Cyber insurance against electronic payment service outages

A document study of terms and conditions from electronic payment service providers and insurance companies

Ulrik Franke^[0000–0003–2017–7914]

RISE SICS – Swedish Institute of Computer Science, SE-164 29 Kista, Sweden
`ulrik.franke@ri.se`

Abstract. Society is becoming increasingly dependent on IT services. One example is the dependence of retailers on electronic payment services. This article investigates the terms and conditions offered by three electronic payment service providers, finding that they only guarantee best effort availability. As potential mitigation, five cyber insurance policies are studied from the perspective of coverage of electronic payment service outages. It is concluded that cyber insurance does indeed give some protection, but that coverage differs between insurers and between different policy options offered. Thus, a retailer who wishes to purchase cyber insurance should take care to understand what is on offer and actively select appropriate coverage.

Keywords: cyber insurance, payment systems, service outages, document study

1 Introduction

In modern society, we are becoming increasingly dependent on IT services. IT brings value by enabling new services, or by making existing ones more efficient. The flip side of this coin is that the consequences of outages and disruptions to these IT services are becoming larger and more difficult to manage.

A relatively new tool for managing these increasing risks is cyber insurance. This tool, as an addition and a complement to the existing cyber security and risk management toolbox, has received much attention in recent years. For example, the EU Agency for Network and Information Security (ENISA) has published a number of reports on the effective use of cyber insurance [7], [8], and the OECD is studying how to make better use of cyber insurance to tackle cyber risk management [16]. When the World Economic Forum presented a “playbook” for public-private collaboration to increase cyber resilience in January 2018, one of the chapters was devoted to cyber insurance [21]. From the practitioner perspective, renowned IT strategy consultancies like Gartner offer advice on how to use cyber insurance effectively [20], and academically, literature reviews are being published [6], [15].

One example of a sector with growing dependence on IT services is the retail sector in its relation to electronic payment service providers. As put by Gartner, “payment functionality must be 24/7” [10]. In this respect, Sweden is an interesting example of a country at the forefront of the transition from cash to electronic payments. From its peak in 2007, the value of Swedish cash in circulation in 2017 has approximately halved [1]. The share of payments initiated electronically (measured by total transaction value) was at 98.3 % in 2015 [2]. Even though at the moment, these trends are at odds with a global average where cash remains important [1], it is reasonable to assume that the future of payments is increasingly electronic, and studying an early adopter country thus makes sense.

Despite best efforts, in reality electronic payment services are not available 24/7. It is easy to find anecdotal media reports of outages in Sweden. In January 2018, payments could not be made with cards issued by the SEB bank for a few hours [19]. In July 2017, 13 000 point-of-sale (POS) terminals all over Sweden were unavailable for a few hours. The electronic payment service provider confirmed that the incident affected all sorts of businesses, and the spokesman is quoted as not being able to recall any outage of this magnitude having occurred before [18]. In August 2017, VISA card payments with some cards issued by the Nordea bank could not be processed [11]. The list goes on. Incidents like these are part of the motivation for the Swedish Civil Contingencies Agency in funding an ongoing research project addressing payment system resilience [13], [12].

Managing outages is one of the areas where cyber insurance can help. Whereas in the US, cyber insurance has traditionally mostly focused on 3rd party liabilities connected with data and privacy breaches, cyber insurance in Europe has to a larger extent addressed the 1st party costs of business interruption [9]. For example, insurer AIG reported in 2015 that while less than 20 % of their cyber insurance customers in the US opt for network interruption coverage, more than 70 % of customers in the EMEA region do [5].

The research presented in this article resides at the intersection of the two trends outlined above: (i) cyber insurance and (ii) electronic payment service resilience. More precisely, the research questions are: (i) What (basic) protection against electronic payment service outages is offered in electronic payment service provider terms and conditions, and (ii) what (additional) protection can cyber insurance offer? These questions are addressed through a document study of terms and conditions from electronic payment service providers and insurance companies active on the Swedish market.

The reminder of this article unfolds as follows. Section 2 briefly describes related work, situating the contribution within the existing literature. Section 3 then outlines the method used, before Section 4 describes the results. Findings are analyzed and discussed in Section 5, before Section 6 concludes the article.

2 Related work

The literature on cyber insurance is relatively abundant. However, until recently, it has been characterized by a lack of empirical studies. In a now slightly dated literature review, Böhme & Schwartz note that the study of cyber insurance has been more concerned with developing theoretical models than with empirical research [4]. In a more recent review, Eling & Schnell conclude that more empirical research is needed, both on the demand and the supply sides [6].

Contents and coverage analysis of cyber insurance policies is an area where some empirical work has been done. A recent and relatively large-scale study was made by Romanosky et al. who analyzed more than 100 cyber insurance policies from the US [17]. The results give an interesting high-level view of cyber insurance, but do not answer specific questions about electronic payment service outages, and is limited to the US. Marotta et al. in their review catalog the coverage of 14 cyber insurance policies offered by the big global actors [15]. It is shown that they all offer some sort of business continuity coverage, but the details of this coverage with respect to, e.g., electronic payment services are not elaborated. Majuca et al. conducted an early study of coverage, which describes the development from hacker insurance policies in the late 1990s to the more mature cyber insurance developed in the next decade [14]. However, this work is now more than a decade old, so it has limited value when assessing the current state of coverage. The same can be said of Baer et al. who show that business interruption was covered by all major insurance companies already in 2007, but gives no further details on electronic payment service outages [3].

To summarize, no existing work in the literature seems to offer a detailed analysis of how insurance policy coverage relates to terms of service offered in a concrete application domain such as electronic payment services. Thus, this article makes a contribution to the empirical cyber insurance literature, an area that has been identified as underdeveloped.

3 Method

The relevance of the research questions was first exploratively discussed with the Swedish Trade Federation. The Swedish Trade Federation also provided the terms and conditions of two major electronic payment service providers active on the Swedish market; Verifone and Nets. Verifone is one of the big global actors in payments services. In Sweden, they connect more than 26 million POS terminals to the cloud.¹ Nets is a regional actor in payments services, focusing on the Nordic and Baltic region, where more than 300 000 retailers used their services in 2016.² As these documents are also publicly available, these service providers are not anonymized.

¹ <https://www.verifone.com/sv/se/om-verifone-sweden>, accessed March 9, 2018.

² <https://investor.nets.eu/nets-as-an-investment>, accessed March 9, 2018.

As a complement to the traditional electronic payment service providers, the terms and conditions of challenger payments provider iZettle were also analyzed.³ The iZettle Reader is plugged into a smart phone or tablet, creating a POS system that accepts not only (i) traditional card payments, but also (ii) contactless payments with cards or services like Apple Pay or Android Pay, and (iii) mobile payments such as the Swedish Swish service, which is based directly on bank accounts and circumvents the card infrastructure. Thus, even though when iZettle was founded in 2010, it built on the card system, it has now expanded into the cardless payments market. Arvidsson identifies iZettle as one of the causes behind the reduction in cash payments in Sweden [2], and this, together with its expansion into cardless payments, and its marketing tagline “never lose a sale” makes it a suitable complementary object of study.

Five cyber insurance policies were obtained from insurance companies active on the Swedish cyber insurance market as part of another study [9]. As these policy documents were obtained in confidence, and are not always publicly available, the insurance companies are anonymized throughout the study. More detailed anonymized information about the coverages they offer, their underwriting processes, and their typical annual premiums can be found in the previous study [9]. Additionally, non-binding recommendations by the German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, GDV) on general terms and conditions for cyber risk insurance were studied, as a sixth example of a cyber insurance policy. These recommendations are also publicly available.

All three sets of service provider terms and conditions were in Swedish, whereas four of the cyber insurance policies were in English with just a single Swedish language policy. The GDV recommendations were read in an English version, though the GDV makes it clear that this is for informational purposes only and that the German version shall prevail.

Regarding language and terminology, as pointed out by one of the reviewers, it would be good to be able to offer the reader a table of standard terms so as to better understand the contribution given in the next section. Unfortunately, there is no such standard terminology in place. Indeed, previous research shows that ambiguity about cyber insurance coverage is common [9], [6] and the OECD identifies this as an important impediment on the demand-side of the cyber insurance market [16]. A noteworthy effort to rectify this is the work by ENISA to establish a common risk assessment language, resulting in a report published in late 2017 [8], but such work has not yet had any substantial impact.

The documents were read and analyzed with respect to the research questions, i.e. essentially from the perspective of a retailer who experiences an outage in the electronic payment service. Following preliminary analysis, some remaining questions were posed to the insurance company representatives. Most questions were thus resolved.

³ <https://www.izettle.com/se/pos>, accessed March 13, 2018.

4 Results

4.1 Electronic payment service provider terms and conditions

The *Verifone* terms and conditions⁴ include several clauses that may be applicable to different kinds of service outages. While the service provider offers a support service where the physical POS terminal is replaced if broken, this service explicitly does not apply in case of communications network outages (7.1.b, 7.2). Service availability is explicitly addressed in Section 12 of the terms and conditions, where the service is described as normally being available 24 hours a day, but with exceptions for maintenance, upgrades, and planned service outages (12.1), which the provider reserves the right to perform as communicated on its website (12.2). In case of faults, outages, and disruptions, the provider is obliged to take action to restore service, but explicitly does not accept any liability. There are also some general clauses that may apply to service outages: Section 3.5. defines the service provided “as-is” with no guarantees made about its suitability for the customer or about continuous operation of either the POS terminal or the payment service. Section 22 limits the liability of the service provider to only direct damages to the customer caused by service provider violating the contract, explicitly excludes indirect damage such as lost revenue, profit or production (22.2), and also caps any liability accepted to the sum of payments made by the customer to the service provider in the six months before the incidents, though maximally three times the Price Basic Amount, an annually inflation adjusted sum currently 45 500 SEK (some €4 550). Finally, Section 23 is a *force majeure* clause, excluding liabilities for, e.g., power and telecommunications outages.

The *Nets* terms and conditions⁵ are similar. Section 4 gives the service provider the right to interrupt the service in order to perform repairs, maintenance or improvements, or for other reasons, though planned service outages have to be communicated beforehand, if possible. It is also explicitly stated that the provider is not responsible for the availability or functionality of 3rd party services such as telecommunications or card acquisition (4). Section 7 defines the right of the service provider to discontinue service if the customer does not pay, and explicitly excludes any liability for resulting damages, including any lost transactions. Section 12 limits the liability of the service provider with regard to any specific indirect or additional damages to the customer, explicitly excluding lost revenue, profit, customers, and goodwill. Any liability for direct damages is capped to the sum of payments made by the customer to the service provider in the twelve months before the incidents. Section 13 is a *force majeure* clause, in general excluding any liability for damages resulting from the service provider not being able to fulfill the contract because of circumstances outside

⁴ https://www.verifone.com/sites/default/files/SE_Allmanna%20villkor%20tjanstepaket%20v%202016-11-01%20.pdf, accessed March 6, 2018.

⁵ https://www.nets.eu/globalassets/documents/sweden/in-swedish/terms-etc/nets_payment-terminals_terms_se_20170401.pdf, accessed March 6, 2018.

of the service provider’s control. Section 13 also more specifically excludes liabilities in certain jurisdictions for any damages caused by outages or lack of IT systems availability, as well as disruptions in electricity or telecommunications, and including computer viruses and data breaches.

The *iZettle* terms and conditions⁶ follow the same pattern. Service availability is addressed in Section 11, where it is said that though service is normally available 24/7, the service provider does not guarantee that it is error-free or uninterrupted (11.1). Furthermore, it is explained that maintenance and upgrades can result in interruptions and that even though the service provider will try to communicate about any planned service outages beforehand, this is not guaranteed. The customer also explicitly agrees to understanding that “bugs” do occur, and can lead to disruptions (11.2). The service provider also explicitly excludes any responsibility for the availability of the telecommunications operator services that are needed for the payment service to work (11.3). Section 13.3 explicitly excludes any responsibility for the service being available at all times. Section 14.1 more generally excludes liability for indirect damages and lost profit, and Section 14.3 is a *force majeure* clause that also excludes any liability for the actions or omissions of 3rd parties.

4.2 Cyber insurance policy coverage

On a very general level, typical cyber insurance policies can be described as composed of coverage of (i) 1st party costs (e.g., lost revenue from business interruption, cyber extortion costs, forensic and restoration costs, incident-related legal and PR costs, etc.) and (ii) 3rd party liability costs (e.g., notification costs related to data and privacy breaches, liabilities for spreading malware, fines, media liability, etc.) [9]. The policy parts investigated in this article pertain to 1st party costs, specifically the kinds of business interruption that can be caused by electronic payment service outages. In addition to the overall indemnity limit and deductible of the policy, business interruption coverage is also limited by a *waiting period*, which can be seen as a non-monetary deductible. Waiting periods may be as short as 6 or 8 hours, but are more typically 24, 36, 48, or 72 hours [9]. Only losses incurred after the waiting period has expired are covered. General exclusions common to all policies investigated include claims related to bodily injury and property damage, as well as *force majeure*. Specifically, the investigated policies can be characterized as follows:

Insurance company A offers coverage for business income loss (i.e., reduction in sales, etc.) and business income interruption costs (i.e, costs incurred to minimize the business income loss). The extent of the business income loss is determined using historical data pertaining to the insured’s business before the incident, but the policy does not detail the calculation. Infrastructure failures, including electrical power interruptions and failures in telecommunications, are excluded, except for infrastructure that is under the control of the insured.

⁶ <https://www.izettle.com/se/villkor>, accessed March 12, 2018.

Events at outsourced service providers are explicitly covered (with payment processing as an example). Depending on which additions are purchased, coverage can be either of only interruptions caused by security failures, i.e. antagonistic incidents, or of non-antagonistic systems failures, e.g., a patch that failed.

Insurance company B offers coverage for business interruption loss (i.e., reduction in net profit) and recovery costs (e.g., costs to remove malware, reconstruct data, find programming errors, etc.). The reduction in net profit is calculated based on the net profit of the period corresponding to the outage in the previous 12 months. Recovery costs are capped by the demonstrable business interruption loss. Both antagonistic (malware, hacking, DDoS, etc.) and non-antagonistic (human error, programming error, etc.) events are covered. Power failure is covered only in electrical systems controlled by the insured. A similar exclusion relates to outages in internet access, unless the infrastructure is under the control of the insured.

Insurance company C offers coverage for business interruption loss of profit and operational expenses (i.e., renting IT equipment and buying services to minimize the loss of profit). The loss of profit is calculated based on the profit earned in the previous 60 days, adjusted for a business trend. Notably, only antagonistic network compromise (e.g., unauthorized access and DDoS attacks) is covered. Electrical failure is excluded, except when caused solely by the negligence of the insured in performing technology services. Finally, the computer system affected must be controlled, operated or owned by the insured, creating something of a grey zone when it comes to electronic payment services.

Insurance company D offers basic coverage for business interruption loss. The loss is calculated based on the revenues earned in the past 36 months. In the standard policy, company D covers only this loss, but additional coverage for (i) mitigation costs and (ii) restoration costs is available as extensions. Mitigation costs are capped by the corresponding business interruption loss incurred. Similarly, only business interruptions due to cyber attacks are covered in the standard policy, but coverage of business interruptions due to (i) human error or technical failure as well as (ii) to legal or regulatory requirements are available as extensions. Business interruptions resulting from interruptions or disturbances in electricity, internet, telecommunications, etc. infrastructure that are outside the control of the insured are excluded, as are scheduled service interruptions (including maintenance or repairs lasting longer than expected) and any failure on the part of the insured to anticipate higher demand than normal. Finally, the standard policy limits coverage to insured's own computer system (which must be leased, operated or owned by the insured), so in order to cover an outage at the electronic payment service provider, an additional contingent business interruption (CBI) endorsement must be attached. This would essentially include the electronic payment service provider system into the definition and thus extend the cover to business interruption loss, but not cover any restoration costs for the service provider.

Insurance company E offers coverage for business interruption loss, as well as (i) forensic and restoration costs, and (ii) incident management costs related

to insured incidents. The loss is calculated based on a reference time period three months before the incident, with room for additional adjustment. Outages in electricity, telecommunications, etc., are excluded, as are any losses caused by a business interruption being prolonged because the insured fails to follow instructions given, or cannot afford to take appropriate action. Antagonistic and non-antagonistic business interruptions are covered alike.

The insurance policy recommended by the *German Insurance Association (GDV)* covers business interruption loss (A4-1) as well as forensic cost and loss assessment expenses (A2-1). The interruption loss covered is based on a daily rate specified in the particular insurance policy (A4-1.3.1). Infrastructure outages such as interruptions in electricity, telephone, or internet service are excluded (A1-17.5), as are interruptions resulting from planned service outages, introduction of new software (including major releases of existing software used), untested software, or “software errors which are not based on a security gap” (A4-1.2). These provisions, in particular the last one, limit the extent to which non-antagonistic incidents are covered. Finally, losses resulting from the failure, interruption or malfunctioning of services from external service providers are excluded (A1-2.2), meaning that many outages in electronic payment services are not covered. In practice, the exclusion of external service providers may be carved back, but only restrictively and for named external service providers.

5 Analysis and discussion

5.1 Protection against outages

The electronic payment service provider terms and conditions essentially guarantee best effort only. Though the service providers have some soft obligations to communicate about outages (planned and unplanned), all three sets of terms and conditions are explicitly excluding any liabilities for damages or lost income resulting from service disruptions. Liabilities for infrastructure outages in, e.g., electricity or telecommunications are also excluded. There are also some additional caps on any remaining liabilities. It is noteworthy that the terms and conditions of iZettle do not differ in any relevant way from the traditional service providers with respect to availability and liability for business interruption.

The insurance policies can offer some protection. While all policies offer some coverage of business interruption losses and costs to restore service, there are important differences: Some policies cover only antagonistic disruptions (e.g., DDoS or malware), whereas others cover non-antagonistic disruptions (e.g., misconfigurations or failed upgrades) as well. Some policies cover only interruptions in IT services directly controlled by the insured, whereas others cover interruptions in the external payment service provision as well. The principles for calculating the insured losses differ. Most insurers define a time period to be used as a reference, sometimes with provisions about additional adjustment, but the GDV recommendations instead suggest using a daily rate specified in the particular insurance policy. Finally, no insurer offers coverage of systemic infrastructure disruptions of electricity, telecommunications, etc.

To summarize, a retailer relying only on the electronic payment service provider terms and conditions will get best effort business continuity from the service provider. Cyber insurance can offer additional protection, in the form of risk transfer, for a wide range of business interruptions, but the details of the policy are important to scrutinize. Cyber insurance cannot offer protection against systemic infrastructure disruptions of electricity, telecommunications, etc. Such risks will have to be otherwise mitigated, e.g., using uninterruptible power supply solutions and standby generators etc., or just accepted. However, it is noteworthy that if a retailer does choose to invest in such backup electricity supply, and this also fails, many insurance policies *do* offer coverage of power failures in electrical systems controlled by the insured. Thus, such risk mitigation can also bring about some risk transfer, though the magnitude of such effort is probably prohibitive for many (smaller) retailers.

5.2 Validity and reliability

Validity is very good, in the sense that the documents investigated are precisely the documents governing electronic payment service outages from the perspectives of the payment service providers and insurers, respectively. In the case of the electronic payment service providers, this is the case without exception. As for the insurers, policies are typically subject to some negotiation in the underwriting process, so the exact coverage can vary. However, negotiations mostly involves agreeing to which add-on coverage from an existing list is selected (well illustrated by Insurance company D above) and setting numbers such as waiting periods, deductibles, indemnity limits, and premiums. It is not the case that general exclusions applied by all insurers, such as the exclusions of systemic infrastructure disruptions, are in any meaningful way up for negotiation.

Reliability is also good. Though the documents studied are only samples from the larger sets of all electronic payment service provider terms and conditions and all cyber insurance policies, there are good reasons to believe that the samples are relevant and representative. In the case of the electronic payment service providers, the two traditional ones were chosen by the Swedish Trade Federation precisely because they are mainstream providers with substantial market shares. As for the challenger payments provider, the situation is more complicated, because on the fintech startup scene, there are many more upstarts than incumbents. The choice of iZettle is in this sense a compromise, selecting a major player with a substantial market share, but still a non-traditional company that has been instrumental in transforming the Swedish payment scene and now also works outside the card ecosystem. However, it is clear that the findings cannot be generalized to the terms and conditions of all upstart electronic payment service providers. In the case of the insurers, the sample covers about half of the market actors offering cyber insurance in Sweden [9]. Thus, it is known that the sample is not small and unrepresentative. Furthermore, the comparison to the GDV recommendations offers an additional perspective, indicating that the insurance policies on the Swedish market are quite similar to those (recommended) in Germany.

This leads naturally to the question of generalizing the results to other markets, beyond Sweden. Two strong arguments suggest that this is possible. First, electronic payment service providers are often global (e.g., Verifone) and terms and conditions are largely set by VISA and MasterCard in the form of the Payment Card Industry Data Security Standard (PCI DSS). As all electronic payment service providers need to adhere to this standard, the scope for deviation is small, and terms and conditions are very similar. Thus, the results of this study can reasonably be generalized to most countries.

A similar argument, though not quite as strong, holds for the insurance companies. None of the insurance companies investigated work in Sweden only, and most of them are global companies. Thus, much of the coverage they offer – and do not offer – can be expected to apply across many markets. Though offers can differ depending on regional demand as well as differences in law cross jurisdictions, the basic principles found in the insurance policy documents can be expected to hold in most countries. The most common difference is probably that cyber insurance is not offered at all, rather than that its coverage is radically different.

6 Conclusion

Uninterrupted access to electronic payment systems is becoming increasingly important to the retail industry. This has raised concerns, as electronic payment service providers only offer best effort availability (though it must be noted that this, for the most part, is very high). This finding is confirmed by the results.

One way to better manage the risk is to buy cyber insurance. The analysis in the preceding section shows that this is indeed a relevant tool, but that it comes with important caveats. A checklist for a retailer wishing to procure protection would include the following areas:

Non-antagonistic incidents are not always covered. The retailer should carefully consider whether such coverage is desirable, and if so, make sure to select an insurer offering it.

Systemic failures in electricity and other infrastructure is never covered. This risk thus has to be either accepted or mitigated with backup electricity supply, multiple telecommunications subscriptions, etc.

Interruptions in the external electronic payment service are often excluded from the policy as not being part of the insured's IT environment. Here care must be taken to re-negotiate policies, purchase add-ons, or switch to another insurer, to make sure that outages are covered. As some insurers require an ex ante list of the external service providers to be covered, care also has to be taken to understand the architecture of the card payment system, to get full protection.

The calculation of interruption loss differs between insurers, especially with regard to the time period used as reference period for the outage. Depending on the circumstances of the insured, some calculation principles may be more beneficial than others.

A few interesting avenues for future work suggest themselves. First, it would be interesting to complement the study by also looking at insurance claims, i.e., actual cases of electronic payment service outages being covered by insurance. This would require the cooperation of an insurer willing to share data, but would be rewarding in giving a more precise understanding of the coverage offered in practice. Second, it would be interesting to conduct interviews with retailers who have procured cyber insurance, or who have actively chosen not to, to learn more about how cyber insurance fits into their wider risk management strategies.

Acknowledgments

This research was supported by the the Swedish Civil Contingencies Agency, MSB (agreement no. 2015-6986). The author would like to thank Bengt Nilervall of the Swedish Trade Federation for sharing electronic payment service provider terms and conditions, Dr. Oliver Lamberty of the Deutsche Rückversicherung AG for sharing the GDV recommendations and the insurance companies for sharing actual insurance policy documents and responding to some additional questions. Furthermore, the paper was improved by the comments of three anonymous reviewers.

References

1. Arvidsson, N.: The future of cash. In: Teigland, R., Siri, S., Larsson, A., Puertas, A.M., Bogusz, C.I. (eds.) *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*, pp. 85–98. Routledge (2018)
2. Arvidsson, N.: The payment landscape in sweden. In: Teigland, R., Siri, S., Larsson, A., Puertas, A.M., Bogusz, C.I. (eds.) *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*, pp. 238–252. Routledge (2018)
3. Baer, W.S., Parkinson, A.: Cyberinsurance in IT security management. *IEEE Security & Privacy* **5**(3) (2007). <https://doi.org/10.1109/MSP.2007.57>
4. Böhme, R., Schwartz, G.: Modeling Cyber-Insurance: Towards a Unifying Framework. In: *Workshop on Economics of Information Security – WEIS* (2010)
5. Camillo, M.: System failure: a real and present danger. *Insurance Day* (2015), <https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/insurance-day-aig-cyber-article-system-failure-brochure.pdf>, accessed March 9, 2018.
6. Eling, M., Schnell, W.: What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance* **17**(5), 474–491 (2016). <https://doi.org/10.1108/JRF-09-2016-0122>
7. ENISA: Cyber insurance: Recent advances, good practices and challenges. Tech. rep., European Union Agency for Network and Information Security (2016), <http://dx.doi.org/10.2824/065381>
8. ENISA: Commonality of risk assessment language in cyber insurance. Tech. rep., European Union Agency for Network and Information Security (2017). <https://doi.org/10.2824/691163>
9. Franke, U.: The cyber insurance market in Sweden. *Computers & Security* **68**, 130–144 (2017). <https://doi.org/10.1016/j.cose.2017.04.010>

10. Gillespie, P.: The Top 10 Questions to Ask When Selecting a Digital Commerce Payment Vendor . Tech. rep., Gartner, Inc. (Oct 2016), iD: G00311154
11. Tekniska problem för Nordea-kunder [Technical problems for Nordea customers]. Göteborgs-Posten (August 25 2017)
12. van Laere, J., Berggren, P., Gustavsson, P., Ibrahim, O., Johansson, B., Larsson, A., Lindqwister, T., Olsson, L., Wiberg, C.: Challenges for critical infrastructure resilience: cascading effects of payment system disruptions. In: 14th International Conference on Information Systems for Crisis Response and Management. pp. 281–292 (2017)
13. Larsson, A., Ibrahim, O.I.M., Olsson, L., van Laere, J.: Agent based simulation of a payment system for resilience assessments. In: Proceedings of the International Conference in Industrial Engineering and Engineering Management. pp. 314–318. IEEE (2017). <https://doi.org/10.1109/IEEM.2017.8289903>
14. Majuca, R.P., Yurcik, W., Kesan, J.P.: The evolution of cyberinsurance. arXiv preprint [cs/0601020](https://arxiv.org/abs/0601020) (2006)
15. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A.: Cyber-insurance survey. *Computer Science Review* **24**, 35–61 (2017)
16. OECD: Enhancing the Role of Insurance in Cyber Risk Management (2017). <https://doi.org/10.1787/9789264282148-en>
17. Romanosky, S., Ablon, L., Kuehn, A., Jones, T.: Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? In: Proceedings of the 16th Workshop in the Economics of Information Security (WEIS 2017) (2017)
18. Tidningarnas Telegrambyrå: Problem med kortbetalning i hela landet [Card payment problems all over the country]. Sydöstran (July 24 2017)
19. Bankstrul för SEB – kortbetalning fungerar inte [Bank trouble for SEB – card payments do not work]. Värmlands Folkblad (January 10 2018)
20. Wheeler, J.A., Akshay, L., Proctor, P.E.: Understanding When and How to Use Cyberinsurance Effectively. Tech. rep., Gartner, Inc. (Mar 2015), g00274770
21. Cyber resilience playbook for public-private collaboration. Tech. rep., World Economic Forum (2018), http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf, accessed March 9, 2018. REF 110117.