employees during the beginning of the COVID-19 pandemic. The sources were MSB, CERT-SE, Krisinformation.se,[3] the Swedish Security Service, the National Defence Radio Establishment (FRA), FOI, the European Union Agency for Cybersecurity (ENISA), Europol, cybersecurity companies, traditional media, trade press, cybersecurity blogs/podcasts, and informal civil servant contacts. It also asked if the administrative authority had communicated to their employees about specific cyber risks: phishing, invoice fraud, video meetings, unsanctioned cloud collaboration, social engineering, telecommuting, and if their decision to communicate to their employees was affected by specific factors: phishing attempts, attempts at invoice fraud, video meeting incidents, unsanctioned cloud collaboration, social engineering, non-compliant telecommuting, network traffic changes, and/or previous crisis experience. For Part 2 we also provided free-text fields for the administrative authorities to be able to fill out possible other sources of information, risks, or factors not mentioned among the given response options. In Part 3 we asked if the administrative authority would be willing to participate in future research on cyber situation awareness.

The questionnaire was distributed as a standard web form. The form did not have unique respondent links or password protection. An email with an invitation to complete

[1] https://www.scb.se/.

[2] http://www.myndighetsregistret.scb.se/Myndighet.

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

the questionnaire was sent to all administrative authorities with an official email listed in the Statistics Sweden record. Of the 250 administrative authorities on record, 236 had an official email address listed. As a majority of the emails listed pointed to the registrar of the administrative authority, we asked that the questionnaire should be forwarded to a member of staff with insight into the administrative authority's work on cybersecurity. The initial invitation was sent on June 6, 2020. Three of the emails could not be delivered, leaving 233 administrative authorities. A first reminder was sent to non-responding administrative authorities on June 22, 2020, and a second reminder on June 30, 2020. The questionnaire was closed on August 1, 2020.

When the data collection was closed, a spreadsheet file containing the data was downloaded and the data was subsequently aggregated and analyzed. For additional information, the administrative authorities were then manually matched to their respective ministries as listed by the Government Offices.[4]

IV. Results

We received 174 responses to our request. 134 administrative authorities responded to the questionnaire, of which 130 were questionnaires filled out on the web and four were questionnaires submitted via email. 25 administrative authorities emailed and referred to their host authorities and 15 declined to participate, citing, e.g., work load or security concerns. Of the 25 administrative authorities referring to host authorities, 11 had host authorities having responded to the questionnaire, 7 had host authorities not among the administrative authorities, 4 had host authorities which did not respond to the questionnaire, and 3 had host authorities which declined to participate. The results presented below are based on the responses from the 134 administrative authorities who provided a completed questionnaire. It should be noted, however, that these 134 responses represent 145 administrative authorities, including the 11 that are hosted by other administrative authorities providing a response, giving a coverage of 58 %.

In the first part of the questionnaire, we gathered background data on the administrative authority: how they organize their cybersecurity work, and how they self-assess their cybersecurity maturity level.

Regarding the organization of cybersecurity, 13 % of respondents report that they have a department working with cybersecurity, 28 % report having one or more dedicated staff members working with cybersecurity, 48 % report having a staff member with cybersecurity as one of his/her tasks, and 10 % report having outsourced cybersecurity. Table I provides an overview of the organization of cybersecurity at the respondents.

The self-assessed maturity level shows that 64 % of the administrative authorities self-assess as not yet having implemented systematic cybersecurity work. Table II presents the self-assessed maturity level of the administrative authorities.

[4]https://www.regeringen.se/.

TABLE I
Organization of cybersecurity at Swedish administrative authorities.

Organizational form	N	%
Cybersecurity department	18	13
≥ 1 dedicated staff	38	28
< 1 dedicated staff	64	48
Outsourced cybersecurity	14	10
Total	134	99

TABLE II
Self-assessed cybersecurity maturity level at Swedish administrative authorities.

Maturity level	N	%
Initiated cybersecurity work	54	40
Documented cybersecurity work	32	24
Implemented systematic cybersecurity work	32	24
Evaluated systematic cybersecurity work	12	9
Optimized systematic cybersecurity work	4	3
Total	134	100

We received responses from administrative authorities covering all eleven Swedish ministries as well as the Prime Minister's office. A majority of the respondents (56 %) belong to three ministries, viz. the Ministry of Education and Research, the Ministry of Finance, and the Ministry of Culture. It should be noted that Swedish public universities and university colleges are administrative authorities belonging to the Ministry of Education and Research. Fig. 1 shows the distribution of the responding administrative authorities with regard to ministries.

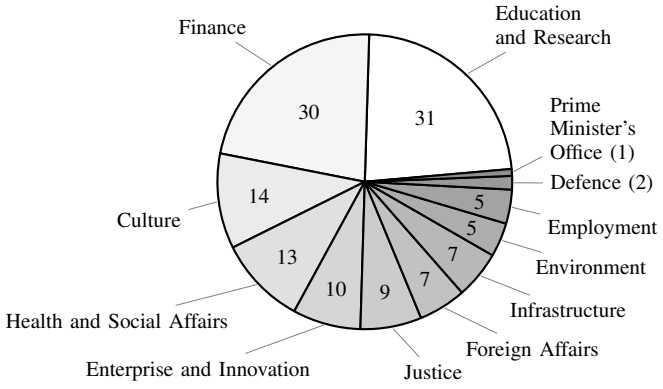

Fig. 1. Distribution of the 134 responding administrative authorities across ministries.

COVID-19-specific data was gathered in Part 2 of the questionnaire. As shown in Fig. 2, when asked about the usefulness of information from specific sources, most respondents, 89 %, found information from MSB to be useful, and for 31 % the information from MSB also influenced communication to employees. Most influential on communication, 39 %, were informal contacts with civil servants at other government agencies, which 83 % of respondents found useful. Other sources

mentioned in the free-text field were, among others, the Public Health Agency, mentioned by 6 administrative authorities, vendors, social media, and sector-specific networks. Fig. 2 presents a more detailed breakdown of the responses into: very useful and influenced communications, very useful, somewhat useful and influenced communications, somewhat useful, and not useful.

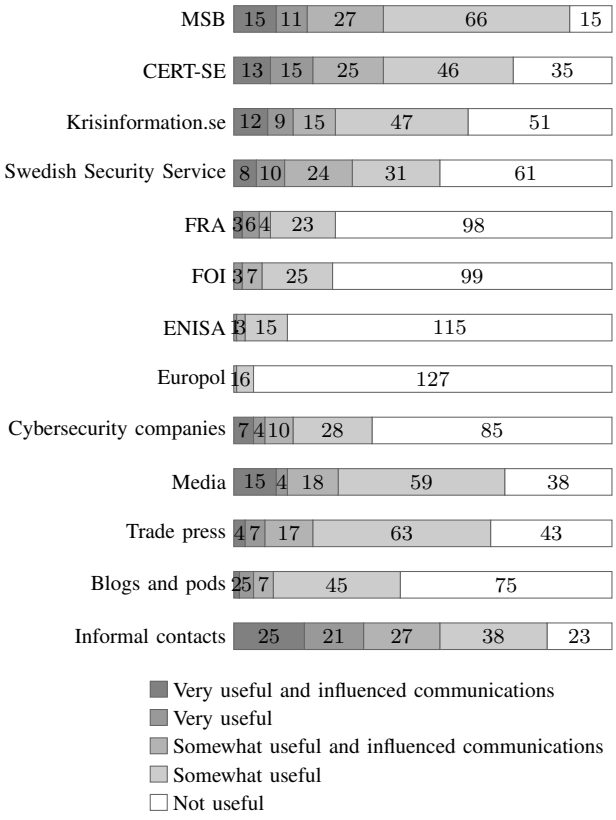

Fig. 2. Usefulness of different information sources on the administrative authorities' work on cybersecurity during the COVID-19 pandemic.

Concerning the question about communication to employees to stay vigilant about specific cybersecurity risks, 90 % of respondents have communicated about risks in connection with video meetings, 87 % about telecommuting, 74 % about phishing, 68 % about unsanctioned cloud collaboration, 52 % about invoice fraud, and 47 % about social engineering. Fig. 3 provides an overview of the risks communicated by the respondents. Other risks communicated to employees include public WiFi, disinformation, installing security updates, social media, and family members using government equipment.

As depicted in Fig. 4, little more than half of the respondents (54 %) reported that others' reporting and/or own observation of incidents at video meetings influenced the decision to communicate to employees. About half of the respondents (54 %) reported that others' reporting and/or own observation of phishing attempts influenced the decision to communicate to employees. Nearly half of the respondents (48 %) reported that previous experience of crisis situations, others' and/or own, influenced the decision to communicate to employees.

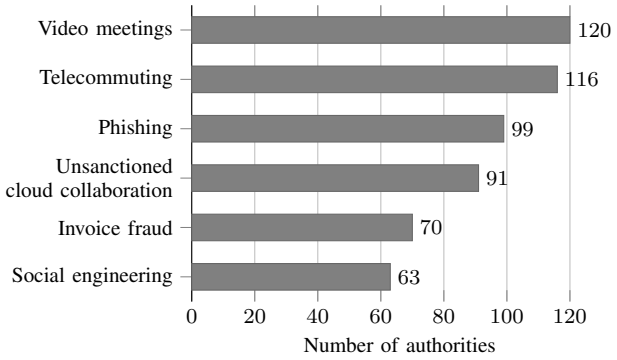

Fig. 3. Swedish administrative authorities' communication to employees about specific cyber risks during the COVID-19 pandemic.

40 % of respondents reported that others' reporting and/or own observation of telecommuting that did not comply with the authority's policy influenced the decision to communicate. 38 % of respondents reported that cooperation in unsanctioned cloud services, either others' reports and/or own observation of said factor, influenced the decision to communicate to employees. Roughly one third (34 %) of respondents reported that others' reports and/or own observation of attempts at invoice fraud influenced the decision to communicate to employees. 33 % of respondents responded that others' reports and/or own observation of changes in network traffic influenced the decision to communicate to employees. Finally, 32 % of respondents reported that others' reports and/or own observation of social engineering influenced the decision to communicate to employees.

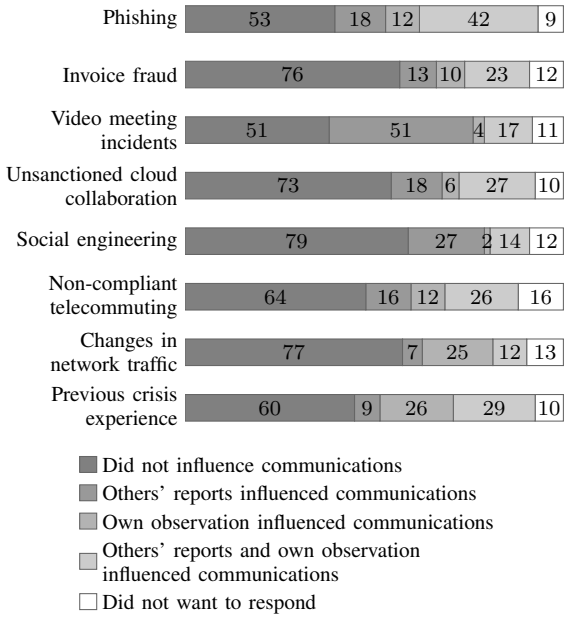

Fig. 4. Factors influencing Swedish administrative authorities' decision to communicate to employees during the COVID-19 pandemic.

V. Discussion

Looking at how the administrative authorities organize their cybersecurity work, 58 % have either outsourced cybersecurity completely or assigned it as one out of several tasks to a single staff member (see Table I). It is natural to interpret this as a relatively low prioritization of cybersecurity work. This interpretation is strengthened by the fact that 38 % of those leading cybersecurity work at Swedish government agencies claimed, in 2014, to lack competencies, resources, or mandates to conduct appropriate cybersecurity work [16].

64 % of the administrative authorities have not implemented (but only initiated or documented) their cybersecurity policies (see Table II). Though a crude self-assessed measure, this is also in line with previous findings: in 2014, 26 % of government agencies did not verify policy compliance, 26 % did not have a chief information security officer or similar, 37 % did not evaluate their information security work at all or only to a very limited extent, and 65 % did not have a continuity plan [16]. Against this background, it is reasonable to conclude that Swedish government administrative authorities in general still have a relatively long way to go in implementing their cybersecurity work. This matters for employee awareness: implementing and following up on the implemented policies would be important to actually be able to reinforce the cybersecurity among the employees who work with and through digital means. It is not uncommon with perception differences between technical IT support staff and ordinary users working in their ordinary offices [18], and during a pandemic, with office work carried out at home, it becomes even harder for the organization to keep control and reinforce specific routines and provide sanctioned means of working. People's personal use of digital means and devices becomes entangled with official duties and means. One way to secure a higher awareness, besides communicating directly and specifically to employees, would be to also provide different forms of tools for tunneling information and to block different forms of tools, devices and protocols from office computers.

Information stemming from MSB was considered to be useful or useful and also influencing communication to employees by 89 % of the administrative authorities. As MSB was given a government assignment to coordinate confirmed information from the government agencies to the public during the COVID-19 pandemic and have also participated in press conferences from the onset of the pandemic, this rating shows that they have been able to reach out. CERT-SE and Krisinformation.se are subsidiaries of MSB, providing thematic information on cybersecurity and crises, respectively. It should be noted that MSB also has ongoing government assignments, unrelated to the pandemic, aimed at improving public sector cybersecurity. MSB shall 1) develop a scale describing the level of the systematic information security work,[5] and 2) educate the public sector to raise the level of public sector information security.[6] Agencies like FRA and FOI, on the other hand, were not rated as especially useful or influencing communication, which could be explained by them not having an assignment to communicate, but rather to gather information that can be distributed by others.

The administrative authorities seem to have well-functioning professional networks, as more than four fifths of the respondents rated the information gathered from informal contacts between civil servants as useful or useful and also influencing communication. One such network mentioned in the free-text field was the ITCF network, a network for IT managers at Swedish universities and university colleges. In the free-text field, the respondents also mentioned the Public Health Agency as providing useful information during the pandemic. The Public Health Agency issued an authority regulation and general advice[7] stating that, wherever possible, all employees should work from home, thus driving the telecommuting.

When communicating about cyber risks at the beginning of the pandemic, the administrative authorities mainly focused on risks associated with the pandemic-driven switch of locale from the main office to the home office. To better understand this communication, it is useful to distinguish between *first-order risks* (such as data leaking through insecure cloud collaboration or video meetings) and *second-order risks* (where data leaked through the first-order risks are used to create potent attacks such as highly realistic invoice fraud).

It is clear from the results (depicted in Fig. 3) that employee communications has focused more on first-order risks such as video meetings (90 %) and telecommuting (87 %), than on second-order risks such as invoice fraud (52 %) or social engineering more generally (47 %). While the first-order risks might be what immediately springs to mind when thinking about the risks associated with working from home, the second-order risks should certainly not be forgotten. Indeed, they may be more important, serving as the means to gain unauthorized access to valuable information through trusted shared government services.

Looking at the most common own observations influencing the administrative authorities' decision to communicate, thus trying to enhance the employees' cyber situation awareness, we have previous crisis experience (41 %) and phishing (40 %). While risks with video meetings were communicated by 90 % of respondents, only 16 % of them report having firsthand experience which influenced communication whereas 38 % were influenced to communicate by others' reports.

The reliability of this study, i.e., whether the results of the study could be reproduced under similar conditions, is good. However, as we are targeting the administrative authority and not the individual, we cannot be certain that all individual employees of a responding administrative authority would provide the same responses. In our request we asked for the questionnaire to be forwarded to someone with insights into the cybersecurity work and it is reasonable to believe that the administrative authority has been able to identify the person/s best suited to respond. The reliability is also good considering

[5]Ministry of Justice record number Ju2019/03058/SSK.

[6]Ministry of Justice record number Ju2019/03057/SSK.

[7]Regulation HSLF-FS 2020:12.

that administrative authorities of all ministries are represented. One threat to reliability is that the link to the questionnaire was "open," meaning that there was no unique link and password for each respondent. Anyone in possession of the link could follow it and complete the questionnaire.

There are also threats to validity, i.e., whether the results accurately depict what was supposed to be measured. Regarding the construction of the questionnaire, there were no definitions provided for different maturity levels for cybersecurity, so the results should be interpreted in light of this. Also, there could be differences in how the respondents interpret "own observation," e.g., whether it is interpreted as an actual event having occurred or if it is interpreted as a period of time during which observation activity occurs. This question of interpretation is the main threat to the validity of this study. For most questions and alternatives, however, interpretations seem relatively straightforward and unambiguous.

VI. Conclusions

This paper presents a first attempt to understand an organization's urgent, and in many ways emergent, ways to manage cybersecurity issues in a time which did not allow for reflection and proactive assessments and actions. Most organizations were befuddled into a situation where employees had to work from home during the pandemic. Quickly, government agencies had to adapt to an unforeseen situation and face a situation where the organization is threatened by technologies beyond their control.

Communication based on reliable sources and spreading awareness to employees about different security risks when using the office computer at home became a way to manage a distributed organization. It seems that most administrative authorities in this study have some awareness of the security risks, and are able to handle urgent threats. However, policies might not be enough to handle distributed cyber situation awareness. On the one hand, it is somewhat disconcerting that 64 % of administrative authorities have not yet reached the implemented level. On the other hand, it is encouraging that MSB has been given government assignments to educate the public sector in cybersecurity and to develop a cybersecurity maturity level measurement instrument.

As outlined in Section I, the paper addresses three research questions:

1) To what degree did Swedish administrative authorities find cybersecurity information resources useful at the beginning of the COVID-19 pandemic?

We find that most respondents, 89 %, found information from MSB to be useful, and for 31 % of the administrative authorities the information also influenced the communication to employees. Most influential on communication, 39 %, were informal contacts with civil servants at other government agencies, which 83 % of respondents found useful. It follows that information from an agency with a government assignment to communicate on COVID-19 issues along with inter-agency informal contacts were important, whereas information from sources without a direct assignment to communicate were not considered as useful.

2) How many Swedish administrative authorities have communicated to their employees about specific cybersecurity risks at the beginning of the COVID-19 pandemic?

The results show that 90 % of respondents have communicated about risks in connection with video meetings, 87 % about telecommuting, 74 % about phishing, 68 % about unsanctioned cloud collaboration, 52 % about invoice fraud, and 47 % about social engineering, thus having a strong focus on first-order risks.

3) What factors influenced Swedish administrative authorities to communicate to their employees about cybersecurity at the beginning of the COVID-19 pandemic?

The most common own observations influencing the administrative authorities' decision to communicate, thus trying to enhance the employees' cyber situation awareness, we find to be previous crisis experience (41 %) and phishing (40 %). While risks with video meetings were communicated by 90 % of respondents, only 16 % of them report having firsthand experience which influenced communication whereas 38 % were influenced to communicate by others' reports.

This investigation opens up for future follow-up interview studies with experts at the administrative authorities acting as respondents in this study. In such studies, we would seek to understand the needs, knowledge, and proactive actions that different decision-makers at different echelons consider, how they act to build appropriate awareness, and also how they subsequently act upon such understanding. Research following this line of inquiry would form an important step towards understanding how cyber situation awareness evolves in an organization.

Acknowledgments

This study was supported by the Swedish Armed Forces.

Appendix: Questionnaire

(Translated from Swedish.)

1. About the authority

1.1. Authority

1.2. How is the authority's cybersecurity work organized?
The following response options were available: the authority has a cybersecurity department / the authority has at least one dedicated staff member responsible for cybersecurity / the authority has one staff member who has cybersecurity as one of their tasks / the authority has outsourced cybersecurity.

1.3. The authority'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 authority'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 administrative authorities at the civil servant level
- Other source [free text]

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

2.2. Has the administrative authority 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 in 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 authority's staff been affected by the following factors?

- Phishing attempts
- Attempts at invoice fraud
- Incidents at video meetings
- Cooperation in unsanctioned cloud services
- Social engineering
- Telecommuting that does not comply with the authority'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 authority for a follow-up interview?

REFERENCES

[1] OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris, France: OECD Publishing, 2015.

[2] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Security & Privacy*, vol. 7, no. 4, pp. 61–64, 2009.

[3] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[4] M. R. Endsley, "Situation awareness global assessment technique (SAGAT)," in *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference (NAECON 1988)*, vol. 3. Piscataway, NJ: IEEE, 1988, pp. 789–795.

[5] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

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

[7] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015.

[8] K. Xu, F. Wang, and X. Jia, "Secure the Internet, one home at a time," *Security and Communication Networks*, vol. 9, no. 16, pp. 3821–3832, 2016.

[9] T.-S. Chou, "Security threats on cloud computing vulnerabilities," *International Journal of Computer Science & Information Technology*, vol. 5, no. 3, pp. 79–88, 2013.

[10] 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.

[11] 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

[12] 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.

[13] 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

[14] D. Lindahl, B. Liljedahl, and A. Waleij, "Cyberattacks in the healthcare sector during the first three months of the Covid-19 pandemic," Swedish Defence Research Agency, Stockholm, Sweden, FOI Memo 7062, 2020.

[15] 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.

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

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

[18] M. A. Tariq, J. Brynielsson, and H. Artman, "The security awareness paradox: A case study," in *Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*. Piscataway, NJ: IEEE, 2014, pp. 704–711.