




The Cost of Incidents in Essential Services—Data from Swedish NIS Reporting

Ulrik Franke^{1,2}(✉) , Johan Turell³, and Ivar Johansson³

¹ RISE Research Institutes of Sweden, SE-164 29 Kista, Sweden
`ulrik.franke@ri.se`

² KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

³ MSB Swedish Civil Contingencies Agency, SE-651 81 Karlstad, Sweden
`{johan.turell, ivar.johansson}@msb.se`

Abstract. The NIS Directive aims to increase the overall level of cyber security in the EU and establishes a mandatory reporting regime for operators of essential services and digital service providers. While this reporting has attracted much attention, both in society at large and in the scientific community, the non-public nature of reports has led to a lack of empirically based research. This paper uses the unique set of all the mandatory NIS reports in Sweden in 2020 to shed light on incident costs. The costs reported exhibit large variability and skewed distributions, where a single or a few higher values push the average upwards. Numerical values are in the range of tens to hundreds of kSEK per incident. The most common incident causes are malfunctions and mistakes, whereas attacks are rare. No operators funded their incident costs using loans or insurance. Even though the reporting is mandated by law, operator cost estimates are incomplete and sometimes difficult to interpret, calling for additional assistance and training of operators to make the data more useful.

Keywords: NIS Directive · Reporting · Incident cost · Cyber security economics · Cyber insurance

1 Introduction

Modern society depends on essential digital services for a wide range of activities. Whether we buy goods and services using payment systems, commute to work, need healthcare, or just want to relax with a glass of drinking water in the light of a lamp, these activities require dependable networks and information systems. With poor cyber security, society is vulnerable, both to accidents and to attacks.

The NIS Directive is a piece of EU-wide legislation aiming to increase the overall level of cyber security in the union [23]. More precisely, the directive focuses on disruptions (most often, but not exclusively, loss of service) at operators of essential services and digital service providers. Under the directive, all

This research was funded by the Swedish Civil Contingencies Agency (MSB).

© The Author(s) 2021

D. Percia David et al. (Eds.): CRITIS 2021, LNCS 13139, pp. 116–129, 2021.

https://doi.org/10.1007/978-3-030-93200-8_7

member states had to establish national CSIRT units, cooperating with each other, to whom operators of essential services [23, Art. 14] and digital service providers [23, Art. 16] must report any incidents. Failure to file reports will result in penalties. As opposed to the GDPR, which is a single regulation applying equally throughout the union, the NIS Directive is a directive, which is implemented differently in each country.

The mandatory reporting scheme of the NIS Directive has attracted much attention, both in society at large and in the scientific community. An important reason for this is that although it is generally agreed that the (prospective) costs of the kind of service interruptions covered by the NIS Directive are considerable (see e.g. [20]), there is also a lack of reliable and credible statistics on such incident costs (see [1, 9] for discussions of some of the methodological challenges).

This lack of data is unfortunate, because *asymmetric information* has been identified as an important explanation for cyber security failures in the literature on the economics of cyber security [2, p. 612]. In the absence of data about incidents and their costs it is difficult to make decisions improving security, such as switching from less secure to more secure vendors in procurement, investing in the best security measures, removing single points of failure, or passing effective laws.

It is against this background that this paper uses previously non-public data from Swedish NIS reporting to shed light on incident costs, thus making a unique and timely contribution. More precisely, the following research questions are investigated:

- RQ1:** How much do incidents in Swedish essential services, as defined in the NIS Directive, cost?
- RQ2:** How do the operators of Swedish essential services, as defined in the NIS Directive, fund their incident costs?
- RQ3:** What are the causes behind incidents in Swedish essential services, as defined in the NIS Directive?
- RQ4:** How can reporting be improved to raise quality?

The remainder of this paper is structured as follows: The next section describes some related work on the NIS Directive. Section 3 explains the method used before Sect. 4 describes the results. The costs found and other observations made are discussed in Sect. 5, before Sect. 6 concludes the paper.

2 Related Work

The NIS Directive is attracting scholarly attention. The literature includes both overarching considerations on cyber security regulation and governance [5, 22, 26] and country-specific case studies (e.g., on the NIS implementation in Greece [21] and the UK [27], the interplay between the NIS Directive and the Danish national strategy for cyber and information security [18], and the impact of the NIS Directive on cyber insurance in Norway [3]). However, to the best of our knowledge, there are no published empirical studies based on incident reporting.

This is not surprising, given the fact that the incident reports are, typically, not available for research.

As for disruption and outage incident costs more generally, a recent systematization of knowledge on quantification of cyber risk finds surprisingly few studies on outage costs [28]. One source of cost data is operational risk databases in banking (e.g. [4, 15, 16, 25]), but these databases include incidents caused by many kinds of operational risks besides outages. One study dedicated to costs of service outages reports data from the transportation, food, and government sectors in Sweden [13], but these are a non-random sample of case-studies.

To conclude, it is evident that the NIS Directive is interesting to study, but that the relatively short time-span since its implementation and the non-public nature of the mandatory reporting has led to a lack of empirically based research. Thus, the present paper makes a unique contribution to the literature.

3 Method

In general, NIS reports are not publicly available, neither to researchers nor to the public at large. Even though Sweden has a long tradition of government transparency¹ including the world's oldest freedom of information law [19], this is the case in Sweden as well: access to NIS reports is restricted to prevent crime.

However, the fact that the NIS reports, *in full*, are classified as secret does not mean that *parts* of them, or *aggregated information* from them, cannot be made publicly available. This constitutes the basis for the method used to investigate the research questions listed in Sect. 1.

The second and third authors, employed at the Swedish Civil Contingencies Agency (MSB), have access to the NIS incident reports in their professional capacities. The aggregated data used in this paper was produced in a three-step process: (i) The second and third authors compiled data from NIS reports. (ii) The second and third authors assessed whether the resulting aggregate (descriptive statistics as shown in Sect. 4) could be released or had to remain secret. (iii) The aggregate data thus vetted was made available to the first author as well. (It should be noted, however, that under the Swedish freedom of information law, *anyone* could ask for the data, have it vetted, and released to the extent possible.)

The data set thus released and analyzed consists of all the Swedish NIS reports from 2020 (the first full year with available reports); a total of 88 mandatory reports, following incidents at service providers covered by the NIS Directive.

Out of the 88 reports, 34 contained cost information pertaining to (i) the cost of the incident, (ii) the cost of the resulting disruption, or (iii) the cost of preventive actions taken. The vast majority of these 34 reports emanate either

¹ Public access to official documents is enshrined in the Freedom of the Press Act: “To encourage the free exchange of opinion and availability of comprehensive information, every Swedish citizen shall be entitled to have free access to official documents.” (Chapter 2, Article 1).

from (i) health and medical services, or from (ii) drinking water supply services. (This is also the case for the full set of 88 reports; the cost subset is representative in this respect.) This also means that most respondents are from the public sector, which manages much of health and medical services and almost all drinking water plants in Sweden.

Three additional caveats concerning the method should be mentioned: First, even though the reports all come from mandatory reporting, this does not mean that all reports are complete in the sense that every piece of information asked for has been provided. The 34 reports considered all include *at least one* cost estimate, but many of them exhibit considerable ‘holes’ in the data supplied, as will be evident in the next section. The most common cost estimate supplied was the *lowest possible cost* of incident, disruption, and preventive actions taken, respectively.

Second, incidents under the NIS Directive are first and foremost *availability* incidents (i.e. disruptions of one sort or another), not confidentiality or integrity incidents. In practice, the reported incidents have integrity consequences every now and then, whereas confidentiality aspects are almost completely absent.

Third, the confidential nature of the data and the division of labor between the authors means that even though the results reported in Sect. 4 are intended to be self-contained and interesting in their own right, part of the discussion in Sect. 5 is also informed by additional trends or details from the reports that cannot be disclosed.

4 Results

As part of the mandatory reporting, operators were asked to give a number of cost estimates. These results are reported in the following.

Giving estimates, operators could mark their numbers as being certain or not certain. In the following diagrams, visualizations that are based only on numbers that are *certain* are circumscribed with a solid line (\square), visualizations that are based only on numbers that are *not certain* are not circumscribed (\blacksquare), and visualizations that are based *both* on numbers that are certain and on numbers that are not certain are circumscribed with a dotted line ($\square\blacksquare$). Thus, in set notation, $\square \cap \blacksquare = \emptyset$ and $\square \cup \blacksquare = \square\blacksquare$.

4.1 Costs Entailed by Incidents

Operators’ estimates for the three kinds of cost are shown in Fig. 1. As in the NIS reporting forms, the numbers are given in SEK. (10 SEK is roughly one euro or one US dollar.)

A few immediate observations can be made from Fig. 1. First, medians are typically much smaller than averages (arithmetic means), typical for a skewed distribution, where most cost estimates are relatively small, but a single or a few higher values push the average upwards. This is a well-known phenomenon in cyber incident surveys [1, 9].

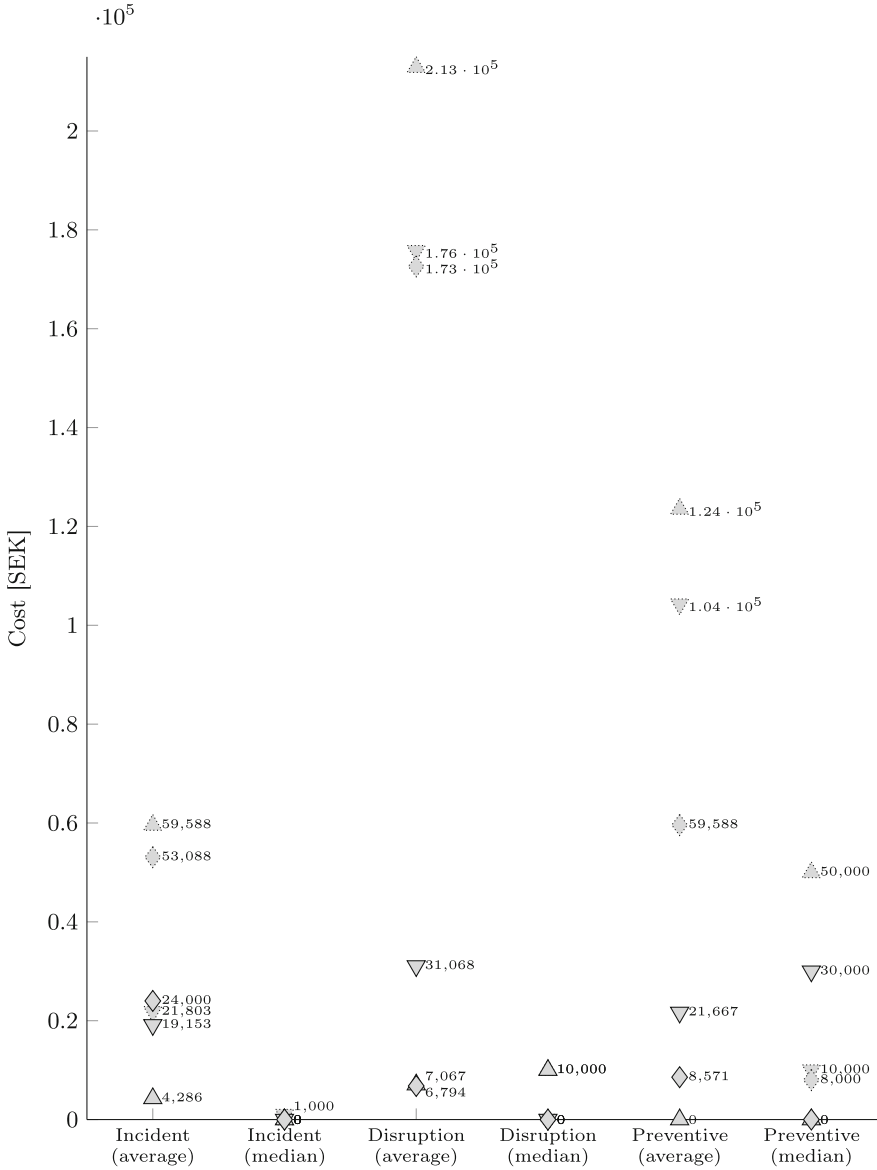


Fig. 1. Operators' estimated costs. Upwards triangles indicate highest possible cost; downwards triangles indicate lowest possible cost; diamonds indicate probable cost. Markers that are circumscribed with a solid line (□) indicate that the estimates being aggregated were marked as certain by the operators; markers that are circumscribed with a dotted line (⊞) indicate that the estimates being aggregated include *both* certain and not certain estimates.

Second, the values of highest possible, lowest possible, and most probable costs often seem counterintuitive. For example, for the certain incident costs, both the average and the median of the highest possible cost is smaller than the average and the median, respectively, of the lowest possible and most probable cost. The reason is incomplete data. The estimates being aggregated to form a highest possible cost do not come from (exactly) the same set of operators as the estimates being aggregated to form a lowest possible or most probable costs. In fact, while the operators are supposed to fill out all three (highest possible, lowest possible, and most probable costs), many have only filled out one of them.

Third, the average values based on both certain and uncertain estimates are higher than average values based on certain estimates only. This is particularly evident for the disruption costs, though the tendency is clear also for the incident and preventive costs.

Fourth, the numerical values of costs—while exhibiting large variability—are in the range of tens to hundreds of kSEK per incident. If the annual number of incident at any one operator is reasonably small, this cost range is roughly in line with previous results about annual outage costs in Swedish enterprises [13, Table 1].

4.2 Funding of Costs Entailed by Incidents

Operators were also asked how costs were funded. Responses on funding of the cost of *incidents* are given in Fig. 2. Responding to this question, operators could allocate the cost over six funding sources indicated (including an ‘other’ option), subject to the constraint that the total cost summed to 100%.

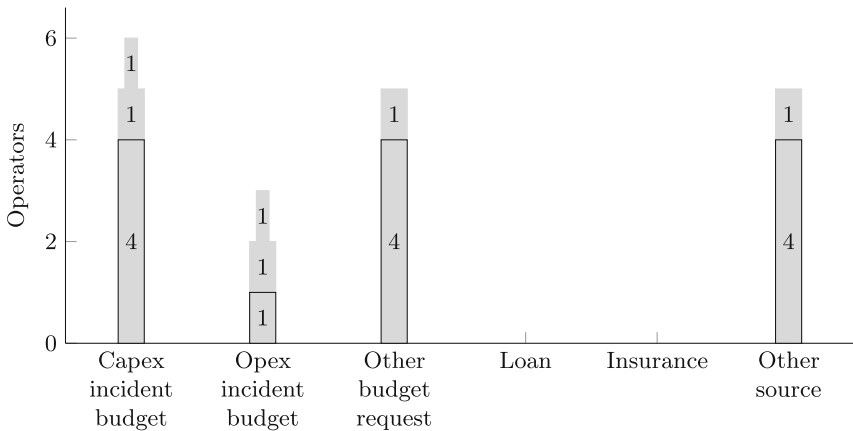


Fig. 2. Operators’ funding of *incident* costs. Budget allocations that are circumscribed with a solid line (◻) were marked as certain by the operators; budget allocations that are not circumscribed (◼) were marked as not certain. 100% allocations have full width; 50% allocations have half width. $N = 33$

For example, the leftmost bar in Fig. 2 shows the number of operators who took the incident cost from a capex incident budget.² There were four operators who certainly took 100% of costs from there, one operator who probably, but not certainly, took 100% of costs from there, and one operator who probably, but not certainly, took 50% of costs from there.

As seen in the figure, no operator used loans or insurance to cover costs. Furthermore, it should be noted that out of 34 operators, only 18 (5.5 capex + 2.5 opex + 5 other budget + 0 loans + 0 insurance + 5 other) have allocated their total cost over the six funding sources given in the question. Only 1 operator did not answer (thus $N = 33$). The remaining 15 *did* answer, but *did not* allocate 100% of costs over the funding sources. This may appear strange, but can be explained by the observation that many of those who incurred a zero cost (understandably) did not bother to distribute this zero cost over different sources.

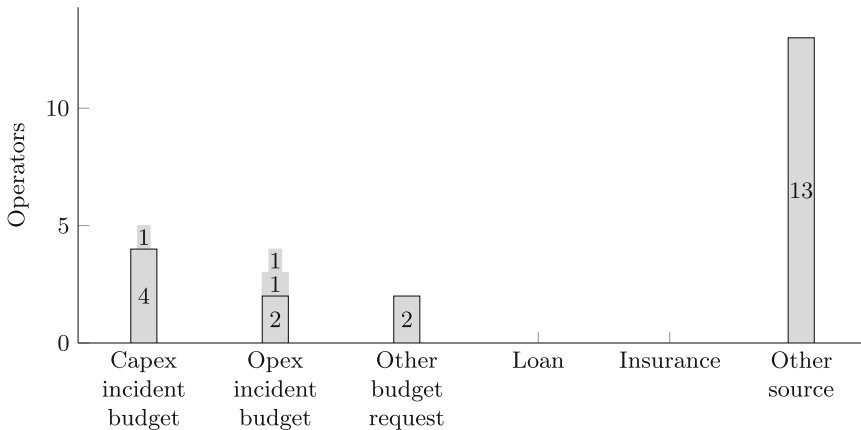


Fig. 3. Operators' funding of *disruption* costs. Budget allocations that are circumscribed with a solid line (◻) were marked as certain by the operators; budget allocations that are not circumscribed (◼) were marked as not certain. 100% allocations have full width; 50% allocations have half width. $N = 30$

Responses on funding of the cost of *disruptions* are given in Fig. 3. As before, operators allocated the cost over six funding sources, assigning percentages, and indicating certainty.

Again, no operator used loans or insurance to cover costs.

² Capital expenses (capex) are one-time costs incurred when buying an asset. Operating expenses (opex) are recurring costs that are incurred for as long as an asset is used.

4.3 Causes of Incidents

The NIS reporting forms also include an assessment of the cause of the incident reported, as shown in Fig. 4.

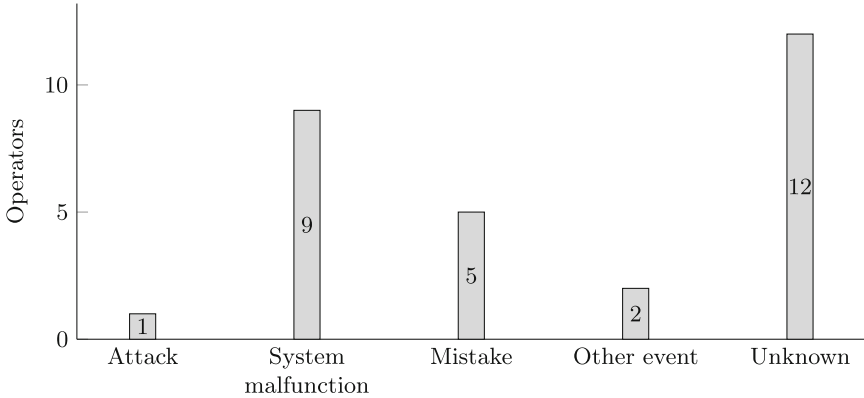


Fig. 4. Causes of incidents. 5 operators did not answer according to the instructions in the form, either by not giving any cause (1) or by giving combinations of two causes (4), resulting in $N = 29$.

Perhaps the most striking feature of Fig. 4 is the large number of unknown causes: between a third and half of reporting operators do not know the causes of the incidents they report. It is also noteworthy that while attacks receive much attention in the media and elsewhere, attacks are not identified as being behind a significant portion of NIS incidents. In this respect, the NIS reports differ considerably from a recent investigation of Swedish manufacturing firms, where 7% of the 649 respondents reported that they had experienced interruptions from intentional attacks in the past 12 months, and 7% reported interruptions from unintentional incidents in the same period [14, Fig. 3].

5 Discussion

In the following, the results from the previous section are discussed from a few different perspectives.

5.1 Characteristics of Operators Incurring High Cost

As mentioned in Sect. 3, the most common cost estimate supplied by the operators was the *lowest possible cost* of incident, disruption, and preventive actions taken, respectively. (Thus, in Fig. 1, the markers representing the most data points are the downwards triangles.)

Considering the *top five* lowest possible *incident* costs, these operators are *not* from any particular sector (such as healthcare). However, what they do have in common is that they have all identified vulnerabilities (in a broad sense, not necessarily particular CVEs) which, had they been addressed before the incident, could have prevented it or at least limited its consequences. In all of these cases, the operators report that they have identified significant preventive measures that they are about to implement, are in the process of implementing, or have already implemented.

Considering the *top five* lowest possible *disruption* costs, four out of five operators are from health and medical services. Again, most of these operators identified vulnerabilities which, had they been addressed before the incident, could have prevented it or at least limited its consequences. When (the lowest possible) preventive costs have been assessed, they are in the 50,000–250,000 and 400,000–450,000 SEK ranges.

Considering the *top five* lowest possible *preventive* costs, these operators are *not* from any particular sector. All but one of these operators identified vulnerabilities which, had they been addressed before the incident, could have prevented it or at least limited its consequences.

A general observation is that the operators incurring the highest costs for the incident and the disruption, respectively, are operators whose information technology infrastructure does not conform to best practices. For example, the equipment used is old and basic security such as network segmentation, backups, traffic monitoring, etc. are not in place. These technical solutions give the impression that the IT environment for the essential service was set up about a decade ago but has not been maintained since. Thus, once incidents occur, the costs of maintenance and upgrades, previously postponed, suddenly catch up with the operator.

Most of these operators report incidents in *their own infrastructures*. This can be contrasted with the fact that out of the 88 NIS reports received in 2020, 68% (60 reports) concerned incidents occurring in the infrastructure of an external vendor used by the operator. Thus, there is a tendency that while most incidents occur in the infrastructure of external vendors, the *most costly* incidents occur in the infrastructure of the operators themselves. A possible explanation is that, in the two sectors mostly represented in the reporting, incidents in the operators' own infrastructure often entail tangible extra costs for additional manual labor, e.g., using more physicians and nurses to administer appropriate treatment and care despite medical records being unavailable, or sending personnel to inspect water purification on site.

5.2 Cyber Insurance

As seen in Figs. 2 and 3, no operator used insurance to cover costs. From one perspective, this is a bit surprising: Sweden has a relatively high cyber insurance adoption rate. In absolute numbers, it is known that at least some 110,000 Swedish enterprises have cyber insurance [12, p. 24], and a recent survey of cyber

security practices of Swedish manufacturing firms indicated that some 30% of companies has cyber insurance [14, Fig. 6].

However, high cyber insurance coverage in manufacturing, or private sector at-large, does not necessarily mean that the, mostly public, operators of essential infrastructure are among the insured. One explanation could thus be that public sector enterprises do not typically have cyber insurance policies. Another explanation could be that the interruptions fall short of the waiting periods, typically some 24, 36, 48, or 72 h, during which no indemnity is paid [10]. A third explanation could be that even though an enterprise has a cyber insurance policy, not all business interruptions are necessarily covered [11]. (The converse is also true; it might be that an insurance policy *not* designed to cover cyber incidents might still unintentionally do so; a phenomenon of great concern to insurers, known as *silent cyber coverage* [29].)

5.3 Validity and Reliability

The validity of the findings is good: All the reports are based on actual incidents entailing actual costs for the operators, and the cost estimates had to be produced within four weeks after the incidents, meaning that circumstances were fresh in the memory of respondents. From this perspective, validity is better than, for instance, if cost estimates had been based on annual summaries collected *ex post* (as in, e.g., [13]), or based on fictitious scenario estimates (as in, e.g., [20]).

Reliability, on the other hand, is threatened by the difficulty to correctly assess costs. It is very probable that different operators have used different ways to assess costs. This is also reflected in the incompleteness and relative difficulty of interpretation of some of the results reported in Sect. 4 (such as the large number of ‘other’ responses illustrated in Figs. 2 and 3). Clearly, figures must be interpreted with some caution in light of this.

In contrast, reliability is strengthened by the fact that ideally, there should be no *sampling bias* at all: indeed, this is not a sample but a *census* of incidents, since all operators are required by law to report. This is a considerable strength, that in theory goes a long way towards rectifying the well-known problems of bias and incomplete data in cyber incident surveys [1, 9]. Nevertheless, the results reported in Sect. 4 also illustrate some practical limits to this argument: even though operators are forced to report incidents, it is more difficult to force quality in the reporting.

One possible source of confusion could be that the costs of the incident (such as an outage in the operational technology controlling a water plant) and those of the resulting disruption (such as water needing to be cleaned) might be difficult to distinguish. However, the nature of operations of most respondents in the data set is such that this should not be a problem.

Here, it is also worth reminding that operators could mark estimates as being certain or not certain. Cost estimates marked as certain are often reported when the same error happens over and over again, meaning that the cost is well-known. Examples include recurring incidents in sensor systems run by the operator or in external services run by service providers.

5.4 Generalization to Other Countries

Another aspect of validity and reliability concerns the possibility to generalize results to other countries. On a general level, the NIS Directive is in place throughout the EU, and the Swedish experiences should be relevant to infer tentative conclusions about other countries as well. On a more particular level, however, it is important to bear in mind that the NIS Directive has been implemented in different ways in different countries. Thus, before generalizing to any particular country, it is useful to consult the comparison of implementations compiled by the European Commission [8]. In particular, it is important to bear in mind the distinction between incident cost (as depicted in Fig. 2) and disruption cost (as depicted in Fig. 3) which may not be upheld in reporting from other countries.

Again, it should also be stressed that the NIS definition of incidents may be different from how the ‘cyber incident’ term is used in other contexts. The NIS definition is broader in that it includes incidents regardless of cause, whereas in other contexts it is common to (implicitly or explicitly) focus on attacks only. At the same time, the NIS definition is narrower in its focus on availability only (as opposed to integrity and confidentiality). As a consequence, any comparisons of costs reported in Sect. 4 with costs reported in other studies should be made with care, and assumptions about comparability should be made as explicit as possible.

5.5 Usefulness of Data from NIS Reporting

In conjunction with the discussion of validity and reliability, it is also appropriate to discuss the wider usefulness of the cost data that can be obtained from mandatory NIS reporting. As seen in Sect. 4, results are incomplete and sometimes difficult to interpret. This can be contrasted to some of the prior expectations.

For example, since lack of actuarial data on cyber incidents is a known impediment to the development cyber insurance [4, 6, 24, pp. 94–95], it has been proposed that the mandatory incident reporting regimes of the GDPR and the NIS Directive could create relevant cyber data for insurers [7, 17]. While this idea may indeed have some potential, the data in Sect. 4 clearly illustrates that such data is no panacea.

Even if hurdles relating to security and competition were solved, just making NIS reporting, as-is, available to insurers would not by itself solve the problem of lack of data for cyber insurance. Making the most of the reporting requires additional quality assurance mechanisms. In particular, it seems that in order to make cost estimates from NIS reports more useful, operators might need additional assistance and training in producing such estimates in a reliable and uniform way. With increasing experience of how reporting works in practice, it may also become possible to revise the forms to facilitate better reports, though this should be made with some caution as it makes future longitudinal studies more difficult.

6 Conclusions

Based on data consisting of all the mandatory NIS reports in Sweden in 2020, this paper has investigated economic aspects of the incidents reported. The costs reported exhibit large variability and skewed distributions, where a single or a few higher values push the average upwards. The numerical values are in the range of tens to hundreds of kSEK per incident. Operators were also asked about incident causes. It is noteworthy that the most common incident causes are malfunctions and mistakes, whereas attacks are rare. For many incidents, however, the cause is unknown.

A general observation is that the operators incurring the highest costs have technology infrastructures that do not conform to best practices (e.g., using old equipment lacking basic security).

No operators funded their incident costs using loans or insurance. This is somewhat surprising, since Sweden has a relatively high cyber insurance adoption rate. However, it may be that the cyber insurance coverage is lower among the operators of essential infrastructure.

Apart from the concrete results on incidents costs, the data set also reveals that even though the reporting is mandated by law, operator cost estimates are incomplete and sometimes difficult to interpret. This points towards future work: Operators probably need additional assistance and training in producing cost estimates in a reliable and uniform way, so that the data becomes more useful.

References

1. Anderson, R., et al.: Measuring the cost of cybercrime. In: Böhme, R. (ed.) *The Economics of Information Security and Privacy*, pp. 265–300. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39498-0_12
2. Anderson, R., Moore, T.: The economics of information security. *Science* **314**(5799), 610–613 (2006). <https://doi.org/10.1126/science.1130992>
3. Bahşi, H., Franke, U., Langfeldt Friberg, E.: The cyber-insurance market in Norway. *Inf. Comput. Secur.* **28**(1), 54–670 (2019). <https://doi.org/10.1108/ICS-01-2019-0012>
4. Biener, C., Eling, M., Wirfs, J.H.: Insurability of cyber risk: an empirical analysis. *Geneva Pap. Risk Insur. Issues Pract.* **40**(1), 131–158 (2015). <https://doi.org/10.1057/gpp.2014.19>
5. van Eeten, M.: Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digit. Policy Regul. Gov.* **19**(6), 429–448 (2017). <https://doi.org/10.1108/DPRG-05-2017-0029>
6. EIOPA European Insurance and Occupational Pensions Authority: Cyber risk for insurers—challenges and opportunities (2019). <https://doi.org/10.2854/305969>
7. EIOPA European Insurance and Occupational Pensions Authority: EIOPA strategy on cyber underwriting (2020). <https://doi.org/10.2854/793935>

8. Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems (2019). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0546>. COM(2019) 546
9. Florêncio, D., Herley, C.: Sex, lies and cyber-crime surveys. In: Schneier, B. (ed.) *Economics of Information Security and Privacy III*, pp. 35–53. Springer, New York (2013). https://doi.org/10.1007/978-1-4614-1981-5_3
10. Franke, U.: The cyber insurance market in Sweden. *Comput. Secur.* **68**, 130–144 (2017). <https://doi.org/10.1016/j.cose.2017.04.010>
11. Franke, U.: Cyber insurance against electronic payment service outages. In: Katsikas, S.K., Alcaraz, C. (eds.) *STM 2018*. LNCS, vol. 11091, pp. 73–84. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01141-3_5
12. Franke, U.: Cybersäkerhet för en uppkopplad ekonomi [Cyber security for the online economy]. *Entreprenörskapsforum* (2020). <http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-48918>
13. Franke, U.: IT service outage cost: case study and implications for cyber insurance. *Geneva Pap. Risk Insur. Issues Pract.* **45**(4), 760–784 (2020). <https://doi.org/10.1057/s41288-020-00177-4>
14. Franke, U., Wernberg, J.: A survey of cyber security in the Swedish manufacturing industry. In: *2020 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, June 2020. <https://doi.org/10.1109/CyberSA49311.2020.9139673>
15. Goldstein, J., Chernobai, A., Benaroch, M.: An event study analysis of the economic impact of IT operational risk and its subcategories. *J. Assoc. Inf. Syst.* **12**(9), 1 (2011)
16. Ibrahimovic, S., Franke, U.: A probabilistic approach to IT risk management in the Basel regulatory framework: a case study. *J. Financ. Regul. Compliance* **25**, 176–195 (2016). <https://doi.org/10.1108/JFRC-06-2016-0050>
17. Insurance Europe: Key messages on EIOPA’s cyber underwriting strategy (2020). <https://www.insuranceurope.eu/publications/1718/key-messages-on-eiopa-s-cyber-underwriting-strategy/>. Published June 15, 2020
18. Jensen, M.S.: Sector responsibility or sector task? New cyber strategy occasion for rethinking the Danish Sector Responsibility Principle. *Scand. J. Mil. Stud.* **1**(1), 1–18 (2018)
19. Kassen, M.: Understanding transparency of government from a Nordic perspective: open government and open data movement as a multidimensional collaborative phenomenon in Sweden. *J. Glob. Inf. Technol. Manage.* **20**(4), 236–275 (2017). <https://doi.org/10.1080/1097198X.2017.1388696>
20. Cloud Down: Impacts on the US economy. Technical report, Lloyd’s of London (2018). <https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down>
21. Maglaras, L., Drivas, G., Noou, K., Rallis, S.: NIS directive: the case of Greece. *EAI Endorsed Trans. Secur. Saf.* **4**(14), 154769–154775 (2018)
22. Markopoulou, D., Papakonstantinou, V., de Hert, P.: The new EU cybersecurity framework: the NIS Directive, ENISA’s role and the General Data Protection Regulation. *Comput. Law Secur. Rev.* **35**(6), 105336 (2019). <https://doi.org/10.1016/j.clsr.2019.06.007>

23. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Off. J. Eur. Union L* **194**, 1–30 (2016). <http://data.europa.eu/eli/dir/2016/1148/oj>
24. OECD: Enhancing the Role of Insurance in Cyber Risk Management (2017). <https://doi.org/10.1787/9789264282148-en>
25. Rachev, S.T., Chernobai, A., Menn, C.: Empirical examination of operational loss distributions. In: *Perspectives on Operations Research*, pp. 379–401. Springer, Cham (2006). https://doi.org/10.1007/978-3-8350-9064-4_21
26. Timmers, P.: The European Union’s cybersecurity industrial policy. *J. Cyber Policy* **3**(3), 363–384 (2018). <https://doi.org/10.1080/23738871.2018.1562560>
27. Wallis, T., Johnson, C.: Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. In: *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1–10 (2020). <https://doi.org/10.1109/CyberSA49311.2020.9139641>
28. Woods, D.W., Böhme, R.: SoK: quantifying cyber risk. In: *2021 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos, CA, USA, pp. 211–228. IEEE Computer Society, May 2021. <https://doi.org/10.1109/SP40001.2021.00053>
29. Wrede, D., Stegen, T., von der Schulenburg, J.M.G.: Affirmative and silent cyber coverage in traditional insurance policies: qualitative content analysis of selected insurance products from the German insurance market. *Geneva Pap. Risk Insur. Issues Pract.* **45**(4), 657–689 (2020). <https://doi.org/10.1057/s41288-020-00183-6>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

