The Geneva Papers, **2018**, **43**, (239–274)

www.genevaassociation.org

Perceptions of Corporate Cyber Risks and Insurance Decision-Making

Guido de Smidt[a] and Wouter Botzen[b,c,d]
[a]Aon Risk Solutions, Rotterdam, The Netherlands.
E-mail: gds@maildienst.nl
[b]Department of Environmental Economics, Institute for Environmental Studies (IVM), Vrije Universiteit Amsterdam, Amsterdam, The Netherlands.
[c]Utrecht University School of Economics, Utrecht University, Utrecht, The Netherlands.
[d]Risk Management and Decision Processes Center, The Wharton School, University of Pennsylvania, Philadelphia, USA.

This study provides an analysis of individual perceptions of cyber risks amongst professional decision makers. Data are collected using a survey of corporate professionals who are engaged in risk and insurance decision-making in various functional roles mainly in large companies. The study focuses on the perceived probability as well as the anticipated financial impact of cyber risks. Behavioural factors—the availability heuristic, threshold level of concern, degree of worry and trust in one's own organisation's capabilities—are found to have significant influences on the perceived probability and impact of cyberattacks. The probability of a successful cyberattack is overestimated, and the financial impact is underestimated. Given the high perceived expected value of cyberattack losses relative to the costs of cyber risk insurance, it appears that professional decision makers deviate from the expected value-based decision-making by being reluctant to insure for cyber risk.
The Geneva Papers (2018) **43,** 239–274. https://doi.org/10.1057/s41288-018-0082-7

Keywords: availability heuristic; intuitive thinking; insurance demand; risk perceptions

Article submitted 12 May 2017; accepted 5 February 2018; published online 20 March 2018

Introduction

The interest in human behaviour regarding low-probability/high-impact (LPHI) risks, also known as tail risks, is increasing, inspired by the financial crisis and other catastrophic events, such as natural disasters and, more recently, threats of cyberattacks. The academic literature on this subject is growing, as well as the coverage in more popular books[1] and in newspapers and magazines. For instance, The New York Times devoted more than 700 articles to cybercrime and data breaches in 2015 alone[2].

Cyber risk is a complex type of risk, surrounded by information asymmetry between specialised ICT security staff and more general staff and management, and by opacity that also exists between a company and external partners, such as regulators. Some cyber risks

[1] Taleb (2007); Ariely (2009).
[2] Verizon Enterprise Solutions (2015)

can occur frequently and can be characterised as high-probability/low-impact risks, but another substantial part of the cyber risk domain consists of potentially very high losses and forms a low-probability/high-impact risk.[3] We expect that the large organisations on which we focus are more vulnerable to uncertain large losses because of cybercrime, and that it is this part of cyber risk which motivates their decisions to prepare for it.

More than 40 years of research by behavioural economics scientists has empirically shown that in making decisions under risk, people often deviate from rational behaviour, as formalised, for example, in the expected utility theory.[4] This especially applies to low-probability/high-impact risks because most people lack experience with this type of risk event.[5] Individuals are more likely to exhibit bounded rationality in responding to complex risks, also because it is cognitively costly to be perfectly informed about all low-probability/high-impact risks a person faces. This was already described by Herbert Simon in 1957 in his book Models of Man.[6] Moreover, instead of acting only perfectly rationally, people are often subject to systematic and predictable biases, and they use simple rules of thumb (heuristics) that simplify complex decision-making under risk, possibly derived from intuitive thinking.[7] Individual perceptions and responses to risks are heterogeneous. For instance, psychological research demonstrates that in areas such as finance, men are more overconfident than women and that women generally are more risk-averse than men.[8]

Risk perceptions, which can deviate substantially from objective or experts' assessments of risk, can be an important driver of individual decision-making about risk.[9] Research on individual risk perceptions often focuses on the perception of the sheer probability of a catastrophic event. In addition, an examination of the individual perception of the monetary consequences (impact) of such an event is relevant since perceived consequences may have a big influence on protective behaviour.[10] As an illustration, a recent study of flood risk perceptions of floodplain residents in New York City (post hurricane Sandy) shows that anticipated damage is largely underestimated, which may explain why many households in these floodplains make insufficient preparation for flooding.[11]

It has been proposed that several intuitive thinking processes may explain why people under- or overestimate the perceived probability or consequences of low-probability/high-impact risks. For example, according to the availability heuristic, people perceive hazard events as a high risk when they find it easy to imagine, recall or conceptualise the occurrence of such an event.[12] In this regard, individual experience of a hazard or media attention can play an important role in shaping risk perceptions.[13] Also, emotions such as fear, anxiety or worry influence individual perceptions of low-probability/high-impact

[3] Ponemon (2016).
[4] Neumann and Morgenstern (1947).
[5] Kunreuther and Pauly (2004).
[6] Simon (1957).
[7] Stanovich and West (2000); Kahneman and Tversky (2000); Slovic (2000); Kahneman (2011).
[8] Barber and Odean (2001).
[9] Flynn *et al.* (1993); Slovic (2000).
[10] Barberis (2013).
[11] Botzen *et al.* (2015).
[12] Tversky and Kahneman (1973).
[13] Gennaioli and Shleifer (2010).

risks.[14] Terrorism and the risk of dying from a shark attack are examples of risks 'that come easy to mind', are related with fear, and may therefore be overestimated.[15] Overconfidence and trust in the risk management capacities of others may play a role in the underestimation of risks.[16]

This paper examines perceptions of cyber risk as an example of low-probability/high-impact risks. Cyber risk as a result of cybercrime is an emerging risk, spreading around on the breeding grounds of the digitalised society. Cyber risk may be largely misunderstood, caused by the 'iceberg character' of the risk. Many cyber breaches remain under the surface, and only the largest cases are published. From the top of this iceberg, however, 79,790 cyber security incidents were reported by 70 organisations in 2015, resulting in 2,122 confirmed data breaches in 61 countries.[2] Moreover, cyber risk has many faces, from the relatively well-known denial-of-service attack to digital asset damage, system interruption, data loss, stealing of monetary values, theft of private data, espionage, reputational damage and extortion. Cyber events with a negative outcome do have a potentially large impact in terms of direct and indirect losses. This is also the case for the Netherlands, which is the focus of our data collection on cyber risk perceptions. As an illustration, Deloitte developed a Value at Risk (VaR) model for cyber risk in the Netherlands with a 95 per cent confidence interval (once in 20 years). The major findings are that the expected value loss is approximately EUR 10 billion or 1.5 per cent of GDP of the Dutch economy annually. The expected loss for most large Dutch organisations is significant but not critical. The VaR estimate (worst-case scenario), however, is typically eight times higher.[17]

The recent Global State of Information Security Survey 2018 by Price Waterhouse Coopers, CIO and CSO, is based on responses of more than 9,500 professional decision makers worldwide and gives a good picture of the actual state of cyber risk.[18] It reveals that large cyber security breaches have become more common and that many organisations worldwide still struggle to comprehend and manage emerging cyber risks in an increasingly complex digital society. Moreover, many boards still see cyber risk as an IT problem. The U.S. Department of Homeland Security has identified more than 60 entities in the U.S. critical infrastructure where damage, caused by a single cyber incident, could reasonably result in USD 50 billion in economic damages, or 2,500 immediate deaths, or a severe degradation of the U.S. national defence. It is anticipated that 40 per cent of successful cyberattacks result in disruption to operations, 39 per cent in loss or compromise of sensitive data, 32 per cent in negative impact on the quality of products produced, 29 per cent in physical property damage and 22 per cent in harm to human life.[18] Despite awareness of cyber risk, many companies remain unprepared to deal with cyberattacks. For instance, 44 per cent of respondents answer that they do not have an overall information security strategy, 48 per cent state they do not have an employee security awareness program, 54 per cent state they do not have an incident–response process and 39 per cent of respondents are very confident in their organisational capabilities to cope with cyberattacks.[18]

[14] Loewenstein *et al.* (2001).
[15] Johnson *et al.* (1993); Ruscio (2002).
[16] Slovic (2000).
[17] Deloitte (2016).
[18] PWC (2017).

It has been argued that the management of cyber risks in organisations may be influenced by perceptions of cyber risks and behavioural biases[19]; however, we are not aware of a quantitative study on cyber risk perceptions. We aim to fill this gap by collecting data using a survey that elicits cyber risk perceptions of a sample of professionals who are part of the decision-making unit on cyber risk and who work mainly in large corporations facing the threat of cyberattacks. In large organisations, professional decision-making about the mitigation of cyber risk is often complex. The decision-making unit consists of many disciplines such as ICT, risk management, legal, procurement and senior management, and differs in composition according to type of organisation. This may explain why 90 per cent of our respondents indicate that although they are part of the decision-making unit, someone else is ultimately responsible for cyber risk. Furthermore, information asymmetry occurs. Senior management, for instance, is often poorly informed about the technical aspects of cyber security and relies largely on the opinion of ICT staff (Aon working practice).

An interesting aspect of our study is that while most risk perception studies focus on laypeople consisting of the general public, our sample consist of professionals who are engaged in risk and insurance decision-making in their professional life. It has been observed that intuitive thinking processes influence laypeople's risk perceptions in other contexts, such as for flood insurance.[11] We examine whether similar intuitive thinking processes influence the cyber risk perceptions of professionals in terms of perceived probability and consequences. In particular, we estimate the influence of the availability heuristic and emotional factors, such as threshold level of concern, worry and trust on perceptions of the probability, and consequences of cyberattacks. This is relevant since several risk-perception studies have found that intuitive decision processes or biases that influence risk perceptions of laypeople can also influence risk perceptions of experts.[20] For instance, Slovic *et al.* [21] showed that what they call "non-scientific" factors, such as gender and world views, are significantly related to expert judgement of chemical risks. Rowe and Wright[22] conclude on the basis of an assessment of nine empirical studies that there is little empirical evidence for common expectations that experts judge risk differently from the general public or that experts are more veridical in their risk assessments. Hence, several of the intuitive thinking processes that the literature has identified to influence risk perceptions of laypeople may also be applicable to risk perceptions of experts, in our case, the professionals who make decisions about cyber risk. It has been argued by others that behavioural heuristics and biases are relevant to an examination of decision-making about cyber risks even when such decisions are generally made by knowledgeable professionals.[19]

In addition to studying perceptions of cyber risks, we examine demand for cyber insurance as a risk management measure. The insurance market for cyber risk is developing rapidly. Insurers typically also provide direct response services, such as forensic investigation, as they expect that quick resolution will have a positive influence on the cost incurred. International insurance markets are currently prepared to provide capacity of

[19] Pfleeger and Caputo (2012).
[20] Slovic *et al.* (1995, 2004).
[21] Slovic *et al.* (1995).
[22] Rowe and Wright (2001).

about EUR 100 million per insured limit or organisation (Information Aon Global Broking Centre London). However, organisations often purchase cyber insurance on a relatively small scale. This behaviour is consistent with a preference to insure against small losses, which has been observed in some empirical studies in other contexts.[23]

The remainder of this paper is structured as follows. The first section gives the hypotheses about perceptions of cyber risks that will be tested in our analysis. Then we describe the survey and data collection method, and in the subsequent section we provide the results. The final section presents the conclusions.

Hypotheses about perceptions of cyber risk

Given the uncertainty of cyber risk and a lack of widespread objective information on the probability and impact of cyberattacks for specific organisations, we study the perception of cyber risk by professionals in terms of risk awareness, perceived probability and perceived damage. On the basis of existing research, this section will next discuss several factors that are expected to drive these individual cyber risk perceptions which form the basis for the hypotheses to be tested, as summarised in Table 1.

Availability heuristic

It is generally expected that the perception of the probability of a low-probability risk event is positively influenced by the ease with which relevant (similar) events come to mind.[12] The reason is that risks that are easy to imagine are more salient to people, and this positively influences their risk perception.[13] This decision-making process can result in either overestimation or underestimation of the likelihood and impact of such an event, depending on whether a risk is salient or not. Salience of a risk may be related to personal experience of the risk event and/or the availability of public information or media coverage of risk events. This is related to the availability heuristic which postulates that individuals find it easier to imagine that a certain hazard could involve them if they have experienced it in the past.[12] For instance, an individual who has recently experienced a successful cyberattack may find it easier to imagine that a cyberattack will occur again in the future and will have a higher perception of the likelihood than individuals without cyberattack experience. Lately, much attention has being given to cyber security by governments, the consulting sector, the ICT sector and regulators, which may positively influence cyber risk perceptions. On the other hand, the iceberg effect, the many different kinds of possible appearances of cyber events and the non-salience of information on monetary losses can cause opacity around cyber risk. This opacity may be less for people who have experienced a successful cyberattack, and therefore cyber risk perceptions may be higher for such individuals. We expect that the effect of the availability heuristic explains the risk perception of professional decision makers, and we hypothesise that the experience of a successful cyberattack has a positive impact on cyber risk awareness (H1) and perceptions of the cyber risk probability (H2) and impact (H3).

[23] Slovic *et al.* (1977); Scheffel and Smidt (2012).

Table 1 Summary of hypotheses about factors related to cyber risk perceptions

#	*Description*	*Topic*
H1	Experience of a successful cyberattack is positively related to risk awareness	Availability
H2	Experience of a successful cyberattack is positively related to the perceived probability	Availability
H3	Experience of a successful cyberattack is positively related to the perceived impact	Availability
H4	A high degree of worry is positively related to the perceived probability	Worry
H5	A high degree of worry is positively related to the perceived impact	Worry
H6	Thinking that the cyberattack probability is below the threshold level of concern is negatively related to the perceived probability	Concern
H7	Thinking that the cyberattack probability is below the threshold level of concern is negatively related to the perceived impact	Concern
H8	A high degree of trust in the organisation's risk management is negatively related to risk awareness	Trust
H9	A high degree of trust in the organisation's risk management is negatively related to the perceived probability	Trust

Worry

Emotional feelings related to risk, such as worry, may also influence risk perceptions and decision-making under risk.[14] We hypothesise that high degrees of worry about cyber risk are related to high perceptions of the cyber risk probability (H4) and impact (H5).

Threshold level of concern

Threshold models have proposed that individuals may ignore risks whose subjective odds are perceived to be below their threshold level of concern.[24] It has been shown in the context of flood risk perceptions that perceived probability and impact are lower when individuals find that the flood probability they face is below their threshold level of concern, compared with individuals who find it above their threshold level of concern.[11] We hypothesise that perceptions of cyber risk probability (H6) and impact (H7) are significantly lower if professional decision makers think that their cyber risk probability is below their threshold level of concern.

Degree of trust in one's own organisation (confidence)

Trust is another example of an emotion that may influence individual risk perceptions. Slovic[16] provides evidence that individuals perceive a high risk when they distrust the abilities of the government to adequately manage risks. Botzen *et al.*[11] provide evidence that individuals perceive a lower flood risk when they trust the government's flood risk management capability. In the context of cyber risk, we measure trust as the ability of the organisation to successfully prevent, mitigate or deal with a successful cyberattack. We hypothesise that professional decision makers with a high level of trust in their own organisation's risk management capabilities have lower risk awareness (H8) and lower perceptions of the probability of a cyberattack (H9).

[24] Slovic *et al.* (1977); McClelland *et al.* (1993).

Survey research method and data collection

Survey questions

The survey consists of 16 questions which were asked in the following order: risk awareness, perceived probability, degree of worry, threshold level of concern, perceived financial impact, degree of trust in one's own organisation, salience and other independent variables (general characteristics). Because many cyberattacks remain unsuccessful, the questions are focused on the risk of a successful cyberattack. Appendix A provides the full list of survey questions.

We had to limit the number of questions with this sample group, which consists of professional decision makers mainly in large organisations. The reason is that many of our respondents do have very busy agendas, and we aimed for a response rate that is as large as possible. The disadvantage of this approach is that we are also limited in the number of relationships between variables that can be examined with our data. Hence, the number of explanatory variables for risk perception in this survey is not comprehensive, but we tried to focus on key items as discussed below.

Our main variables of interest are the risk perception variables—cyber risk awareness, perceived probability, perceived financial impact, and the risk management variables: 'the presence of cyber risk insurance coverage', or the 'willingness to purchase' this. Being aware of cyber risk can be seen as a condition for willingness to mitigate the risk. Cyber risk awareness is measured using three questions. The first question asks whether the respondent thinks or is certain that a successful cyberattack on their organisation is possible or not possible. The second question asks about the perceived extent of attractiveness of their organisation for a cyberattack. As cyber risk appears in many forms, the third question is about the expected form of impact(s) of a cyberattack, ranging from reputational damage to system disruption, data loss, investigation cost, legal proceedings, extortion and regulatory scrutiny.

According to expected utility theory and cost–benefit analysis, perceived probability and impact are the main risk perception variables that determine whether people will seek protection against the risk. Perceived probability is measured by two questions: the first question asks for the respondent's estimate of the probability of a successful cyberattack on their organisation (not very often, frequent, very often), and the second question asks for their best estimate of this probability (once in every x years). This second question may be more difficult for respondents to answer since many people have difficulties with probabilistic concepts.[16] The perceived financial impact is measured by two questions. The first question asks for the respondent's estimate of the potential total financial impact (direct and indirect cost) of a successful cyberattack on their organisation in categories, ranging from less than EUR 25,000 to over EUR 1 million. The second question asks for their best estimate of this financial impact.

The variables used for explaining individual variations in the aforementioned risk-perception variables include emotional feelings related to cyber risk, namely salience, the threshold level of concern, degree of worry, and confidence in the risk-mitigating capabilities of their own organisation. Salience is measured by two questions: first, by asking where the respondent obtains information on cyberattacks, and second by asking whether or not the respondent has personally experienced a successful cyberattack in their

organisation, in a previous organisation, or in their direct vicinity. The threshold variable is elicited using a question that asks whether the respondent thinks that the probability of a cyberattack is below their threshold level of concern. The degree of worry is measured by asking how far the respondent agrees with the statement that they are worried about the danger of a successful cyberattack on their organisation. The confidence in their own organisation is measured by the question to indicate the respondent's degree of trust in their own organisation to successfully prevent, mitigate or deal with a successful cyberattack.

Finally, several other variables characterising the respondent that may influence their perception of cyber risk are elicited in the survey. These variables include the type of industry sector where the respondent works, organisational size, the functional role of the respondent, ultimate responsibility for cyber risk, and gender.

Sample and data collection

A total of 1,891 professional decision makers constituting the sample for the study were contacted to participate in the survey. These decision makers were part of the decision-making unit about cyber risk in corporate client organisations of Aon Risk Solutions in the Netherlands. The sample comes from Aon's client database and consists of all business sectors from large to small companies with a certain threshold of annual turnover. Sometimes multiple contacts of one organisation are selected. The survey was executed online via email by Market Research Bureau Multiscope via their proprietary software Socratos. The survey was conducted over two weeks during 2016. A total of 172 persons responded.[25]

Tables B1 and B2 in Appendix B provide summary statistics of the variables. Crosstabs are used for testing the hypothesised relations between variables, and we tested for significant differences in proportions (at the 5 per cent significance level) by comparing column proportions with the z-test. For continuous variables, like the best estimate of the cyberattack probability, significant relations (at the 5 per cent significance level) with categorical variables are examined by comparing means between subgroups of categories of the explanatory variable using the Independent Samples *t* test. Some observations are excluded from the analysis due to missing values, but these are usually only a few observations per question.[26]

Sample characteristics

The respondents form a heterogeneous group in terms of functional roles in their organisation, but all respondents are engaged in risk and insurance decision-making. Approximately 35 per cent are engaged in risk management and/or insurance, 17 per cent in finance/control, 9.5 per cent in senior management, and 39 per cent in legal affairs and other roles. The group 'other' consists of several roles: human resources (responsible for

[25] The first 75 respondents were promised a book as a reward for their participation. Our response rate of about 10 per cent is low, but is not unusual for a sample of professionals. For instance, Dichev *et al.* (2013) had a response rate of 5 per cent to a survey of CFOs, and Christensen *et al.* (2016) had a response rate of 5 per cent to a survey of investors.

[26] In general, the number of missing values per question ranges from 0 to 3. Exceptions are responses to the respondent's best estimates of the perceived probability (65) and impact (115 missing) of a successful cyberattack, which highlights the difficulty of making these estimates.

employee benefits insurance and arrangements), ICT/information security, general policy advice, and internal audit and commercial. Of the respondents, 75 per cent are male and 25 per cent are female. Although female workers seem to be under-represented, there is a general over-representation of male workers among risk and insurance decision makers and in the type of functional roles of the respondents in our sample.

Respondent organisations are dispersed over several industry sectors. About half of the respondents work in the financial services and healthcare sectors, which are over-represented. Other sectors include trade, manufacturing and production, construction and engineering, transportation and logistics, public sector and other services. The sample mainly consists of large organisations where cyber risk is believed to be most relevant. Approximately 80 per cent of the organisations where the respondents work fall into the large segment (more than 1,000 employees) and 10 per cent fall into the medium segment (between 100 and 1,000 employees). The remaining 10 per cent are organisations with less than 100 employees.

Only 5 per cent of the respondents indicate that they are ultimately responsible for cyber risk themselves; 90 per cent indicate that this is the responsibility of somebody else; and another 5 per cent answer that it is not clear who carries the ultimate responsibility. This suggests that in large organisations cyber risk is dealt with in decision-making units, and in the majority of respondent organisations the ultimate responsibility is clearly assigned.

Results

Cyber risk awareness, perceived attractiveness of the organisation for a cyberattack, and estimates of the probability and impact of a successful cyberattack

The answers to the question about awareness of cyber risks in Table 2 show that most respondents are aware of the possibility of a successful cyberattack on their organisation. In particular, 84 per cent are certain or think that a successful cyberattack is possible, and only 16 per cent are certain or think that a cyberattack is not possible.

When we look at the perceived attractiveness regarding one's own organisation (Table 3), the picture is different: 60.6 per cent of respondents perceive their organisation as a very likely or medium attractive target for a cyberattack, whereas 39.4 per cent think that the organisation is an unlikely target or no target. This might indicate a certain "not in my organisation" effect. In other words, it is clear that the large majority of respondents are aware of the possibility of a successful cyberattack, but fewer see their own organisation as an attractive target.

Table 2 Awareness of the possibility of a successful cyberattack (in % of the total sample)

Answer option	*%*
I am certain that a successful cyberattack on my organisation is possible	23.1
I think that a successful cyberattack on my organisation is possible	60.9
I think that a successful cyberattack on my organisation is not possible	15.4
I am certain that a successful cyberattack on my organisation is not possible	0.6

Table 3 Perceived attractiveness of the respondent's organisation for a cyberattack (in % of the total sample)

Answer option	*%*
I think that my organisation is very likely to be a target for a cyberattack	13.5
I think that my organisation has a medium likelihood of being a target for a cyberattack	47.1
I think that my organisation is unlikely to be a target for a cyberattack	32.9
I think that my organisation is no target for a cyberattack	6.5

Overall, the probability of a successful cyberattack on one's own organisation is perceived as high. In particular, the answers to the question about perceived probability with fixed answer categories shows that 4.2 per cent of the population think that a cyberattack occurs very often (every year), 66.1 per cent think that a successful cyberattack might occur frequently (once in every 10 years), and 29.7 per cent answer not very often (once in every 100 years). The question about the respondents' best estimate of the probability of a successful cyberattack resulted in a large number of missing values (65), which confirms that estimating the probability of a cyberattack is difficult for most individuals.

The answers to a question about the expected kinds of impacts of a cyberattack are shown in Table 4. Breach notification, brand/reputation damage, system disruption and data loss are the most expected forms of impact, which are all expected by 65 per cent or more of the respondents. Forensic investigation, digital asset damage, legal proceedings, regulatory scrutiny and extortion demands are impacts that are less often expected, while these impacts are likely to be important in reality. These findings highlight the opacity surrounding cyber risk since the respondents do not have a comprehensive insight into the potential kinds of impacts that can occur.

The answers to the question about the expected financial impact of a successful cyberattack with fixed answer categories are shown in Table 5. Relatively low financial impacts (less than EUR 100,000) are expected by 24.3 per cent of respondents; medium financial impacts (between EUR 100,000 and EUR 1 million) are expected by 42.9 per cent; and high financial impacts (greater than EUR 1 million) are expected by 32.9 per cent. The overall picture is that expected financial impacts seem low, with 67 per cent giving low to medium financial impact categories.

Table 4 Expected kinds of impacts from a cyberattack

Answer option	*%*
Breach notification to authorities and customers	80.8
Brand and reputation damage	69.2
System disruption	78.5
Forensic investigations	22.1
Damage to digital assets	38.4
Legal proceedings	39.0
Regulatory scrutiny	48.8
Extortion demands	21.5
Data loss	67.4

Table 5 Expected financial impacts of a successful cyberattack

Answer option	*%*
Less than €25,000	5.0
Between €25,000 and €100,000	19.3
Between €100,000 and €500,000	23.6
Between €500,000 and €1,000,000	19.3
More than €1,000,000	32.9

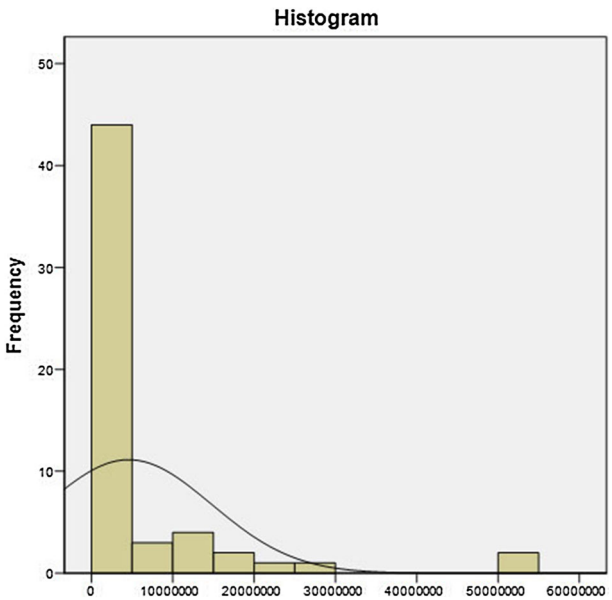

Figure 1. Histogram of the respondents' best estimate of the financial impact of a successful cyberattack.

Many values are missing (115) for the question that asked for the respondent's best estimate of the financial impact of a cyberattack, which suggests that many respondents find it difficult to estimate these impacts. Figure 1 shows the histogram of expected financial impacts of respondents who were able to answer this question. The mean perceived financial impact is EUR 4,569,432, the minimum impact is EUR 2,500 and the maximum expected financial impact is EUR 50 million. There is a large dispersion in the distribution, with a tendency towards relatively low impacts. The distribution is not normal: 71.9 per cent of the estimates of the total financial impact of a successful cyberattack are less than EUR 1 million. On the other side of the spectrum, the outliers range from EUR 20 million to EUR 50 million, which apply to 7.01 per cent of respondents.

There is little objective data available on the financial impacts of cyberattacks. A study by Ponemon[3] reports in a global survey an average data breach cost of USD 4 million.[27] Given that the large majority of our sample (79.5 per cent) consists of large organisations

[27] The average cost per record is USD 158, but differs per sector. In the healthcare sector for instance, the average cost per record is USD 355. The average number of breached records in European countries is 22,607.

with more than 1,000 employees, many of the best estimates of damage (of which the large majority is well below USD 4 million) appear to be on the low side. Large organisations generally maintain higher volumes of digital assets (records) and may face a higher impact from cyber breaches than smaller organisations. Although we cannot exactly match perceived and objective cyber risk levels at an individual company level, overall our findings suggest that many respondents underestimate the potential financial impacts of a successful cyberattack.

Demand for cyber insurance

Cyber insurance is purchased on a small scale. Only 18.4 per cent of the respondents answer that their organisation has purchased cyber insurance, 58.9 per cent of respondents indicate that their organisation lacks cyber insurance, and 22.7 per cent say that their organisation intends to buy cyber insurance in the future. The uptake and demand for cyber insurance is low in view of the unpredictability, the potentially high costs of cyber risk and the challenges faced in fully mitigating the risk through ICT security measures. Since these organisations inevitably maintain insurance for other high-probability/low-impact risks,[28] the observation that many do not demand insurance for low-probability/high-impact cyber risks may signal a preference to insure for small losses that has been observed in other studies.[29]

The low demand for cyber insurance is surprising, given the perceptions of the probability and expected financial consequences of a cyberattack and the premium (pricing) of cyber insurance. This can be illustrated as follows. The general cyber insurance market risk premium is between 0.005 and 0.03 of insured limits.[30] For instance, if the maximum insured loss is EUR 1 million, which would be sufficient for the large majority of respondents who expect lower loss values, the cyber insurance premium would be between EUR 5,000 and EUR 30,000. The expected value of loss by respondents would be about EUR 40,000 if a maximum loss of EUR 1 million is assumed and a probability of 0.04, which are reasonable values for many respondents.[31] Based on expected value calculations, for most respondents, it would make sense to buy cyber insurance, but it appears that many deviate from this decision model in practice.

Feelings towards cyber risks: salience, worry, concern and trust

Salience, which refers to the availability of information on cyber risk, was measured using two questions: (i) the way respondents obtain information on cyber risk; and (ii) whether

[28] Scheffel and Smidt (2012).

[29] Slovic *et al.* (1977).

[30] The estimate of the cyber insurance market risk premium range is based on two observations. First, publication of cyber insurance cost by Data Breach Insurance (Source: https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/) which provides 17 observations across multiple business segments with an average risk premium of 0.00644 (median 0.00360; min. 0.00100; and max. 0.03700; SD 0.00878). Second, a benchmark by Aon Risk Solutions Netherlands which provides 149 observations across multiple business segments with an average risk premium of 0.00332 (median 0.00232; min. 0.00022; and max. 0.03034; SD 0.00350).

[31] The majority of respondents estimate the probability of a successful cyberattack between once in every 5 and once in every 25 years. More than 70 per cent of the respondents give a financial impact value of maximum EUR 1 million.

they have personal experience of a successful cyberattack in their organisation, in a previous organisation, or in their direct vicinity. Overall, salience of risk among the population is high.

Table 6 shows that the majority of respondents have obtained information on cyber risk, which is in line with the wide attention given to the problem of cybercrime in the media. Cyber risk seems to be related mainly to the corporate context because the subject is not often discussed in private. Nevertheless, cyber risks are also an important private matter since, worldwide, large chains of infected private computers exist, the so-called 'botnets'. Many criminal and malicious cyber actions are executed from these botnets. In addition to the large amount of information on cyber risks, many respondents have had some kind of experience with concrete cyberattacks: 20.9 per cent have experienced a cyberattack in their organisation; 2.9 per cent have had this experience in a previous organisation; 7 per cent have experienced it in their direct vicinity; and 33.7 per cent have read about a successful cyberattack in the media. A small majority of 61.0 per cent of respondents have had no personal experience of a successful cyberattack, while 33.7 per cent have read about a successful cyberattack in the media. The overall high levels of salience of cyber risks are in line with all the current attention given to the subject in the media, on the Internet and by business consultants.

Turning to worry about a cyberattack, it is apparent that a small majority of respondents are worried to some extent: 4.1 per cent and 52.6 per cent of respondents, respectively, answered that they strongly agree, or agree, with a statement that they are worried about a cyberattack, while 14.6 per cent disagree and 1.8 per cent strongly disagree. The remainder of 26.9 per cent of respondents are indifferent (neither agree nor disagree). These findings are in line with answers to the question about whether respondents think that the probability of a cyberattack is below their threshold level of concern: a minority of only 18.3 per cent answer that this is the case, and 81.7 per cent answer that this is not the case. These findings indicate that most respondents have negative feelings about cyber risks in terms of worry and concern.

Despite the high degrees of worry and concern about cyber risks, a vast majority of respondents do more or less trust the capabilities of their own organisation to successfully prevent, mitigate or deal with a successful cyberattack. In particular, 34.1 per cent and 56.5 per cent respectively trust their organisation completely or to some extent. A minority distrust the capabilities of their organisation very much (8.2 per cent), or do not trust it at all (1.2 per cent). Given the complexity of managing the risk, this might indicate some degree of overconfidence.

Table 6 Information on cyber risks

Answer options to the question: where do you hear or talk about the possibility of a cyberattack?	*%*
I read about the subject in newspapers, magazines or other publications	78.5
I read about the subject on the Internet	66.9
I discussed the subject with my colleagues	59.3
I talked about the subject with my family and/or friends	8.7
None of the above	4.1

Results of main relations of interest

Output tables with detailed results are reported in Appendix B, and the main significant relations are discussed in the following sections.

The relation between salience and risk awareness, perceived cyber probability, and impact
Our results confirm that salience, or the availability of information, is an important factor influencing risk perception.[12] We find that risk awareness increases when cyber risk is discussed among colleagues and decreases when such discussions do not take place. This applies to both dimensions of risk awareness: the perceived possibility of a successful cyberattack and the perceived attractiveness of one's own organisation for a cyberattack. Respondents who believe that a successful cyberattack on their organisation is possible are significantly more likely to have discussed it with other people than not, while individuals who believe a cyberattack is not possible are more likely not to have discussed it with colleagues.[32] Moreover, the respondents who think that their organisation is a medium attractive target are more likely to have discussed it with colleagues than not, while respondents who think that their organisation is no target are less likely to have discussed it with colleagues.

Furthermore, the use of information sources appears to be significantly related to the perceived possibility of a cyberattack. Respondents who think that a cyberattack on their organisation is possible are significantly more likely to have used information sources, while respondents who think their organisation is not an attractive target are less likely to have used such information sources.[33] The media has also been found to influence cyber risk awareness in the sense that respondents who think that their organisation is not an attractive target for a cyberattack are less likely to read about cyberattacks in the media. Moreover, personal experience of a cyberattack has a significant influence on the awareness of cyber risks. Respondents who are certain that a successful cyberattack is possible[33] or who think that their organisation is a medium attractive target are significantly more likely to have personal experience of a cyberattack in their organisation than not.

For the perceived probability of a cyberattack, significant relations were found between discussions of cyber risks with colleagues and personal experience of a cyberattack. In particular, respondents who estimate the probability as not very often are less likely to have discussed the subject with colleagues, and respondents who estimate the probability as very often are more likely to have experienced a cyberattack. These variables are not significantly related to perceived impacts of a cyberattack, which we did observe to be positively related to reading about cyberattacks in the media.

[32] A similar significant pattern is observed when for this analysis the answer options "I think or am certain that a successful cyberattack is possible" are combined in a separate category, and "I think or am certain that a successful cyberattack is not possible" are combined in a separate category.

[33] No significant effect is observed when for this analysis the answer options "I think or am certain that a successful cyberattack is possible" are combined in a separate category, and "I think or am certain that a successful cyberattack is not possible" are combined in a separate category. This alternative coding results in a loss of information.

Relation between feelings of trust, worry and concern towards cyber risks, with cyber risk awareness, and perceived probability and impact of a cyberattack

Several feelings towards risk were found to be significantly related to cyber risk awareness and the perceived probability and impact of a cyberattack.

Risk awareness appears to be negatively related to a high degree of trust in one's own organisation; respondents who think a successful cyberattack is not possible are more likely to trust their organisation to successfully prevent, mitigate or deal with a cyberattack, and respondents who are certain that a successful cyberattack is possible do not trust their organisation in this regard. Moreover, respondents who think that the probability of a successful cyberattack is low are more likely to have complete trust in their organisation.

Worry is positively and significantly related to the best estimate of the perceived probability of a cyberattack and the perceived impact of a cyberattack. Of respondents who estimate a high financial impact (greater than EUR 1 million), 71.4 per cent have a high degree of worry (strongly agree) as opposed to 32.5 per cent who are worried (agree) and 27.3 per cent who are indifferent (neither agree nor disagree).

Respondents who think that cyber probability is below their threshold level of concern have a significantly lower best estimate and category of the perceived probability and a lower expected impact of a cyberattack. Of the respondents who estimate a low probability, 63.3 per cent indicate that the cyberattack probability is below their threshold level of concern as opposed to 21.8 per cent who think it is above this threshold. Of the respondents who estimate a frequent probability, 72.9 per cent indicate that the cyberattack probability is above their threshold level of concern as opposed to 36.7 per cent who think it is under this threshold. A similar pattern is found for perceived impacts of a cyberattack. Respondents who expect low financial impact below EUR 25,000 are significantly more likely to answer that the cyber probability is below their threshold level of concern, while respondents who expect high impacts between EUR 100,000 and EUR 500,000 are less likely to answer that it is below this threshold.

Other relations

Interesting other relations were observed between cyber risk awareness, the perceived cyber probability and impact, with variables of gender, the functional role of the respondent and responsibility for cyber risks. We did not find significant differences in cyber risk perceptions in relation to organisational size.

Significantly more female than male respondents think that their organisation is a medium attractive target for a cyberattack (64.3 per cent versus 40.5 per cent) and more male than female respondents think that their organisation is not a very attractive target (38.1 per cent versus 19.0 per cent). Moreover, significantly more female than male respondents think that the probability of a cyberattack is high (12.5 per cent versus 1.6 per cent). These findings support evidence from gender research showing more overconfidence among men compared to women.[8]

With regard to the influence of functional role, board members show a significantly higher risk awareness than finance/control staff (12.5 per cent versus 46.2 per cent answer low probability) and legal staff show higher risk awareness than risk managers (15.4 per cent versus 0.0 per cent answer high probability). Moreover, risk managers perceive a higher financial impact than board members (44.4 per cent versus 12.5 per cent). The

perceptions of cyber risks are also related to whether the respondent has ultimate responsibility for cyber risks. Staff who are ultimately responsible for cyber risk estimate lower financial impacts of a cyberattack than other people: 22.2 per cent versus 4.1 per cent estimate impacts lower than EUR 25,000, and 0.0 per cent versus 34.5 per cent estimate impacts higher than EUR 1 million. The low perception of cyber risks among board members and staff responsible for the risk may explain why having insurance coverage for this risk is not a high priority for most companies in our sample.

Comparison of results with recent related field studies

We have compared our results with some recent studies on cyber risk from Advisen, Willis Towers Watson, PWC, and Aon.[34] The report of Marsh[35] focusses on small and medium-sized companies, and hence deviates too much from our sample for a meaningful comparison of results. Advisen (in cooperation with Experian) concludes that internal confidence in organisations is stronger than outward-looking confidence and that companies overestimate their cyber preparedness. This overestimation of preparedness is consistent with the low expected impacts of a cyberattack we find in our sample. It is also consistent with the influence of high trust in one's own organisation on cyber risk perceptions. Furthermore, they conclude that reputational costs are a major concern and that employee negligence in the context of cyber risk is a leading concern.[36]

Willis Towers Watson concludes in a U.K. survey that a certain culture of cyber security is deemed to be important in organisations, many cyber threats exist surrounding employee behaviour, and operating procedures are important in determining cyber risk.[37] Both studies emphasise the importance of behavioural aspects in decision-making about cyber risk, which is consistent with the findings in our study.

The finding of the aforementioned PWC[18] study where 39 per cent of respondents say they are very confident in their organisation's cyberattack capabilities, supports our observation that trust in the organisation's capabilities plays an important role and can indicate a form of overconfidence. Moreover, PWC[18] suggests that a robust global conversation on building resilience against cyber shocks would be productive. This is in line with our finding that discussion between colleagues is positively correlated with higher awareness of cyber risk.

Aon Risk Solutions (in cooperation with the Ponemon Institute) finds in a global survey that intangible information assets are underinsured, contrary to tangible assets (property, plant and equipment) and that organisations tend to disclose more tangible asset losses than information asset losses in their financial statements.[38] Moreover, this study by Aon concludes that companies are still reluctant to purchase cyber insurance coverage, while most companies in the study have experienced a material or significantly disruptive data breach one or more times during the past two years, with an average economic impact of USD 3.6 million.[38] This finding by Aon[38] that there is little cyber insurance demand is consistent with our findings.

[34] Advisen (2017); Willis (2017); PWC (2017); Aon (2017).
[35] Marsh (2016).
[36] Advisen (2017).
[37] Willis (2017).
[38] Aon (2017).

Conclusions

The few studies conducted on assessment of cyber risk indicate that it is a potentially large risk with high potential impacts. Cyber risk can come from anywhere (it is cross-border) and is surrounded by opacity. Because it is an emerging risk, many organisations still need to design adequate risk management strategies for cyberattacks. Insights into cyber risk perceptions may help to improve corporate decision-making with respect to these risks, such as insurance purchases. Up to now, the perception of cyber risks among corporate professional decision makers has hardly been studied. Our study aims to fill this gap by collecting data on a variety of indicators of cyber risk perception from a sample of corporate professionals who are engaged in risk and insurance decision-making in various functional roles mainly in large companies.

The overall picture that emerges from examining answers to the risk perception questions is that overall awareness of the cyber risks is high, the perceived probability is high, but expected impacts of a cyberattack may be underestimated. The high risk awareness is evident from the large majority of respondents who think or are certain that a successful cyberattack on their organisation is possible, and the majority answering that it is likely or very likely that their organisation will be a target for a cyberattack. Nevertheless, for some respondents there appears to be a certain "not in my organisation effect", or "it does happen but not here". Perceived attractiveness of one's own organisation is recognised to a lesser extent. This is remarkable, bearing in mind that the population consists of large organisations, including many healthcare and financial services organisations. These types of organisations are known for their attractiveness as targets for cyberattacks and the presence of large volumes of privacy-sensitive data. Even though overall risk awareness is high, respondents find it difficult to give quantitative estimates of the probability and expected damage of a cyberattack, which may be due to the uncertainty of this emerging risk for which few objective risk assessment studies have been conducted. From the answers to the expected kinds of impacts, it is apparent that few respondents have comprehensive insight into the impact since only a minority expects consequences such as forensic investigations, damage to digital assets, legal proceedings, and extortion demands, although such impacts can occur in reality.

Only a small minority of the organisations (18 per cent) had purchased cyber insurance, although in the Netherlands, such insurance is widely available. In some settings, the limited coverage conditions or high costs relative to risk may be a reason for not buying cyber insurance.[39] However, we do not expect that such supply-side constraints are currently very severe, because the cyber risk insurance market is now well developed.[40] Nevertheless, coverage and/or price conditions may be perceived as undesirable by some corporate buyers.

Alternatively, the low uptake of cyber insurance may be explained by the low expected damage of a cyberattack. Nevertheless, based on the perceived expected value of loss and costs of cyber insurance, it would be desirable for many respondents to demand cyber insurance. This deviation from decision-making based on the expected value of risk may be due to intuitive thinking processes and/or behavioural biases that shape perceptions of

[39] e.g. Eling and Schnell (2016); Shackelford (2012).
[40] Aon Inpoint (2017).

cyber risks. For example, we found that a high degree of trust in an organisation's capacity to manage cyber risks and the absence of experience with a cyberattack results in lower perceptions of cyber risks. With the limited number of observations and control variables, we cannot rule out that other reasons may explain the low demand. In other words, it may be too early to conclude from our results that behavioural biases explain the low demand for cyber insurance, considering the preliminary stage of studies in this field. An example of an alternative explanation is that budget constraints could be a reason for the low demand for cyber insurance, which we cannot examine directly using our survey data. However, we expect budget constraints to be a minor issue for the large organisations in our sample. Experience at Aon shows that large corporations in the Netherlands are able to reserve budgets for insurance if they view a risk as important. Another explanation for the low demand could be that other risk mitigation measures, such as having a communications strategy to deal with reputation losses after a cyberattack, may be deemed more effective for managing cyber risk than insurance.

A variety of relations between our main risk perception variables—awareness, perceived probability, and impact—have been tested in our study. The results with respect to our main hypotheses are summarised in Table 7. From these results, it is apparent that a variety of intuitive thinking processes are related to cyber risk perception. We find evidence of the availability heuristic in that a positive relation exists between experience of a cyberattack and awareness of cyber risk as well as the perceived probability of a successful cyberattack. Experiencing the risk makes it more salient to people and thereby elevates their risk perceptions. Such effects of salience were also found for reading about cyberattacks and discussing cyber risk with colleagues, friends or family. Talking about cyber risk is mainly a corporate affair because it appears that the subject is not discussed often in the private environment.

As clearly seen from Table 7, various feelings towards risks are significantly related to risk awareness and the perceived cyberattack probability and impact. A majority of respondents show a degree of worry towards the risk of a successful cyberattack, and this worry is positively related to the perceived probability and impact of a successful cyberattack. Only a small minority of respondents indicate that the probability of a

Table 7 Summary of results of main hypotheses about factors related to cyber risk perceptions

#	*Description*	*Results*
H1	Experience of a successful cyberattack is positively related to risk awareness	Supported
H2	Experience of a successful cyberattack is positively related to the perceived probability	Supported
H3	Experience of a successful cyberattack is positively related to the perceived impact	Not supported
H4	A high degree of worry is positively related to the perceived probability	Supported
H5	A high degree of worry is positively related to the perceived impact	Supported
H6	Thinking that the cyberattack probability is below the threshold level of concern is negatively related to the perceived probability	Supported
H7	Thinking that the cyberattack probability is below the threshold level of concern is negatively related to the perceived impact	Supported
H8	A high degree of trust in the organisation's risk management is negatively related to risk awareness	Supported
H9	A high degree of trust in the organisation's risk management is negatively related to the perceived probability	Supported

successful cyberattack is too low for concern (below their threshold level of concern), and these respondents have lower cyber risk perceptions. Moreover, our respondents appear to have a high degree of trust in the capacity of their own organisation to successfully prevent, mitigate or deal with a cyberattack, which is negatively related to their awareness of cyber risks and the expected probability of a successful cyberattack.

Several other interesting significant relations were observed regarding cyber risk perceptions, such as functional role, responsibility for cyber risk, and gender. For instance, board members have a higher risk awareness than finance/control staff, while risk managers perceive a higher financial impact than board members. Moreover, legal staff have a higher risk awareness than risk managers. Staff who are ultimately responsible for cyber risk, who in this survey appear to be predominantly board members, estimate lower financial impacts than others. This may be problematic for creating support for adequate cyber risk management strategies in an organisation. With respect to gender, males tend to have lower perceptions of cyber risks than females. It is to be expected that males are over-represented in risk management, ICT and financial sector positions that are responsible for managing cyber risks, which could imply that their lower risk perceptions hamper implementing adequate risk management strategies.

Given the observed challenges individuals experience when forming accurate perceptions of cyber risks, the development of a predictive model to assess total financial impacts and likelihoods of a cyberattack on specific organisations could be useful. In communicating these expert estimates of risk to people in an organisation who are responsible for managing them it is important to adequately frame the risk and provide concrete examples of cyber breaches, their kind of impact and their financial consequences. A high degree of trust in organisational risk management may be unwarranted and create low cyber risk perceptions. Hence, realistic and open communication about the limitations of risk management may be important for creating a sufficiently high cyber risk perception in an organisation. Moreover, setting up structures for colleague and inter-organisational discussions on cyber risk may be an effective way to increase risk awareness, as our results about the influence of salience on risk perception suggest. Future research could examine the effectiveness of such communication strategies to improve awareness and perception of cyber risks. A further investigation of the dynamics of corporate cyber risk decision-making may also be useful. And in general, further research into influencing risk perceptions, the so-called debiasing, is an interesting area for cyber risk research, especially regarding the discrepancy of overestimating probability and underestimating impact. Potential debiasing strategies are explored by Larrick,[41] which could be a useful starting point for such future research.

References

Ariely, D. (2009) *Predictably Irrational: The Hidden Forces that Shape Our Decisions,* New York: Harper Collins Publishers.

Advisen (2017) *2017 Cyber Risk Preparedness and Response Survey*, New York: Advisen Ltd.

Aon (2017) *2017 Global Cyber Risk Transfer Comparison Report,* London: Aon Risk Solutions Ltd.

[41] Larrick (2004).

Aon Inpoint (2017) *Global Cyber Market Overview—Uncovering the Hidden Opportunities,* London: Aon Plc.
Barber, B., and Odean, T. (2001) 'Boys will be boys: gender, overconfidence and common stock investment', *The Quarterly Journal of Economics* 116(1): 261–292.
Barberis, N. (2013) 'The psychology of tail events: Progress and challenges', *American Economic Review* 103(3): 611–616.
Botzen, W.J., Kunreuther, H. and Michel-Kerjan, E. (2015) 'Divergence between individual perceptions and objective indicators of tail risks: Evidence from floodplain residents in New York City', *Judgment and Decision Making* 10(4): 365–385.
Christensen, B.E., Glover, S.M., Omer, T.C. and Shelley, M.K. (2016) 'Understanding audit quality: Insights from audit professionals and investors', *Contemporary Accounting Research* 33(4): 1648–1684.
Deloitte (2016) *Cyber value at risk in The Netherlands,* Amsterdam: Deloitte.
Dichev, I.D., Graham, J. R., Harvey, C.R. and Rajgopal, S. (2013) 'Earnings quality: Evidence from the field', *Journal of Accounting and Economics* 56(2): 1–33.
Eling, M. and Schnell, W. (2016) 'What do we know about cyber risk and cyber risk insurance?', *The Journal of Risk Finance* 17(5): 474–491.
Flynn, J., Slovic, P. and Mertz, C.K. (1993) 'Decidedly different: Expert and public views of risks from a radioactive waste repository', *Risk Analysis* 13(6): 643–648.
Gennaioli, N. and Shleifer, A. (2010) 'What comes to mind', *The Quarterly Journal of Economics* 125(4): 1399–1433.
Johnson, E.J., Hershey, J., Meszaros, J. and Kunreuther, H. (1993) 'Framing, probability distortions and insurance decisions' *Journal of Risk and Uncertainty* 7(1): 35–51.
Kahneman, D. (2011) *Thinking, Fast and Slow,* London: Penguin Group.
Kahneman, D. and Tversky, A. (2000) *Choices, Values and Frames*, New York: Cambridge University Press.
Kunreuther, H. and Pauly, M. (2004) 'Neglecting disaster: Why don't people insure against large losses?', *Journal of Risk and Uncertainty* 28(1): 5–21.
Larrick, R. (2004) 'Debiasing', in Derek J. Koehler and Nigel Harvey (eds.) *Blackwell Handbook of Judgment and Decision Making*, Oxford: Blackwell Publishing Ltd, pp. 316–338
Loewenstein, G.F., Weber, E.U., Hsee, C.K. and Welch, N. (2001) 'Risk as feelings', *Psychological Bulletin* 127(2): 267–286.
Marsh (2016) *2015/2016 Cyber and Data Security Risk Survey Report—for small and midsize employers,* Marsh & McLennan.
McClelland, G.H., Schulze, W.D. and Coursey, D.L. (1993) 'Insurance for Low-Probability Hazards: A bimodal response to unlikely events', in C. Camerer, H. Kunreuther (eds.) *Making Decisions About Liability and Insurance,* Dordrecht: Springer.
Neumann, J.V. and Morgenstern, O. (1947) *The Theory of Games and Economic Behavior* (2nd ed.), Princeton: Princeton University Press.
Pfleeger, S.L. and Caputo, D.D. (2012) 'Leveraging behavioural science to mitigate cyber security risk', *Computers & Security* 31(4): 597–611.
Ponemon (2016) *2016 Cost of a Data Breach Study,* Michigan: Ponemon Institute LLC.
PWC (2017) *Strengthening digital society against cyber shocks—Key findings from The Global State of Information Security Survey 2018*, PWC.
Rowe, G. and Wright, G. (2001) 'Differences in expert and lay judgments of risk: Myth or reality?', *Risk Analysis* 21(2): 341–356.
Ruscio, J. (2002) *Clear Thinking with Psychology: Separating Sense from Nonsense,* Florence: Wadsworth Publishing.
Scheffel, G. and Smidt, G.D. (2012) 'Behavioral Finance and Corporate Insurance Buying: An explorative study into the applicability of behavioral finance to the working practice of Aon', Doctoral Thesis, Nyenrode Business University.
Shackelford, S.J. (2012) 'Should your firm invest in cyber risk insurance?', *Elsevier Business Horizons* 55(4): 349–356.
Simon, H.A. (1957) *Models of Man: Social and Rational-Mathematical Essays on Rational Human Behavior in a Social Setting,* New York: Wiley
Slovic, P. (2000) *The Perception of Risk,* London: Earthscan Ltd.
Slovic, P., Finucane, M.L., Peters, E. and MacGregor, D.G. (2004) 'Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality', *Risk Analysis* 24(2): 311–322.

Slovic, P., Fischhoff, B., Lichtenstein, S., Corrigan, B. and Combs, B. (1977) 'Preference for insuring against probable small losses: Insurance implications', *The Journal of Risk and Insurance* 44(2): 237–258.
Slovic, P., Malmfors, T., Krewski, D., Mertz, C.K., Neil N. and Bartlett, S. (1995) 'Intuitive toxicology. II. Expert and lay judgments of chemical risks in Canada', *Risk Analysis*, 15(6): 661–675.
Stanovich, K.E. and West, R.F. (2000) 'Individual differences in reasoning: Implications for the rationality debate', *Behavioral and Brain Sciences* 23(5): 645–665.
Taleb, N.N. (2007) *The Black Swan: The Impact of the Highly Improbable,* New York: Random House Inc.
Tversky, A. and Kahneman, D. (1973) 'Availability: A heuristic for judging frequency and probability', *Cognitive Psychology* 5(2): 207–232.
Verizon Enterprise Solutions (2015) *2015 Data Breach Investigations Report,* New Jersey: Verizon.
Willis (2017) *2017 Willis Towers Watson Cyber Risk Survey—UK Results*, Willis Towers Watson.

Appendix A. Survey questions

Question 1. Which of the following entries is true for you?

1. I am certain that a successful Cyber Attack on my organisation is possible
2. I think that a successful Cyber Attack on my organisation is possible
3. I think that a successful Cyber Attack on my organisation is not possible
4. I am certain that a successful Cyber Attack on my organisation is not possible

Question 2. How attractive do you think that your organisation is for a Cyber Attack?

1. I think that my organisation is very likely to be a target for a Cyber Attack
2. I think that my organisation has a medium likelihood to be a target for a Cyber Attack
3. I think that my organisation is unlikely to be a target for a Cyber Attack
4. I think that my organisation is no target for a Cyber Attack

Question 3. What kind of impact would you expect from a Cyber Attack on your organisation?

Multiple answers possible

1. Tick
2. No tick

Breach notification to authorities and customers
Brand and reputation damage
System disruption
Forensic investigations
Damage to digital assets
Legal proceedings
Regulatory scrutiny
Extortion demands
Data loss
Other

Question 4a. How do you estimate the probability of a successful Cyber Attack on your organisation with the impact(s) you mentioned in the previous question?

1. Not very often, let's say as often as once in every 100 years
2. Frequently, once in every 10 years
3. Very often, every year

Question 4b. What is your best estimate of this probability?

Open numeric

Once in every …… years

Question 5. To what extent do you agree with the following statement?
I am worried about the danger of a successful Cyber Attack on my organisation.

1. I strongly agree
2. I agree
3. I neither agree or disagree
4. I disagree
5. I strongly disagree

Question 6. Some people think that the probability of a successful Cyber Attack on their organisation is too low to be concerned about. These people find that the probability of a successful Cyber Attack is below their threshold level of concern. Does this apply to you?

1. Yes
2. No

Question 7a. What is your estimation of the potential total financial impact (direct and indirect cost) of a successful Cyber Attack on your organisation?

1. Less than €25,000
2. Between €25,000 and €100,000
3. Between €100,000 and €500,000
4. Between €500,000 and €1,000,000
5. More than €1,000,000

Question 7b. What is your best estimate of this damage?

Open numeric

……. Euro

Question 8. What is the degree of trust in your own organisation to successfully prevent, mitigate or deal with a successful Cyber Attack?

1. In this respect, I do trust my organisation completely
2. In this respect, I do trust my organisation to a certain extent
3. In this respect, I do not trust my organisation very much
4. In this respect, I do not trust my organisation at all

Question 9. Where do you hear/talk about the possibility of a Cyber Attack?

Multiple answers possible

1. Tick
2. No tick

I read about Cyber Attacks in the Newspaper/Magazine/other publications
I read about Cyber Attacks on the Internet
I discussed the possibility of a Cyber Attack with my colleagues
I talked about the possibility of a Cyber Attack with my family and/or friends
None of the above

Question 10. Did you experience a successful Cyber Attack in your organisation, a previous organisation or in your direct vicinity?

Multiple answers possible

1. Tick
2. No tick

I did experience a Cyber Attack in my organisation
I did experience a Cyber Attack in a previous organisation
I did experience a Cyber Attack in my direct vicinity
I read about a Cyber Attack in the media
I did not experience a Cyber Attack

Question 11. To which sector does your organisation belong?

1. Trade
2. Manufacturing & Production
3. Building, Construction & Engineering
4. Transport & Logistics
5. Financial Services
6. Miscellaneous Services
7. Healthcare
8. Public Sector
9. Other

Question 12. What is the size of your organisation?

1. My organisation has more than 1,000 employees
2. My organisation has between 100 and 1,000 employees
3. My organisation has less than 100 employees

Question 13. What is your functional role within the organisation?

1. (Risk) Insurance Manager
2. Risk Manager
3. Legal

4. Finance/Control
5. Board/Senior management
6. Other

Question 14. Who is ultimately responsible for Cyber Risk in your organisation?

1. Me
2. Someone else
3. Not clearly defined

Question 15. Does your organisation use or intend to use Cyber Insurance?

1. My organisation has Cyber Insurance
2. My organisation considers to buy Cyber Insurance
3. My organisation does not have Cyber Insurance

Question 16. I am:

1. Male
2. Female

Appendix B. Tables with detailed results

This appendix provides the tables with output from the statistical analyses. Tables B1 and B2 provide summary statistics of the variables. Tables B3 to B20 provide the output of crosstabs. Z-tests are used to test for differences in column proportions. These outputs should be read as follows: if letters in column proportions in a row are the same then differences in column proportions are not statistically significant at the 5 per cent level, if the letters differ then differences in column proportions are statistically significant at the 5 per cent level.

Table B1 Summary of statistics—respondents/organisations

Sample - respondents	*1.891 - 172*	
	n	*%*
Functional role respondents		
(Risk) insurance manager	30	17.4
Risk manager	29	16.9
Legal	13	7.6
Finance/control	29	16.9
Board/senior management	16	9.3
Other	53	30.8
Missing	2	1.2
Gender respondents		
Male	127	73.8
Female	42	24.4
Missing	3	1.7

Table B1 (continued)

Sample - respondents	*1.891 - 172*	
	n	*%*
Type of organisations		
Trade	11	6.4
Manufacturing & production	14	8.1
Building, construction & engineering	11	6.4
Transport & logistics	3	1.7
Financial services	45	26.2
Miscellaneous services	19	11.0
Healthcare	39	22.7
Public sector	21	12.2
Other	8	4.7
Missing	1	0.6
Organisational size		
> 1,000 employees	136	79.1
100 to 1,000 employees	18	10.5
< 100 employees	17	9.9
Missing	1	0.6

Table B2 Summary of statistics—per question

Question	*n valid*	*%*	*n missing*	*%*	*Mean*	*Median*	*SD*
Q1	169	98.3	3	1.7	———	n.a.	———
Q2	170	98.8	2	1.2	———	n.a.	———
Q3	Multiple answers possible				———	n.a.	———
Q4a	165	95.9	7	4.1	———	n.a.	———
Q4b	107	62.2	65	37.8	18.45	10.00	23.484
Q5	171	99.4	1	0.6	———	n.a.	———
Q6	169	98.3	3	1.7	———	n.a.	———
Q7a	161	93.6	11	6.4	———	n.a.	———
Q7b	57	33.1	115	66.9	4.569.342,11	750.000,00	10.212.402,55
Q8	170	98.8	2	1.2	———	n.a.	———
Q9	Multiple answers possible				———	n.a.	———
Q10	Multiple answers possible				———	n.a.	———
Q11	171	99.4	1	0.6	———	n.a.	———
Q12	171	99.4	1	0.6	———	n.a.	———
Q13	170	98.8	2	1.2	———	n.a.	———
Q14	171	99.4	1	0.6	———	n.a.	———
Q15	163	94.8	9	5.2	———	n.a.	———
Q16	169	98.3	3	1.7	———	n.a.	———

Table B3 Cross-tabulation salience (discussion with colleagues)—risk awareness (possibility)

		I discussed the possibility of a Cyber Attack with my colleagues		*Total*
		Not ticked	*Ticked*	
Which of the following entries is true for you?	I am certain that a successful Cyber Attack on my organisation is possible	17a 25.0%	22 a 21.8%	39 23.1%
	I think that a successful Cyber Attack on my organisation is possible	34 a 50.0%	69 b 68.3%	103 60.9%
	I think that a successful Cyber Attack on my organisation is not possible	16a 23.5%	10b 9.9%	26 15.4%
	I am certain that a successful Cyber Attack on my organisation is not possible	1a 1.5%	0a 0.0%	1 0.6%
Total		68 100.0%	101 100.0%	169 100.0%

Table B4 Cross-tabulation salience (discussion with colleagues)—risk awareness (attractiveness)

		I discussed the possibility of a Cyber Attack with my colleagues		*Total*
		Not ticked	*Ticked*	
How attractive do you think that your organisation is for a Cyber Attack?	I think that my organisation is very likely to be a target for a Cyber Attack	8a 11.6%	15a 14.9%	23 13.5%
	I think that my organisation has a medium likelihood to be a target for a Cyber Attack	26a 37.7%	54b 53.5%	80 47.1%
	I think that my organisation is unlikely to be a target for a Cyber Attack	27a 39.1%	29a 28.7%	56 32.9%
	I think that my organisation is no target for a Cyber Attack	8a 11.6%	3b 3.0%	11 6.5%
Total		69 100.0%	101 100.0%	170 100.0%

Table B5 Cross-tabulation salience (no information source used)—risk awareness (possibility)

		None of the above		*Total*
		Not ticked	*Ticked*	
Which of the following entries is true for you?	I am certain that a successful Cyber Attack on my organisation is possible	37a 22.8%	2a 28.6%	39 23.1%
	I think that a successful Cyber Attack on my organisation is possible	101a 62.3%	2a 28.6%	103 60.9%
	I think that a successful Cyber Attack on my organisation is not possible	23a 14.2%	3b 42.9%	26 15.4%
	I am certain that a successful Cyber Attack on my organisation is not possible	1a 0.6%	0a 0.0%	1 0.6%
Total		162 100.0%	7 100.0%	169 100.0%

Table B6 Cross-tabulation salience (no information source used)—risk awareness (attractiveness)

		None of the above		*Total*
		Not ticked	*Ticked*	
How attractive do you think that your organisation is for a Cyber Attack?	I think that my organisation is very likely to be a target for a Cyber Attack	23a 14.1%	0a 0.0%	23 13.5%
	I think that my organisation has a medium likelihood to be a target for a Cyber Attack	80a 49.1%	0b 0.0%	80 47.1%
	I think that my organisation is unlikely to be a target for a Cyber Attack	53a 32.5%	3a 42.9%	56 32.9%
	I think that my organisation is no target for a Cyber Attack	7a 4.3%	4b 57.1%	11 6.5%
Total		163 100.0%	7 100.0%	170 100.0%

Table B7 Cross-tabulation salience (media)—risk awareness (attractiveness)

		I read about Cyber Attacks in the Newspaper/ Magazine/other publications		*Total*
		Not ticked	*Ticked*	
How attractive do you think that your organisation is for a Cyber Attack?	I think that my organisation is very likely to be a target for a Cyber Attack	7a 19.4%	16a 11.9%	23 13.5%
	I think that my organisation has a medium likelihood to be a target for a Cyber Attack	13a 36.1%	67a 50.0%	80 47.1%
	I think that my organisation is unlikely to be a target for a Cyber Attack	11a 30.6%	45a 33.6%	56 32.9%
	I think that my organisation is no target for a Cyber Attack	5a 13.9%	6b 4.5%	11 6.5%
Total		36 100.0%	134 100.0%	170 100.0%

Table B8 Cross-tabulation salience (personal experience)—risk awareness (possibility)

		I did experience a Cyber Attack in my organisation		*Total*
		Not ticked	*Ticked*	
Which of the following entries is true for you?	I am certain that a successful Cyber Attack on my organisation is possible	24a 17.9%	15b 42.9%	39 23.1%
	I think that a successful Cyber Attack on my organisation is possible	86a 64.2%	17a 48.6%	103 60.9%
	I think that a successful Cyber Attack on my organisation is not possible	23a 17.2%	3a 8.6%	26 15.4%
	I am certain that a successful Cyber Attack on my organisation is not possible	1a 0.7%	0a 0.0%	1 0.6%
Total		134 100.0%	35 100.0%	169 100.0%

Table B9 Cross-tabulation salience (personal experience)—perceived impact

		I read about a Cyber Attack in the media		*Total*
		Not ticked	*Ticked*	
What is your estimation of the potential total financial impact (direct and indirect cost) of a successful Cyber Attack on your organisation?	Less than €25,000	8a 7.7%	0b 0.0%	8 5.0%
	Between €25,000 and €100,000	22a 21.2%	9a 15.8%	31 19.3%
	Between €100,000 and €500,000	25a 24.0%	13a 22.8%	38 23.6%
	Between €500,000 and €1,000,000	21a 20.2%	10a 17.5%	31 19.3%
	More than €1,000,000	28a 26.9%	25b 43.9%	53 32.9%
Total		104 100.0%	57 100.0%	161 100.0%

Table B10 Cross-tabulation degree of trust—risk awareness (possibility)

		What is the degree of trust in your own organisation to successfully prevent, mitigate or deal with a successful Cyber Attack?				*Total*
		In this respect, I do trust my organisation completely	*In this respect, I do trust my organisation to a certain extent*	*In this respect, I do not trust my organisation very much*	*In this respect, I do not trust my organisation at all*	
Which of the following entries is true for you?	I am certain that a successful Cyber Attack on my organisation is possible	9a 15.5%	25a 26.6%	3a 21.4%	2b 100.0%	39 23.2%
	I think that a successful Cyber Attack on my organisation is possible	34a, b 58.6%	57a, b 60.6%	11b 78.6%	0a 0.0%	102 60.7%
	I think that a successful Cyber Attack on my organisation is not possible	14a 24.1%	12a, b 12.8%	0b 0.0%	0a, b 0.0%	26 15.5%
	I am certain that a successful Cyber Attack on my organisation is not possible	1a 1.7%	0a 0.0%	0a 0.0%	0a 0.0%	1 0.6%
Total		58 100.0%	94 100.0%	14 100.0%	2 100.0%	168 100.0%

Table B11 Cross-tabulation degree of trust—perceived probability

		What is the degree of trust in your own organisation to successfully prevent, mitigate or deal with a successful Cyber Attack?				*Total*
		In this respect, I do trust my organisation completely	*In this respect, I do trust my organisation to a certain extent*	*In this respect, Ido not trust my organisation very much*	*In this respect, I do not trust my organisation at all*	
How do you estimate the probability of a successful Cyber Attack on your organisation with the impact(s) you mentioned in the previous question?	Not very often, let's say as often as once in every 100 years	25a 45.5%	19b 20.4%	3a, b 21.4%	1a, b 50.0%	48 29.3%
	Frequently, once in every 10 years	25a 45.5%	72b 77.4%	11b 78.6%	1a, b 50.0%	109 66.5%
	Very often, every year	5a 9.1%	2a 2.2%	0a 0.0%	0a 0.0%	7 4.3%
Total		55 100.0%	93 100.0%	14 100.0%	2 100.0%	164 100.0%

Table B12 Cross-tabulation degree of worry—perceived probability

		To what extent do you agree with the following statement? I am worried about the danger of a successful Cyber Attack on my organisation.					*Total*
		I strongly agree	*I agree*	*I agree neither disagree*	*I disagree*	*I strongly disagree*	
How do you estimate the probability of a successful Cyber Attack on your organisation with the impact(s) you mentioned in the previous question?	Not very often, let's say as often as once in every 100 years	1a 14.3%	17a 19.8%	14a 31.8%	15b 60.0%	2a, b 66.7%	49 29.7%
	Frequently, once in every 10 years	5a, b, c. d 71.4%	64c, d 74.4%	29b, d 65.9%	10a 40.0%	1a, b, c. d 33.3%	109 66.1%
	Very often, every year	1a 14.3%	5a 5.8%	1a 2.3%	0a 0.0%	0a 0.0%	7 4.2%
Total		7 100.0%	86 100.0%	44 100.0%	25 100.0%	3 100.0%	165 100.0%

Table B13 Cross-tabulation degree of worry—perceived impact

		To what extent do you agree with the following statement? l am worried about the danger of a successful Cyber Attack on my organisation.					*Total*
		I strongly agree	*I agree*	*I agree neither disagree*	*I disagree*	*I strongly disagree*	
What is your estimation of the potential total financial impact (direct and indirect cost) of a successful Cyber Attack on your organisation?	Less than €25,000	0a, b 0.0%	1b 1.2%	3a, b 6.8%	3a 12.5%	1a 33.3%	8 5.0%
	Between €25,000 and €100,000	0a 0.0%	17a 20.5%	9a 20.5%	4a 16.7%	1a 33.3%	31 19.3%
	Between €100,000 and €500,000	1a 14.3%	18a 21.7%	12a 27.3%	7a 29.2%	0a 0.0%	38 23.6%
	Between €500,000 and €1,000,000	1a 14.3%	20a 24.1%	8a 18.2%	2a 8.3%	0a 0.0%	31 19.3%
	More than €1,000,000	5a 71.4%	27b 32.5%	12b 27.3%	8a, b 33.3%	1a, b 33.3%	53 32.9%
Total		7 100.0%	83 100.0%	44 100.0%	24 100.0%	3 100.0%	161 100.0%

Table B14 Cross-tabulation threshold level of concern—perceived probability

		Threshold level of concern		*Total*
		Yes	*No*	
How do you estimate the probability of a successful Cyber Attack on your organisation with the impact(s) you mentioned in the previous question?	Not very often, let's say as often as once in every 100 years	19a 63.3%	29b 21.8%	48 29.4%
	Frequently, once in every 10 years	11a 36.7%	97b 72.9%	108 66.3%
	Very often, every year	0a 0.0%	7a 5.3%	7 4.3%
Total		30 100.0%	133 100.0%	163 100.0%

Table B15 Cross-tabulation threshold level of concern—perceived impact

		Threshold level of concern		*Total*
		Yes	*No*	
What is your estimation of the potential total financial impact (direct and indirect cost) of a successful Cyber Attack on your organisation?	Less than €25,000	5a 17.2%	3b 2.3%	8 5.0%
	Between €25,000 and €100,000	6a 20.7%	25a 19.2%	31 19.5%
	Between €100,000 and €500,000	11a 37.9%	25b 19.2%	36 22.6%
	Between €500,000 and €1,000,000	1a 3.4%	30b 23.1%	31 19.5%
	More than €1,000,000	6a 20.7%	47a 36.2%	53 33.3%
Total		29 100.0%	130 100.0%	159 100.0%

Table B16 Cross-tabulation functional role—perceived probability

		What is your functional role within the organisation?						*Total*
		(Risk) Insurance Manager	*Risk Manager*	*Legal*	*Finance/ Control*	*Board*	*Other*	
How do you estimate the probability of a successful Cyber Attack on your organisation with the impact(s)you mentioned in the previous question?	Not very often, let's say as often as once in every 100 years	8a, b 26.7%	7a, b 26.9%	5a, b 38.5%	12b 46.2%	2a 12.5%	14 a, b 26.9%	48 29.4%
	Frequently, once in every 10 years	21a, b, c, d 70.0%	19a, b, c, d 73.1%	6c, d 46.2%	13 b, d 50.0%	14a 87.5%	35a, b, c, d 67.3%	108 66.3%
	Very often, every year	1a, b 3.3%	0b 0.0%	2a 15.4%	1a, b 3.8%	Oa, b 0.0%	3a, b 5.8%	7 4.3%
Total		30 100.0%	26 100.0%	13 100.0%	26 100.0%	16 100.0%	52 100.0%	163 100.0%

Table B17 Cross-tabulation functional role—perceived impact

		What is your functional role within the organisation?						*Total*
		(Risk) Insurance Manager	*Risk Manager*	*Legal*	*Finance/ Control*	*Board*	*Other*	
What is your estimation of the potential total financial impact (direct and indirect cost) of a successful Cyber Attack on your organisation?	Less than €25,000	0a 0.0%	0a 0.0%	0a, b 0.0%	2a, b 7.7%	3b 18.8%	3a, b 5.8%	8 5.0%
	Between €25,000 and €100,000	2a 7.1%	4a, b 14.8%	2a, b 18.2%	7a, b 26.9%	2a, b 12.5%	14b 26.9%	31 19.4%
	Between €100,000 and €500,000	9a 32.1%	7a, b 25.9%	3a, b 27.3%	2b 7.7%	5a 31.3%	11 a, b 21.2%	37 23.1%
	Between €500,000 and €1,000,000	7a 25.0%	4a 14.8%	2a 18.2%	7a 26.9%	4a 25.0%	7a 13.5%	31 19.4%
	More than €1,000,000	10a, b 35.7%	12b 44.4%	4a, b 36.4%	8a, b 30.8%	2a 12.5%	17a, b 32.7%	53 33.1%
Total		28 100,0%	27 100.0%	11 100.0%	26 100.0%	16 100.0%	52 100.0%	160 100.0%

Table B18 Cross-tabulation ultimate responsibility—perceived impact

		Who is ultimately responsible for Cyber Risk in your organisation?			*Total*
		Me	*Someone else*	*Not clearly defined*	
What is your estimation of the potential total financial impact (direct and indirect cost) of a successful Cyber Attack on your organisation?	Less than €25,000	2a 22.2%	6b 4.1%	0a, b 0.0%	8 5.0%
	Between €25,000 and €100,000	3a 33.3%	27a 18.6%	1a 14.3%	31 19.3%
	Between €100,000 and €500,000	1a 11.1%	36a 24.8%	1a 14.3%	38 23.6%
	Between €500,000 and €1,000,000	3a 33.3%	26a 17.9%	2a 28.6%	31 19.3%
	More than €1,000,000	0a 0.0%	50b 34.5%	3b 42.9%	53 32.9%
Total		9 100.0%	145 100.0%	7 100.0%	161 100.0%

Table B19 Cross-tabulation gender—risk awareness (attractiveness)

		I am:		*Total*
		Male	*Female*	
How attractive do you think that your organisation is for a Cyber Attack?	I think that my organisation is very likely to be a target for a Cyber Attack	18a 14.3%	5a 11.9%	23 13.7%
	I think that my organisation has a medium likelihood to be a target for a Cyber Attack	51a 40.5%	27b 64.3%	78 46.4%
	I think that my organisation is unlikely to be a target for a Cyber Attack	48a 38.1%	8b 19.0%	56 33.3%
	I think that my organisation is no target for a Cyber Attack	9a 7.1%	2a 4.8%	11 6.5%
Total		126 100.0%	42 100.0%	168 100.0%

Table B20 Cross-tabulation gender—perceived probability

		I am:		*Total*
		Male	*Female*	
How do you estimate the probability of a successful Cyber Attack on your organisation with the impact(s) you mentioned in the previous question?	Not very often, let's say as often as once in every 100 years	38a	10a	48
		30.9%	25.0%	29.4%
	Frequently, once in every 10 years	83a	25a	108
		67.5%	62.5%	66.3%
	Very often, every year	2a	5b	7
		1.6%	12.5%	4.3%
Total		123	40	163
		100.0%	100.0%	100.0%

Table B21 Significance of relationships—categorical versus continuous variables

Independent variable	>	*Dependent variable*	*p value*	*Significance*
Salience - possibility	>	Best estimate perceived probability	0.007	Significant
Salience - possibility	>	Best estimate perceived impact	0.951	Not significant
Salience - attractiveness	>	Best estimate perceived probability	0.009	Significant
Salience - attractiveness	>	Best estimate perceived impact	0.097	Not significant
Degree of worry	>	Best estimate perceived probability	0.025	Significant
Degree of worry	>	Best estimate perceived impact	0.516	Not significant
Threshold level of concern	>	Best estimate perceived probability	0.001	Significant
Threshold level of concern	>	Best estimate perceived impact	0.740	Not significant
Degree of trust in own organisation	>	Best estimate perceived probability	0.140	Not significant
Degree of trust in own organisation	>	Best estimate perceived impact	0.398	Not significant
Ultimate responsibility	>	Best estimate perceived probability	0.162	Not significant
Ultimate responsibility	>	Best estimate perceived impact	0.406	Not significant
Male/female	>	Best estimate perceived probability	0.144	Not significant
Male/female	>	Best estimate perceived impact	0.542	Not significant

About the Authors

Guido de Smidt is an Account Director at Aon Risk Solutions, Rotterdam, the Netherlands, in the department of Global Accounts & Financial Institutions. He graduated in Business Administration at the Nyenrode Business University Breukelen and in Risk Management for Financial Institutions at the VU University, Amsterdam. He is a certified Risk Manager, Financial Institutions. His research interests are in the fields of behavioural economics, decision-making under risk and (corporate) insurance decision-making.

Wouter Botzen is a Professor in the Department of Environmental Economics at the Institute for Environmental Studies (IVM), Vrije Universiteit Amsterdam, and a Professor at the Utrecht University School of Economics. He is a senior research fellow at the Risk Management and Decision Processes Center at the Wharton School, University of Pennsylvania. His main research interests are individual decision-making under risk, risk management and insurance. He has published widely on these themes.