Cyber incidents, security measures and financial returns: Empirical evidence from Dutch firms

Milena Dinkova[†,*], Ramy El-Dardiry[†] and Bastiaan Overvest[†]
[†]CPB Netherlands Bureau for Economic Policy Analysis

May 25, 2020

Abstract

We employ unique survey data on ICT use and administrative tax record data on Dutch firms to understand how cybersecurity investments relate to the probability of cyber incidents and firm profitability. This dataset allows us to control for firm size, industry, and IT organization. We construct a new indicator to measure the degree of cyber maturity of firms and find that this maturity level tends to increase with firm size. Regression analyses suggest that the relation between maturity level and probability of a cyber incident is inverted U-shaped: a higher maturity level is initially associated with a higher incident probability, but the highest maturity level is associated with fewer reported incidents. This finding is consistent with the hypothesis that basic cybersecurity measures enable better detection of incidents and more sophisticated measures help to prevent incidents. Additionally, we consider firm profitability and find no significant correlation between profits and cybersecurity measures.

JEL Classification Numbers: D22, D83, G14 and M15.

Keywords: cybersecurity, detection, prevention, SME, financial costs of cyber incidents.

Acknowledgements: We thank Gustaaf Wijnker for his help with early analyses and discussions. We also thank the attendants of the presentation at the Digital Trust Center in July 2019 and the participants of the sounding board group (Anne Jager, Bernold Nieuwesteeg, Rutger Leukfeldt, Vincent Slieker, Michel Verhagen, Eelco van Vliet and Rogier van Wanroij) for their comments. Furthermore, we are grateful to Rob Aalbers, Harro van Heuvelen, Stephanie Rosenkranz and Erwin Zijleman for providing useful comments. We would like to thank Eelco van Vliet and Mark Kattenberg in particular for detailed comments and suggestions. We thank Statistics Netherlands (CBS) for providing the data.

[*]Corresponding author: CPB, P.O. Box 80510, 2508 GM, The Hague, The Netherlands. E-mail: m.dinkova@cpb.nl.

1 Introduction

The need for firms to invest in cybersecurity has risen as they have become increasingly reliant on information communication technology (ICT). Eurostat (2018)[1] reports that the vast majority, 96%, of EU-28 enterprises made use of a fixed broadband connection to access the internet. Furthermore, 18% of EU-28 enterprises has linked its business processes automatically to those of their suppliers or consumers. This intensive usage of digital processes and products has often been beneficial, both for consumers and firms. At the same time, the increased dependency on ICT has also made firms vulnerable to cyber incidents. A widely reported example is the Petya malware that infected computers in various countries. The total damage caused by Petya has been estimated at more than 10 billion dollar (Greenberg, 2018).

Firms, especially small and medium sized enterprises (SMEs), are said to be insufficiently aware of cyber risks and to invest too little in prevention (Mijnhardt et al., 2016; Valli et al., 2014). Riek and Böhme (2018) have pointed out, however, that cost estimates for cyber incidents are often scientifically unsound. The above estimate for Petya forms no exception. Estimates are typically based on small surveys or unclear methodologies and published by organizations with a monetary incentive to exaggerate costs. More systematic studies are therefore needed to better understand the true impact of cyber incidents (Anderson et al., 2013).

In this study, we empirically assess cybersecurity in firms. Specifically, we investigate how various ICT-security measures correlate with the probability of cyber incidents. Do firms with more precautions report fewer incidents? In addition, we aim to shed light on how cyber incidents correlate with firms' financial performance. We rely on a large representative ($N = 14,128$) annual survey among Dutch firms. This survey contains answers to a large set of questions about the ICT-use of firms. The survey includes information on ICT-security measures and whether firms faced an ICT-security incident, such as a malware infection, a hardware failure or a DDoS attack. We combine this dataset with administrative tax data of corporate financial records. This enables us to relate reported cyber incidents to the profitability of firms. Our analysis covers different types of cyber incidents, which also includes but is not limited to cyber attacks.

In a simple comparison, we observe a positive relation between the number of security

[1] https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database.

measures and the probability of security incidents as well as company size. Arguably, larger firms are exposed to more outside threats due to a higher visibility and a more intense usage of ICT in absolute terms. We aim to estimate a more precise and clean correlation between security efforts and the probability of a cyber incident. Our chief estimation strategy here is to estimate the probability of a cyber incident, conditional on a multitude of confounding factors such as the firm's sector, the number of employees and, most importantly, various security measures.

This paper relates to several other articles in the literature. One approach, followed for instance by Kamiya et al. (2020), is to exploit stock price data to relate a cyber incident to the market valuation of the affected firm. A drawback of this strategy is that it can only be used for firms that are listed on stock exchanges, whereas in most modern economies only large corporations tend to be listed. In addition, this strategy depends on data on publicly known cyber incidents, which is likely to be only a subset of all incidents known to firms themselves. In a study on disclosure of information on cyber attacks, Amir et al. (2018) find that publicly traded companies tend to underreport cyber attacks associated with relatively large drops in equity value.

Another direction in the literature is the use of survey data. Riek and Böhme (2018) conducted a survey among internet users in six European countries to estimate the costs to consumers of cybercrime. An issue with surveys is that respondents may not be able to recall the amount of monetary losses after an incident and/or that respondents implicitly hold diverging interpretations of which losses are attributable to the incident and which losses are not.

A number of studies on the economics of cyber crime emphasize the importance of a multi-disciplinary approach. See, for instance, Anderson and Moore (2009) for a comprehensive review of relevant concepts like moral hazard, externalities and (mis)perceptions of risk in the context of information security, and Moore et al. (2009) for a general discussion of the economics of online crime.

We contribute to the literature by performing an empirical study on the relationship between security measures and incidents for a representative set of firms within an economy. To the best of our knowledge, using a representative data set for this purpose is unique in the cybersecurity literature. By linking the ICT-use survey to reported profit and loss (P&L) statements, we are the first to study the relation between cybersecurity measures and firm performance for a broad range of companies, including SMEs.

This paper is structured as follows: in Section 2, we provide a short theoretical framework. In Section 3, we describe the data used in this study and we discuss the operationalization of measuring investment in security measures. Section 4 discusses the empirical strategy and the link with the theoretical predictions. Section 5 presents the results, first on the relationship between security measures and the probability of reporting a cyber incident, then on the relationship between a firm's financial performance and the security measures taken and ends with robustness checks. Section 6 offers a short discussion that includes directions for future research and policy perspectives related to the results, followed by a brief section pointing out the limitations of this study. We conclude in Section 8.

2 Theoretical framework

To better understand how investing in cybersecurity can affect a firm's financial performance, we sketch a simple framework. Let $E(\pi)$ denote expected profits of a firm, R the firm's revenue and S investment in security measures. Without much loss of generality, we set the costs of production to zero. The probability of a cyber incident is $\lambda_1(R)$, which we assume is an increasing function of the revenue of the firm. The idea behind this assumption is that large firms have a higher visibility and exposure to cyber incidents. The probability that an incident causes harm is $\lambda_2(S)$, which we assume to be a decreasing and strictly convex function of security investments S. Thus, the probability of the firm suffering harm due to a cyber incident is $\lambda_1(R)\lambda_2(S)$. In that event, the firm's expected profit decreases, which we model by letting only a fraction α of revenue remain. Loss in profit could occur due to, for example, lost online sales or recovering costs. We assume here for simplicity that α is fixed, although in practice it could depend negatively on S, with the interpretation that more security measures not only decrease the probability of an incident but also the impact on revenue. Now, we can formalize expected profits as follows:

$$E[\pi] = [1 - \lambda_1(R)\lambda_2(S)]R + \lambda_1(R)\lambda_2(S)\alpha R - S. \tag{1}$$

The first term on the right-hand side is the expected total revenue if no harmful incident occurs, the second term represents the firm's revenue in case of a harmful incident and S are the security outlays which are independent of the incident realization. Firms optimize profits by choosing S. One crucial assumption is that $\lambda_2(S)$ decreases in S and in the

empirical part of this paper we estimate the relation between S and the probability of security incidents to test this hypothesis.

The first-order condition for profit maximization is

$$\frac{\partial E[\pi]}{\partial S} = -\frac{\partial \lambda_2(S)}{\partial S}\lambda_1(R)R(1-\alpha) - 1 = 0. \tag{2}$$

One implication of this stylized framework is that the level of security measures S is endogenous. A profit-maximizing firm chooses S^* such that expected profits are maximized. In the optimum, $\frac{\partial E[\pi]}{\partial S}|_S^* = 0$. This suggests that the estimated effect on profits at the margin is zero. Under the hypothesis that firms are rational and completely informed we expect to find insignificant effects of security measures on firm profits. If, however, firms structurally underestimate the returns to investments in security, they will invest too little and the effect on profitability at the margin could be positive. In other words: if we observe that for firms (or a subsample of firms, such as small firms) the relation between security measures and profitability is positive, then this is indicative of a lack of awareness or incomplete information. In the empirical part of this paper we report an insignificant relation between security measures and profitability, consistent with the assumption of optimal behavior.

A second implication of this simple model is that larger firms invest more in security than smaller firms. Formally: $\frac{\partial S*}{\partial R} > 0$ and this follows straightforwardly from the first-order condition for profit maximization. To see this, note that the FOC can be written as

$$-\frac{\partial \lambda_2(S)}{\partial S} = \frac{1}{\lambda_1(R)R(1-\alpha)}. \tag{3}$$

The left hand side of this equation decreases in S and the right hand side is constant in S, but decreases in R, leading to lower S for higher values of R. In the empirical part of the paper we find evidence for this positive relationship between firm size and security measures.

A third and final implication is that the probability of a harmful incident ($\lambda_1\lambda_2$) may be non-monotonic in firm size. As a firm becomes larger (R increases) the probability of an cyber incident increases but a firm optimally chooses a higher security level as well, which tends to lower the probability of a costly incident. To see this, note that the effect

of firm size on the probability of an incident is given by:

$$\frac{\partial \lambda_1 \lambda_2}{\partial R} = \frac{\partial \lambda_1}{\partial R}\lambda_2 + \lambda_1 \frac{\partial \lambda_2}{\partial S}\frac{\partial S}{\partial R}. \tag{4}$$

The first part of the right-hand side positive, as the probability of a harmful incident increases in firm size and the second part is negative, as the probability of a harmful incident decreases in security measures S and S^* increases in R. Thus, these are opposite effects and it is an empirical matter whether incidents will be detected more or less often by larger firms. Our regression analysis yields evidence for an inverted U-shaped relation between security measures and the probability of cyber incidents.

3 Data

For the purpose of our study, we combine three datasets: an annual survey on ICT-use of Dutch firms, administrative data on firms financial records (NFO) and the general business register (ABR). All our data sources are provided by Statistics Netherlands (CBS).

3.1 Survey ICT-use of Dutch firms

Our primary data source is the survey on ICT-use of Dutch firms for 2017 administered by Statistics Netherlands (CBS). It contains a myriad of questions on ICT-use, security policy measures, cyber incidents and details about ICT-specialists. Furthermore, the survey also contains information about general firm characteristics such as number of employees and sector. CBS has drawn a representative sample from the Dutch general business register including micro-businesses[2] (between 2 and 10 employees). In 2017, 14,128 firms filled in the survey (with 6,000 being micro-businesses).

In the empirical analysis below, we cluster firms into micro companies (2-9 employees), small companies (10-49 employees), medium sized companies (50-199) and large companies ($\geq$ 200 employees).

Table 1 summarizes the types and causes of cyber incidents that have been elicited in the ICT-use survey from 2017. We construct a simple outcome variable measuring the

[2]Freelancers are not included in the survey.

Table 1: Disentangling cyber incidents

Type of cyber incident	Cause
System failure	Software or hardware malfunction
	Attack from outside (DDoS, ransomware)
Data destruction/mutilation	Software or hardware malfunction
	Infection by malware or breach
Disclosure of sensitive information	Actions by own staff (on purpose or by accident)
	Breach, pharming or phishing

Source: Statistics Netherlands.

occurence of a cyber incident: A binary variable set equal to one if a firm has experienced at least one of the incidents from Table 1. See the appendix for the (translated) relevant questions from the survey.

3.2 Financial records of non-financial organizations

The financial records of non-financial organizations (NFO) contain annual tax records from balance sheets and income statements of approximately 200,000 companies that filed their taxes in the Netherlands. Those records allow us to compute financial indicators as profitability. Financial records are registered at a higher level of the firm structure than the survey on ICT-use: Financial records are at the corporate level and the survey responses at the entity level. Further below, we describe how we tackle this issue. Throughout this paper, we will refer to the unit of observations of the financial records and the survey simply as the firm. As the name suggests, the tax records of organizations from the financial sector are not included in the NFO.

3.3 General Business Register

The General Business Register (Algemeen Bedrijvenregister, ABR) includes all firms that are registered in the Netherlands and provides information about firms at different aggregation levels (corporate level and business entity level). This dataset forms the

backbone of all surveys and administrative datasets of Statistics Netherlands. To merge the ICT-survey with the financial records, it is necessary to link both datasets to the ABR. We linked the ICT-survey to the ABR from 2016, because the ICT-use survey from 2017 asks about the situation in 2016.

Combining all those data sources allows us to create a dataset in which we can link self-reported cyber incidents and security policy measures to financial records. This way, we can detect whether and to what extent cybersecurity measures are correlated with financial outcomes.

3.4 Sample selection

For the analysis of determinants of reporting cyber incidents, we use the ICT-use survey comprising 14,128 observations. The assessment of the financial impact of cyber incidents relies on the combination of the survey data with the administrative financial data. To merge the two data sets, we needed to take into account that parent companies can form a tax group with their subsidiaries and are treated as a single taxpayer. In the financial records, one observation is equal to one tax paying firm (i.e. the holding level). As the survey has been conducted at the entity level, it could happen that several respondents (subsidiaries) of the ICT-survey correspond to one record (holding company) in the financial data. In this case, it is impossible to link the survey response to financial records for those are reported at the parent company level which also includes financial records of other subsidiaries that are not part of the ICT-survey. As a result, we only included firms in our dataset with a unique match with the financial data leaving us with a sample of around 8,000 firms that we use for the second part of our empirical analysis.

This sub-sample is not representative of the entire population of Dutch firms. We can draw conclusions though about non-financial firms with a simple corporate structure, that is the majority of Dutch SMEs[3]. Table 2 provides an overview of the distribution of firms that are part of the subsample and the total sample by firm size. More detailed checks on the representativeness of the subsample can be found in the appendix.

[3]Typically, survey responses could not be matched to tax records 1) for firms that do not pay corporate income tax (for instance one-man businesses and foundations), 2) for firms active in the financial sector (due to the nature of the NFO data) and, 3) as explained above, firms with a complex corporate structure (belonging to the 2000 largest companies in the Netherlands).

Table 2: Distribution of firm size for the subsample and total sample (in percentages)

Firm size		
	Subsample	Total sample
Micro	26	37
Small	42	32
Medium	23	19
Large	9	12

Notes: The subsample comprises 7,858 observations and the total sample 14,128 observations. Percentages may not sum up to exactly 100 due to rounding errors. To examine possible multicollinearity between maturity levels and other explanatory variables like firm size, we computed the variance inflation factors (VIF) for each variable. For all specifications, the VIF was below 4 indicating a low level of multicollinearity. A table of all VIF is available upon request.

3.5 The maturity index

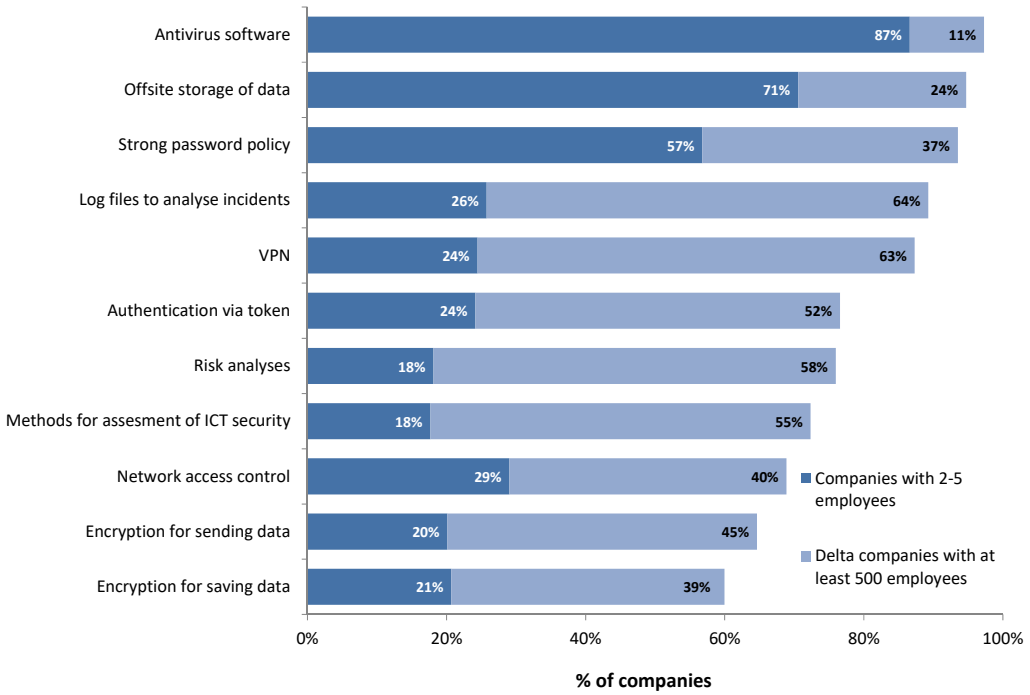
The survey contains eleven different security measures[4], which makes it difficult to consider the relation between security and firm outcomes. We therefore reduce the data by constructing a so-called maturity index. This index proxies the level of cybersecurity sophistication within a company and serves as the main independent variable in our empirical analysis. In the remainder of this section, we explain in more detail how we compute the maturity index.

Fig. 1 shows the eleven different security measures for both the smallest companies (2-5 employees) and the largest companies (500 or more employees). From this figure, we conclude that there is a strong size dependency on the type of cybersecurity measures that are taken, and that relatively few measures appear standard. Antivirus software is the only measure that has become commonplace among both small (87%) and large (98%) companies. On the other side of the spectrum, encryption is hardly found in small companies (20% for sending data and 21% for saving data), while the majority of large

[4]In the appendix, we provide a list of all security measures that were asked in the survey.

companies have encryption in place (65% and 60% respectively).

Figure 1: Percentage of companies that report at least one cyber incident by sector.

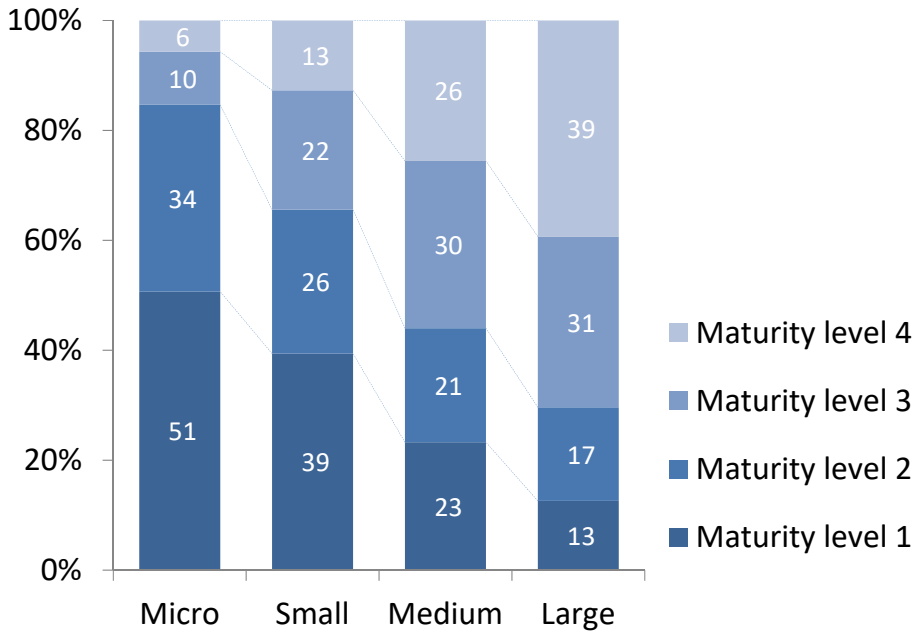


Source: Statistics Netherlands (CBS)

To arrive at the maturity index, we first rank security measures by frequency (Fig. 1). We regard measures that are taken by many firms as basic and measures that few firms adopt as advanced measures. Then, the maturity index is the number of measures a firm has in place, conditional on having the previous measures. It is conditional, because a firm can only advance to a higher index if it has the basic protective measures in place. In this sense, the index punishes for failing to take more basic security measures. In constructing the index, we excluded antivirus software as it turns out not to be an informative indicator[5]. We divide the index in four maturity levels. Firms with (cumulatively) zero or one measure(s) have level 1, firms with two or three measures have level 2, firms with four to six measures have level 3 and firms have level 4 if the cumulative number of measures is higher than six.

[5]It is well-known among experts that some operating systems come with an in-built antivirus software. In that case, respondents might indicate an absence of antivirus software suggesting no protection against viruses even when the opposite is true. As we do not have data on the operating system used by each company, we considered it best to exclude the survey question on anti-virus from our analysis.

Figure 2: Distribution of maturity level by company size.



Note: This figure presents the distribution of cybersecurity maturity levels by four company size classes. The maturity index is calculated via the cumulative procedure as described in the text. *Source*: Statistics Netherlands (CBS).

Consider the following example as an illustration of the maturity index. A company has reported to have implemented the following three security measures: offsite storage of data, strong password policy and VPN. We would consider this company to have a level of two instead of three because it lacks log files to analyze incidents.

Fig. 2 shows the distribution of maturity levels for the four different size categories. Both Fig. 1 and Fig. 2 show that, on average, larger companies have a more sophisticated ICT infrastructure. Those figures also suggest that smaller companies are potentially more vulnerable to outside cyberthreats, in line with observations from the literature (Valli et al., 2014).

We acknowledge that the way we compute the maturity index is one of many possible approaches. We therefore check the robustness of our main results by computing the maturity index in two alternative ways. The first alternative is a simple count of the number of security measures and grouping it into four categories. The second alternative

is based on insights gained from a principal component analysis on the security measures. Here, we divided the security measures into three segments and assigned a score if the company applied security measures from the respective segment. A more detailed explanation of the computation of the second, more intricate alternative measure and a selection of the corresponding estimation results are discussed in the section covering robustness checks (Section 5.3).

4 Empirical strategy

In this section we outline the empirical strategy behind examining the relationships addressed in both research questions. Firstly, we focus on the relationship between reporting a cybersecurity incident and security measures taken. Secondly, we move on to the relationship between financial performance and security measures. For the baseline regressions, we proxy security investments (S in Eq. 1) with the maturity level (M). This is a reasonable proxy as a higher maturity level is likely to require higher investments.

4.1 Probability of (reporting) an incident

When we discussed the theoretical framework in Section 2 of this paper, we assumed that the probability of an incident decreases with the amount of security measures taken by a firm. We empirically test this assumption using a Linear Probability Model (LPM)[6] (adjusted for heteroskedastic standard errors), see Eq. (5). In particular, we estimate the difference in the probability of a firm i reporting at least one incident for different maturity levels relative to a base level:

$$P(I_i = 1 \mid \mathbf{M_i}, \mathbf{F_i}) = \alpha + \mathbf{M_i}'\boldsymbol{\beta} + \mathbf{F_i}'\boldsymbol{\gamma}. \tag{5}$$

I_i is an indicator variable set to 1 if a firm i reported at least one incident. The superscript ' indicates the transpose of a vector. $\mathbf{M_i}$ denotes a vector including three indicator variables for each maturity level (a fourth maturity level is excluded as a ref-

[6] Estimations using a nonlinear model like probit provide similar estimates and standard errors as the linear estimates. Hence, we report our results from the LPM estimations. The nonlinear estimation results using probit are available upon request.

erence category) allowing for nonlinearity in maturity levels. $\mathbf{F_i}$ denotes a vector with firm characteristics. It encompasses ICT specific characteristics such as ICT training offered (to ICT staff and non-ICT staff), whether ICT security is handled internally or being outsourced, and whether a firm uses software for supply chain management system, customer relationship management (CRM) or for enterprise resource planning (ERP). $\mathbf{F_i}$ also includes sector dummies, the logarithm of the number of employees and indicator variables for process and product innovation and e-commerce activity. The vector $\boldsymbol{\beta}$ contains the regression coefficients of reporting an incident for each maturity level relative to the base maturity level (level 1, low maturity), $\boldsymbol{\gamma}$ is a vector representing the regression coefficients of a cyber incident for firm characteristics and α is the intercept.

4.2 Linking profitability and security measures

Next, we consider the relationship between a firm's financial performance and the investment in security measures. When discussing the theoretical framework earlier in this paper, we stated that a profit-maximizing firm chooses the level of security measures such that expected profits are maximized. We will test this theoretical prediction by linking a firm's financial performance with its investment in security measures (again proxied by the maturity index). As a measure for financial performance we use profitability (π), which we calculate as the ratio of net income (Π) and revenue (R) in 2016. We estimate this relationship using Ordinary Least Squares (OLS) regression analysis:

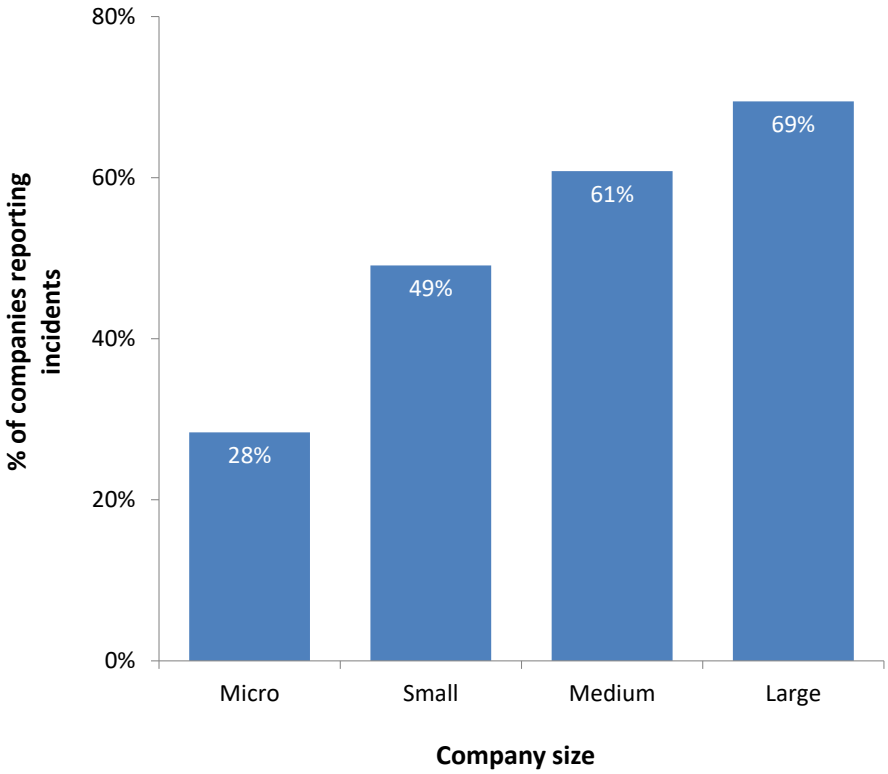
$$\pi_i = \kappa + \mathbf{M_i}'\boldsymbol{\delta} + \mathbf{F_i}'\boldsymbol{\zeta} + \nu_i, \tag{6}$$

where π_i is the profitability of firm i. In contrast to Eq.(5), $\boldsymbol{\delta}$ and $\boldsymbol{\zeta}$ are now vectors containing regression coefficients indicating the change in profitability associated with differences in maturity levels or other firm characteristics respectively. As in Eq.(5), we allow for a nonlinear relationship between maturity levels and the dependent variable. The error term is denoted by ν_i. The other right-hand side variables follow the specification of Eq.(5).

5 Results

5.1 Cyber incidents and security measures

Figure 3: Self reported occurrence of cyber incidents by company size



Source: Statistics Netherlands (CBS)

To gain a better high-level understanding of the patterns in the survey, we summarize the survey data by firm size. Fig. 3 shows the percentage of companies that report at least one incident as a function of company size. The percentage of companies reporting incidents increases from 28% for the smallest companies to 69% for the largest companies. This observation is remarkable given that we have seen previously, in Fig. 2, that the cybersecurity infrastructure becomes more mature with increasing firm size. Yet, this pattern is consistent with Kamiya et al. (2020), who find that more visible (proxied by company size) firms have a higher probability of being targets of a cyber attack. We hypothesize that the size dependency of incidents stems from 1) stronger exposure to outside threats due to higher outside visibility of larger firms, 2) heavier usage of ICT in absolute terms increasing the likelihood of a cyber incident to occur in larger firms

Table 3: Estimated relative probabilities of reporting at least one incident by firm size

	(1)	(2)	(3)	(4)	(5)
Dependent variable	Micro	Small	Medium	Large	All
Firm reported at least 1 incident (dummy)					
Maturity level: Medium low	0.034**	0.033*	0.041	0.040	0.042***
	(0.014)	(0.019)	(0.028)	(0.043)	(0.010)
Maturity level: Medium high	0.118***	0.070***	0.034	0.083**	0.103***
	(0.025)	(0.021)	(0.026)	(0.039)	(0.012)
Maturity level: High	0.081***	0.009	-0.048	0.043	0.032**
	(0.031)	(0.026)	(0.029)	(0.040)	(0.014)
Observations	5,219	4,579	2,679	1,651	14,128
R-squared	0.104	0.098	0.082	0.059	0.157
Joint significance maturity dummies (p-value)	0.000	0.005	0.004	0.152	0.000

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Reference category: Low maturity level (base level probability is 2% for gross sample.). Also included in our estimations, but not reported here are: log(size), sector dummies, security patching, innovation (process, product), use of e-commerce, software use, IT training offered. The complete estimation results can be found in the appendix. To examine possible multicollinearity between maturity levels and other explanatory variables like firm size, we computed the variance inflation factors (VIF) for each variable. For all specifications, the VIF was below 5.6 indicating a low level of multicollinearity. A table of all VIF is available upon request.

and 3) on average a higher maturity level. The regression analysis controls for 1) and 2) by including sector dummies, the number of employees and ICT-characteristics as covariates.

The estimation results of Eq.(5) are presented in Table 3. This table gives the estimated probabilities of reporting at least one incident for different maturity levels relative to the reference category (low maturity level). We estimated the relative probabilities of reporting incidents for each firm size separately (columns 1-4) and for all firm sizes (last column).

We observe an inverted U-shaped relationship between the probability to report an incident and maturity levels when considering the full sample, see column 5. First, estimated probabilities are higher for higher maturity levels: the probabilities relative to the lowest maturity level become more positive in absolute terms. The estimated probability for firms with a medium-low maturity level is more than 4 percentage points higher and for firms with a medium-high maturity level 10 percentage points higher than for firms with a low maturity level. For firms with a "High" maturity level, the probability of reporting an incident decreases. For the gross sample, the base level probability (the probability that we compare the estimated coefficients against) is about 2 percent. Those results suggest that first, the firms' awareness of cyber security problems increases with taking

more basic security measures. In other words, taking basic security measures helps firms in detecting cybersecurity problems. This can explain the positive correlation between firm size and reporting incidents. Once firms report to have additionally taken more advanced security measures (such as conducting penetration tests, risk analyses and using encryption), a lower reported probability of cyber incidents can be an indication of the effectiveness of more advanced/ mature measures in reducing the occurrence of cyber incidents.[7] This hypothesis could be tested further if there would be data available on reported and actual occurrences of cyber incidents. This inverted U-shaped relationship remains when looking at specific firm size categories in Table 3, although the significance of this relationship varies per size category.

5.2 Profitability of security investments

Next, we study the relationship between cybersecurity measures and financial performance. Fig. 4 uses violin plots to show the probability distribution of profitability for the four different maturity levels. A violin plot presents the probability density of a variable. As defined in Section 4.2, profitability is the ratio of net income and revenue. The maturity levels all show similar profitability distributions: there are long tails in both directions, the profitability mean is located around 5 percent, and the peak in probability is above zero, but below the mean. This graph therefore does not indicate a dependence of profitability on the cybersecurity measures taken. We will have to rely on regression analysis to understand whether other factors hide a potential correlation. Company size, for instance, is an obvious factor that could blur correlations between measures and profitability given the strong size dependence of cyber incidents.

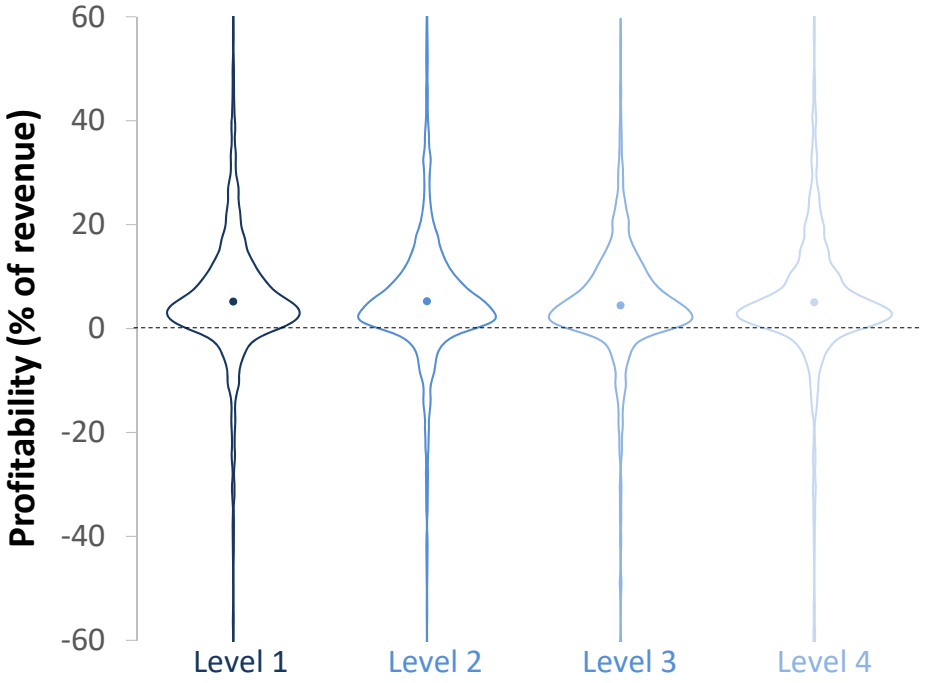
The rich data set at our disposal also allows us to inspect the companies' cybersecurity spending. This way, we can link (reported) expenditures to industry wide benchmarks on cybersecurity spending[8]. Fig. 5 shows the profitability of companies with different cost levels.

The companies have been clustered into ten equally sized bins based on their relative cost level. Companies that do not report costs are left out of this analysis. The dots

[7] We also looked at the relationship between the separate security measures and the probability of reporting an incident. However, the results did not point at a specific pattern and were not conclusive. That is why we did not include them here. They are available upon request.

[8] See for instance an overview of benchmarks in this BCG report on cybersecurity by Asen et al. (2019). Common benchmarks are for instance security spending as a percentage of IT spending.

Figure 4: Profitability probability distribution curves per maturity level.



Source: Statistics Netherlands (CBS)

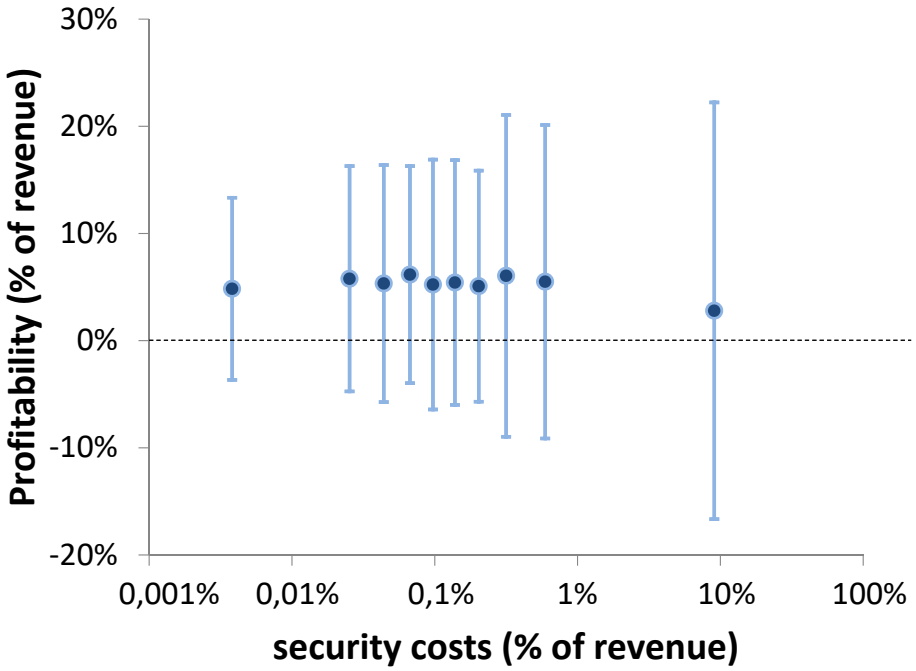
indicate the mean profitability and mean security spending of a decile, and the error bars indicate the standard deviation. There is no obvious correlation between profitability and reported spending.

To test whether other covariates such as software use of firms, size and sector change the relationship between cybersecurity maturity and profitability as given by Fig. 4, we estimate Eq.(6). See Table 4 for the regression results.

The estimation results from Table 4 draw a similar picture as in Fig. 4 – there are no statistically significant differences in profitability related to differences in maturity levels. In Section 5.3, we will test the robustness of the results from Table 4 by including alternative measures of maturity as a main regressor replacing the maturity index used in the previous sections.

We therefore conclude that the main take-away from the analyses in this subsection is that we do not have empirical evidence that cybersecurity is related to profitability at the margin.

Figure 5: Profitability versus cybersecurity spending.



Source: Statistics Netherlands (CBS)

5.3 Robustness checks

To test the robustness of our results regarding the relationship between taking cybersecurity measures and the probability of reporting incidents we conducted three sensitivity analyses. Firstly, instead of using the maturity level as the main regressor, we use a simpler measure to proxy the use of security measures. We count the number of security measures taken[9] and divide the sum into four categories ranging from low to high number of security measures. For consistency, we use similar bins as with the maturity index. Secondly, based on insights from a principal component analysis on the security measures, we come up with an alternative scoring system leading to another alternative maturity index. The results from the previous section appear to be robust to those modifications. At last, we examine the relationship between security measures and different types of incidents corresponding to Table 1.

[9]The same security measures are considered as for the computation of the maturity index.

Table 4: Estimated profitability by firm size

	(1)	(2)	(3)	(4)	(5)
Dependent variable Profitability in 2016: Net income/ Net revenue	Micro	Small	Medium	Large	All
Maturity level: Medium low	-0.004	0.003	0.009	0.002	0.002
	(0.009)	(0.005)	(0.006)	(0.010)	(0.004)
Maturity level: Medium high	-0.015	0.007	-0.009	-0.018*	-0.003
	(0.013)	(0.005)	(0.007)	(0.010)	(0.004)
Maturity level: High	0.026*	0.001	-0.002	-0.007	0.004
	(0.015)	(0.008)	(0.008)	(0.012)	(0.005)
Observations	2,014	3,329	1,777	738	7,858
R-squared	0.019	0.013	0.028	0.045	0.007
Joint significance maturity levels (p-value)	0.140	0.561	0.053	0.196	0.504

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: We excluded all zeroes and the last percentile (out of 100) of the profitability distribution. The distribution of profitability has been sampled before removing the zeroes. Reference category: Low maturity level. Also included in our estimations, but not reported here: log(size), e-commerce, sector dummies, security patching and innovation (process and product). The complete estimation results are reported in the appendix. To examine possible multicollinearity between maturity levels and other explanatory variables like firm size, we computed the variance inflation factors (VIF) for each variable. For all specifications, the VIF was below 4.7 indicating a low level of multicollinearity. A table of all VIF is available upon request.

5.3.1 Simple maturity index: count of the security measures

The estimations related to the probability of reporting an incident and the count of the security measures are reported in Table 5. For the complete estimation results of this model, see Table 11. We observe a similar inverted U-shaped relationship between the amount of security measures taken and the probability of reporting an incident. Firms with relatively low amounts of security measures taken report higher probabilities of incidents implying increasing awareness. After a tipping point of above five measures (out of ten), the cut-off for the category *medium high*, estimated reported probabilities declined for all firms and for micro and small firms.

Analogous to the analyses above, we re-estimated the financial regressions by 1) using the number of security measures instead of the maturity index and 2) using the subsample of firms with e-commerce activity.

Table 6 shows the estimated profitability for the sum of security measures taken (divided into categories) and Table 12 in the appendix reports the complete estimation results. Those results are consistent with the findings from Section 5.2: there appear to be no differences in the profitability of firms for different levels of investment in security measures (i.e. number of security measures taken).

Table 5: Estimated probabilities of reporting incidents by firm size (number of security measures)

	(1)	(2)	(3)	(4)	(5)
Dependent variable	Micro	Small	Medium	Large	All
Firm reported at least 1 incident (dummy)					
Security measures (sum): Medium low	0.123***	0.107***	0.193***	0.194***	0.150***
	(0.016)	(0.020)	(0.035)	(0.070)	(0.011)
Security measures (sum): Medium high	0.180***	0.148***	0.181***	0.188***	0.189***
	(0.021)	(0.022)	(0.036)	(0.068)	(0.012)
Security measures (sum): High	0.112***	0.076***	0.056	0.154**	0.108***
	(0.028)	(0.028)	(0.039)	(0.070)	(0.015)
Observations	5,219	4,579	2,679	1,651	14,128
R-squared	0.118	0.105	0.097	0.062	0.169
Joint significance maturity dummies (p-value)	0.000	0.000	0.000	0.021	0.000

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Security measures(sum) refers to the number of security measures taken in the categories low-high. Reference category: Low number of security measures taken. The cut-offs for the categories are 0-2, 3-5, 6-8 and 9-10 security measures respectively. We control for the same variables as in section 5.2. The complete estimation results can be found in the appendix.

Table 6: Estimated profitability by firm size (number of security measures)

	(1)	(2)	(3)	(4)	(5)
Dependent variable	Micro	Small	Medium	Large	All
Profitability in 2016: Net income/ Net revenue					
Security measures (sum): Medium low	-0.007	-0.001	0.008	0.019	-0.000
	(0.010)	(0.005)	(0.007)	(0.012)	(0.004)
Security measures (sum): Medium high	-0.016	0.007	0.001	0.006	-0.001
	(0.012)	(0.006)	(0.008)	(0.011)	(0.005)
Security measures (sum): High	0.027*	0.009	0.017*	0.012	0.012**
	(0.015)	(0.008)	(0.009)	(0.013)	(0.005)
Observations	2,014	3,329	1,777	738	7,858
R-squared	0.021	0.013	0.028	0.042	0.008
Joint significance maturity levels (p-value)	0.035	0.365	0.143	0.322	0.022

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: We winsorised the sample as in section 6.2. Reference category: Low maturity level. We included the same covariates as in section 6.2. Complete estimation results are reported in the appendix.

5.3.2 A more sophisticated alternative maturity index

We conducted a principal component analysis (PCA) on the security measures to check for alternative cut-off points for a maturity index. The PCA in itself does not lead to conclusive results as the principal components are hard to interpret due to a relative equal distribution of factor loadings. Examining the signs and magnitudes of the factor loadings did provide us though with a general idea to divide the set of security measures into three segments: A, B and C.

Segment A contains the measures offsite storage and strong password policy. Segment B comprises both encryption for sending and receiving data. And lastly, segment C contains the other security measures which are not part of segments A and B.[10]. We assign a score of 1 when a firm reported to apply security measures from a particular segment. This way, we obtain four alternative maturity levels (ranging from scores zero to three). The results confirm the patterns we observed in Sections 5.1 and 5.2. We again found an inverted U-shaped relationship between maturity levels and the estimated probability to report incidents. Similarly, we found no relationship between maturity levels and profitability.[11]

5.3.3 Types of incidents and maturity levels

The main dependent variable when studying the relationship between cyber incidents and security measures is a binary variable of whether or not a firm has reported at least one (out of six different types of) cyber incidents. To check whether the relationship between taking security measures in the shape of the maturity index differs across incident types, we estimated separate regression models per incident type. The results are reported in Table 13. We can recognize the inverted U-shaped relation between maturity levels and the probability of reporting an incident for system failure due to IT problems (columns 9 and 10). For system failure due to an attack, we have evidence for a positive linear relationship between maturity levels and the probability of reporting this type of incident. As to data leaks (data breaches and internal incidents) and incidents of data destruction (IT-related or due to an attack), we cannot confirm the pattern. An explanation for the deviating results is that data leaks and data destruction incidents are

[10] Those measures are: log files to analyze incidents, VPN for access outside company, authentication via token, risk analyses, network access control, methods for assessment of ICT security.

[11] Results are available upon request.

not reported as often as system failure incidents. Not surprisingly so, as especially the first type of incident is very delicate. Moreover, this short analysis raises the question whether the bundle of security measures covers prevention from all different types of security incidents. A complicating factor of this analysis is that oftentimes firms report several types of incidents at the same time which cannot be captured by the estimation results in Table 13.

6 Discussion

Our results indicate that there is a relationship between the occurrence of cyber incidents and the cybersecurity maturity of a firm, while the relationship between firm performance and security measures is not significant. In this section, we reflect on the significance of these results and we put forward several future research directions.

The design of our research enables us to reveal correlations between self-reported incidents, security measures, and financial performance. We believe that those correlations are a necessary first step in understanding the importance of cybersecurity from an economic perspective. One approach to facilitate causal identification is to collect data on security investments and incidents for a longer time period. For example, having panel data might enable a difference-in-differences study on the impact of measures on firm outcomes.

While using a representative survey has many advantages, there is also a drawback in our context, as the observation of cyber incidents is to a certain extent dependent on the ICT maturity of a firm. Some forms of cybercrime, such as stealing processing power to mine cryptocurrencies, can go unnoticed in companies with a low cybersecurity awareness. Thus, it is likely that ICT mature firms observe and report more incidents. To circumvent this issue, an objective detection of cyber incidents is required. One option would be to focus on those cyber incidents that can be detected by third parties. The occurrence of DDoS attacks, e.g., can be deduced from monitoring IP traffic. This route is followed by e.g. Straathof & Overvest (2015). A second option would be to control the attack itself, i.e. to set up "mock attacks", as ethical hackers do in penetration tests. This enables the researcher to measure the success rate of those attacks. Although such an experimental scheme could yield interesting insights on effective cybersecurity measures, it quickly runs into operational and ethical problems, which hamper the scalability of

this approach.

Our analysis did not show a significant relation between the financial performance of a firm and the maturity of its cybersecurity infrastructure. At first glance, this finding is in sharp contrast with reports that highlight significant costs for individual firms following a cyber incident[12]. However, this contrast might in part be explained by tail risks. In that case, high cost cyber incidents are rare and may not show up in the survey. The insignificant effects on profitability could also suggest that most security investments are simply ineffective in preventing costly incidents. Perhaps because a dogged attacker will always find a loophole in the ICT defense system. A final interpretation of the insignificant result is that firms, at the margin, optimize their investment in cybersecurity. Remember from section 2 that a profit-maximizing firm invests in security such that the marginal investment has a zero return. More research, along the lines of the above discussion, is needed to better understand the impact of security measures and firm outcomes.

For policy makers it is important to know whether there are failures in the market for cybersecurity. In the presence of market failures, government action might be justified. It is tempting to conclude that based on this study there is no reason to believe that such market failures exist. Such a conclusion would be based on the observation that there is no relationship between cybersecurity maturity and firm performance: firms thus seem to optimize their security level. We find such a conclusion premature for two reasons. Firstly, government schemes to promote cybersecurity and create awareness were already present in the Netherlands during the period covered by the data. Secondly, there is a possibility that the costs of cybersecurity incidents end up with other parties than the firms themselves, e.g. consumers or government agencies. The presence of such external effects would constitute a market failure in itself that is not covered in this paper.

7 Limitations

Next to its merits, our study is also subject to a number of limitations we would like to point out in this section.

Incidents and security measures are self-reported by the firms responding to the ICT

[12]See e.g. the report *The Cost of Malicious Cyber Activity to the U.S. Economy* by the Council of Economic Advisers (2018) for several illustrations of high costs incidents.

survey. Despite being representative for the Dutch firm population, the information on the occurence of incidents and the security measures taken might not reflect the actual number of security incidents taking place. As suggested in the previous section, a way to mitigate this discrepancy between actual and reported incidents is to gather objective data and compare them to self-reported data as in this study. For this reason, we were very careful in interpreting our results.

Furthermore, sample selection is an issue for the results on the relationship between firm performance and security measures. Linking the ICT survey to administrative tax record data leaves us with a subsample that is not representative for the general population of Dutch firms anymore. However, the results are representative for non-financial Dutch SMEs.

8 Conclusion

We have studied how the occurrence of cybersecurity incidents and the financial performance of firms relate to cybersecurity measures. For that purpose, we have leveraged a representative ICT-use survey on Dutch firms and clustered companies into four cybersecurity maturity levels based on security measures taken. We found that the probability of self-reported cyber incidents first correlates positively with maturity, i.e. more cyber mature firms have a higher probability of reporting cyber incidents. However, for companies with the highest cybersecurity maturity, the probability of reporting cyber incidents decreases. These findings appear across company size categories and are robust for different definitions of cybersecurity maturity. The results suggest that a certain level of cybersecurity infrastructure is needed to adequately detect incidents and further investments in cybersecurity measures then help to prevent incidents.

We did not find any significant relationships between the profitability of firms and their cybersecurity maturity. This finding suggests that firms invest rationally in cybersecurity. Our study emphasizes the importance of quantitative studies on cybersecurity for understanding the socio-economical impact of cybercrime and opens up new research directions.

References

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Springer.

Anderson, R. & Moore, T. (2009). Information Security: Where Computer Science, Economics and Psychology Meet. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, 2717–2727.

Asen, A., Bohmayr, W., Deutscher, S., Gonzalez, M., & Mkrtchian, D. (2019). Are you spending enough on cybersecurity? Technical report, Boston Consultancy Group.

CEA (2018). The cost of malicious cyber activity to the U.S. economy. Technical report, The Council of Economic Advisers.

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *WIRED online magazine*.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 1–31.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, *56*(2), 106–115.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, *23*(3), 3–20.

Riek, M. & Böhme, R. (2018). The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, 1–16.

Straathof, S. & Overvest, B. (2015). What drives cybercrime? empirical evidence from DDoS attacks. *CPB Discussion Paper*.

Valli, C., Martinus, I. C., & Johnstone, M. N. (2014). Small to medium enterprise cyber security swareness: An initial survey of Western Australian business. In *Proceedings*

of International Conference on Security and Management, (pp. 71–75)., Las Vegas, USA. CSREA Press.

9 Appendix

Relevant questions from ICT survey

ICT-specialists

Does your company employ one or more ICT-specialists?
◯ Yes ◯ No

Did your company offer courses or training to ICT-specialists employed at your company in order to improve their ICT skills?
◯ Yes ◯ No

Did your company offer courses or training to other employees at your company in order to improve their ICT skills?
◯ Yes ◯ No

Automatic data exchange within a company

Does your company use ERP-software (Enterprise Resource Planning) to share information between different departments (for instance accounting, planning, production, marketing)?
◯ Yes ◯ No

Does your company use CRM-software (Customer Relationship Management) to administer client data?
◯ Yes ◯ No

Does your company use a system for chain integration or supply chain management (or something similar) to digitally exchange business information with other businesses?
◯ Yes ◯ No

ICT security: general questions

<*Intro*> The following questions are about ICT security. We [CBS] ask about measures, controls and procedures a company is taking with regard to ICT systems with the aim to maintain integrity, authenticity, availability and reliability of data and data systems.

Who was mainly responsible for ICT security and data protection of your company in 2016?

◯ Own staff ◯ External supplier ◯ Not applicable

Did your company do security updates (security patching) mostly automatically or mostly (partially) manually?

◯ Mostly entirely automatically ◯ Mostly (partially) manually ◯ Not applicable

How much money did your company spend in 2016 on ICT security measures (excl. VAT)?

◯ (estimation in thousands of Euro) ◯ It is not possible to provide an estimation

ICT-security: security measures

Does your company take the following security measures? (Yes/No)

- Antivirus software
- Strong passwords policy
- Identification and authentication of users through software or hardware-tokens in order to gain access to ICT systems (or two-factor authentication)
- Encryption technologies to store data and/or documents
- Encryption technologies to send data and/or documents, for instance by email
- Store (backup) data at another physical location (offsite data-backup)
- Network access control (only devices that meet certain requirements are granted access to the business network, e.g. devices that have the most recent update of an operating system)
- Virtual private network (VPN) for internet access outside the company (short explanation of what a VPN network entails)
- Saving log-files for subsequent analysis of incidents
- Methods to assess the ICT security in your company, for instance letting a third party check the security measures or conducting tests
- Risk analyses (periodically assess the probability of being attacked or having an incident and possible consequences thereof)
- Other measures

ICT-security: security incidents

How often did the following ICT-security incidents occur in your company in 2016?

System failure due to ICT-related security incidents, like a malfunctioning hardware or software

◯ Never ◯ 1 or 2 times ◯ 3 or 4 times ◯ More than 4 times

System failure due to an external attack, e.g. DoS (denial of service) or ransomware attacks

◯ Never ◯ 1 or 2 times ◯ 3 or 4 times ◯ More than 4 times

Destruction or mutilation of data due to ICT-related security incidents, such as malfunctioning hardware or software

◯ Never ◯ 1 or 2 times ◯ 3 or 4 times ◯ More than 4 times

Destruction or mutilation of data due to an infection by malicious software or unauthorized electronic access

◯ Never ◯ 1 or 2 times ◯ 3 or 4 times ◯ More than 4 times

Disclosure of confidential electronic data due to breach, pharming or phishing

◯ Never ◯ 1 or 2 times ◯ 3 or 4 times ◯ More than 4 times

Disclosure of confidential electronic data due to own staff, purposefully or accidentally

◯ Never ◯ 1 or 2 times ◯ 3 or 4 times ◯ More than 4 times

E-commerce

Did your company receive orders for goods and services in 2016 via a website or an application?
◯ Yes ◯ No

Checks on sample selection

Table 7: Maturity level by firm size for each sample (in percentages)

Panel A: Subsample (n=7,858)					
Firm size	Micro	Small	Medium	Large	Total
Maturity level					
Low	11.73	17.31	6.16	1.46	36.66
Medium low	8.76	11.33	5.01	1.90	26.99
Medium high	3.27	9.15	6.76	2.94	22.12
High	1.87	4.58	4.68	3.09	14.23
Total	25.63	42.36	22.61	9.39	100.00
Panel B: Total sample (n=14,128)					
Firm size	Micro	Small	Medium	Large	Total
Maturity level					
Low	18.71	12.77	4.41	1.47	37.37
Medium low	12.56	8.49	3.94	1.99	26.97
Medium high	3.57	7.04	5.77	3.63	20.00
High	2.10	4.12	4.85	4.59	15.66
Total	36.94	32.41	18.96	11.69	100.00

Notes: Total indicates the row totals and column totals respectively.

Table 8: Distribution across key characteristics (in percentage shares)

	Key characteristics	Not part of final sample	Part of final sample	Pr(T>t)	Total sample
Maturity level	Low	0.382	0.367	0.053	0.374
	Medium low	0.269	0.270	0.943	0.270
	Medium high	0.174	0.221	0.000	0.200
	High	0.175	0.142	0.000	0.157
Firm size	Micro (2-9 employees)	0.511	0.256	0.000	0.369
	Small (10-49 employees)	0.199	0.424	0.000	0.324
	Medium (50-199 employees)	0.144	0.226	0.000	0.190
	Large (200 and more employees)	0.146	0.094	0.000	0.117
Sector	Manufacturing	0.161	0.209	0.000	0.188
	Energy & Water supply	0.016	0.017	0.593	0.017
	Construction	0.039	0.053	0.000	0.047
	Wholesale and retail trade	0.170	0.192	0.001	0.182
	Transportation and storage	0.070	0.064	0.130	0.066
	Accommodation and food serving	0.041	0.030	0.001	0.035
	Information and communication	0.061	0.105	0.000	0.086
	Financial	0.045	0.000	0.000	0.020
	Real estate	0.034	0.000	0.000	0.015
	Other specialised business services	0.158	0.148	0.131	0.152
	Renting and other business support	0.076	0.142	0.000	0.113
	Healthcare	0.129	0.039	0.000	0.079
	Number of observations	6,270	7,858		14,128

Notes: Percentage shares (when multiplied by 100) of key characteristics if firm is not part of the final subsample (column 1) and if firm is part of the final subsample (column 2). Column 3 returns the p-value of a two-sided t-test for the equality of means. The null hypothesis is equality of means, the alternative hypothesis is that the means significantly differ from each other.

Table 9: Estimated probabilities of reporting incidents by firm size (all results)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Dependent variable	Micro		Small		Medium		Large		All	
Firm reported at least 1 incident (dummy)	coeff.	se	coeff.	se	coeff.	se	coeff.	se	coeff.	se
Maturity level: Medium low	0.034**	(0.014)	0.033*	(0.019)	0.041	(0.028)	0.040	(0.043)	0.042***	(0.010)
Maturity level: Medium high	0.118***	(0.025)	0.070***	(0.021)	0.034	(0.026)	0.083**	(0.039)	0.103***	(0.012)
Maturity level: High	0.081***	(0.031)	0.009	(0.026)	-0.048	(0.029)	0.043	(0.040)	0.032**	(0.014)
log(firm size)	0.053***	(0.010)	0.034**	(0.013)	-0.011	(0.021)	0.018	(0.014)	0.057***	(0.003)
Orders received via website or app (=1)	0.128***	(0.019)	0.066***	(0.019)	0.037	(0.023)	0.051*	(0.028)	0.084***	(0.011)
Supply chain management system used (=1)			0.033	(0.021)	0.010	(0.022)	0.051**	(0.024)		
CRM used (=1)			0.084***	(0.018)	0.078***	(0.022)	0.000	(0.027)		
ERP software used (=1)			0.044**	(0.018)	0.070***	(0.025)	0.045	(0.031)		
Securty patching: automatic (=1)	0.148***	(0.014)	0.183***	(0.020)	0.204***	(0.035)	0.147**	(0.057)	0.185***	(0.011)
Securty patching: manually (=1)	0.180***	(0.017)	0.231***	(0.022)	0.227***	(0.036)	0.197***	(0.057)	0.227***	(0.012)
Product innovation in 2016 (=1)	0.129***	(0.023)	0.015	(0.021)	0.056**	(0.023)	0.037	(0.027)	0.065***	(0.012)
Process innovation in 2016 (=1)	0.059**	(0.025)	0.076***	(0.020)	0.075***	(0.022)	0.020	(0.027)	0.081***	(0.011)
Offered IT-training to IT-specialists in 2016 (=1)			-0.021	(0.026)	0.012	(0.024)	0.009	(0.031)		
Offered IT-training to other employees in 2016 (=1)			0.059**	(0.023)	0.047**	(0.023)	0.019	(0.027)		
sector = 2, Energy & Water supply	-0.015	(0.048)	0.010	(0.053)	0.032	(0.072)	0.038	(0.080)	-0.000	(0.030)
sector = 3, Construction	0.006	(0.030)	0.041	(0.034)	0.082	(0.051)	0.102*	(0.061)	0.038*	(0.020)
sector = 4, Wholesale and retail trade	0.010	(0.019)	0.027	(0.024)	-0.018	(0.030)	-0.017	(0.042)	0.004	(0.013)
sector = 5, Transportation and storage	-0.036	(0.024)	0.043	(0.031)	-0.059	(0.045)	0.032	(0.053)	-0.018	(0.017)
sector = 6, Accommodation and food serving	-0.061**	(0.030)	-0.040	(0.040)	-0.026	(0.053)	-0.202**	(0.101)	-0.074***	(0.022)
sector = 7, Information and communication	-0.023	(0.026)	-0.053*	(0.030)	-0.103***	(0.039)	-0.132**	(0.063)	-0.051***	(0.016)
sector = 8, Financial	-0.001	(0.043)	-0.027	(0.053)	-0.066	(0.077)	0.062	(0.088)	-0.024	(0.029)
sector = 9, Real estate	0.088**	(0.043)	0.020	(0.071)	0.006	(0.093)	0.039	(0.110)	0.059*	(0.033)
sector = 10, Other specialised business services	0.047**	(0.021)	0.031	(0.024)	0.021	(0.035)	-0.012	(0.051)	0.031**	(0.014)
sector = 11, Renting and other business support	-0.022	(0.026)	-0.028	(0.028)	0.018	(0.030)	0.022	(0.042)	-0.017	(0.015)
sector = 12, Healthcare	0.034	(0.027)	0.032	(0.034)	0.163***	(0.047)	0.124***	(0.038)	0.046***	(0.016)
Observations	5,219		4,579		2,679		1,651		14,128	
R-squared	0.104		0.098		0.082		0.059		0.157	
Joint significance security measures (p-value)	0.000		0.000		0.000		0.001		0.000	
Joint significance sector dummies (p-value)	0.004		0.073		0.001		0.001		0.000	
Joint significance innovation variables (p-value)	0.000		0.000		0.000		0.140		0.000	
Joint significance maturity dummies (p-value)	0.000		0.005		0.004		0.152		0.000	

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Not all questions were asked to all firms, hence the empty cells. The estimations of the total sample take this into account. Reference categories: Low maturity level and security patching (category: not applicable), sector 1 (industry).

Table 10: Profitability and maturity levels by firm size (all coefficients)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Dependent variable	Micro		Small		Medium		Large		All	
Profitability in 2016: Net income/ Net revenue	coeff.	se	coeff.	se	coeff.	se	coeff.	se	coeff.	se
Maturity level: Medium low	-0.004	(0.009)	0.003	(0.005)	0.009	(0.006)	0.002	(0.010)	0.002	(0.004)
Maturity level: Medium high	-0.015	(0.013)	0.007	(0.005)	-0.009	(0.007)	-0.018*	(0.010)	-0.003	(0.004)
Maturity level: High	0.026*	(0.015)	0.001	(0.008)	-0.002	(0.008)	-0.007	(0.012)	0.004	(0.005)
log(firm size)	0.007	(0.004)	-0.003	(0.002)	-0.008***	(0.002)	-0.003	(0.002)	-0.003***	(0.001)
Orders received via website or app (=1)	-0.024***	(0.009)	-0.004	(0.005)	-0.007	(0.006)	-0.006	(0.010)	-0.009**	(0.004)
Supply chain management system used (=1)			-0.003	(0.006)	0.001	(0.006)	0.002	(0.009)		
CRM used (=1)			-0.004	(0.005)	0.009	(0.006)	0.001	(0.008)		
ERP software used (=1)			-0.001	(0.005)	0.001	(0.007)	-0.017*	(0.010)		
Security patching: automatic (=1)	-0.015	(0.011)	-0.007	(0.006)	0.004	(0.008)	0.002	(0.010)	-0.006	(0.005)
Security patching: manually (=1)	-0.007	(0.012)	-0.001	(0.006)	0.008	(0.009)	-0.010	(0.011)	-0.002	(0.005)
Product innovation in 2016 (=1)	-0.009	(0.011)	-0.000	(0.006)	0.003	(0.007)	0.013	(0.011)	0.002	(0.004)
Process innovation in 2016 (=1)	0.010	(0.012)	-0.001	(0.006)	-0.009	(0.006)	-0.004	(0.011)	-0.001	(0.004)
Offered IT-training to IT-specialists in 2016 (=1)			-0.003	(0.008)	0.008	(0.007)	0.018	(0.011)		
Offered IT-training to other employees in 2016 (=1)			0.006	(0.007)	0.003	(0.007)	0.004	(0.010)		
sector = 2, Energy & Water supply	-0.006	(0.036)	-0.018	(0.018)	0.025	(0.026)	-0.022	(0.025)	-0.008	(0.014)
sector = 3, Construction	0.014	(0.017)	-0.018**	(0.008)	-0.025**	(0.010)	-0.005	(0.016)	-0.009	(0.006)
sector = 4, Wholesale and retail trade	-0.012	(0.010)	-0.018***	(0.006)	-0.015*	(0.008)	-0.018	(0.014)	-0.015***	(0.004)
sector = 5, Transportation and storage	0.016	(0.017)	-0.004	(0.008)	-0.025**	(0.011)	-0.001	(0.014)	-0.003	(0.006)
sector = 6, Accommodation and food serving	-0.093**	(0.045)	0.007	(0.013)	0.010	(0.017)	-0.032	(0.047)	-0.005	(0.011)
sector = 7, Information and communication	-0.012	(0.015)	0.008	(0.009)	0.001	(0.012)	-0.027	(0.032)	0.000	(0.006)
sector = 10, Other specialised business services	0.010	(0.013)	0.006	(0.007)	0.009	(0.010)	-0.025	(0.022)	0.007	(0.006)
sector = 11, Renting and other business support	0.009	(0.014)	-0.014*	(0.007)	-0.014	(0.009)	0.000	(0.015)	-0.006	(0.005)
sector = 12, Healthcare	0.049**	(0.024)	0.023*	(0.013)	0.000	(0.016)	-0.041**	(0.019)	0.006	(0.009)
Observations	2,014		3,329		1,777		738		7,858	
R-squared	0.019		0.013		0.028		0.045		0.007	
Joint significance maturity levels (p-value)	0.140		0.561		0.053		0.196		0.504	
Joint significance patching vars (p-value)	0.321		0.317		0.575		0.355		0.276	
Joint significance sector dummies (p-value)	0.041		0.000		0.018		0.130		0.002	

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Not all questions are asked to all firms, hence the empty cells. Reference categories: Low maturity level, security patching (category; not applicable), sector 1 (industry).

Table 11: Estimated probabilities of reporting incidents by firm size (alternative maturity level)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Dependent variable	Micro		Small		Medium		Large		All	
Firm reported at least 1 incident (dummy)	coeff.	se	coeff.	se	coeff.	se	coeff.	se	coeff.	se
Maturity level: Medium low	0.123***	(0.016)	0.107***	(0.020)	0.193***	(0.035)	0.194***	(0.070)	0.150***	(0.011)
Maturity level: Medium high	0.180***	(0.021)	0.148***	(0.022)	0.181***	(0.036)	0.188***	(0.068)	0.189***	(0.012)
Maturity level: High	0.112***	(0.028)	0.076***	(0.028)	0.056	(0.039)	0.154**	(0.070)	0.108***	(0.015)
log(firm size)	0.047***	(0.010)	0.030**	(0.013)	-0.013	(0.021)	0.019	(0.014)	0.052***	(0.003)
Orders received via website or app (=1)	0.124***	(0.019)	0.065***	(0.019)	0.036	(0.023)	0.051*	(0.028)	0.081***	(0.011)
Supply chain management system used (=1)			0.026	(0.021)	0.010	(0.021)	0.057**	(0.024)		
CRM used (=1)			0.076***	(0.018)	0.068***	(0.022)	-0.003	(0.027)		
ERP software used (=1)			0.033*	(0.018)	0.053**	(0.025)	0.046	(0.032)		
Security patching: automatic (=1)	0.114***	(0.014)	0.155***	(0.020)	0.169***	(0.036)	0.120**	(0.057)	0.143***	(0.011)
Security patching: manually (=1)	0.151***	(0.016)	0.205***	(0.022)	0.189***	(0.037)	0.167***	(0.058)	0.187***	(0.012)
Product innovation in 2016 (=1)	0.118***	(0.023)	0.012	(0.021)	0.059***	(0.023)	0.040	(0.027)	0.061***	(0.011)
Process innovation in 2016 (=1)	0.048*	(0.025)	0.069***	(0.020)	0.068***	(0.022)	0.020	(0.027)	0.071***	(0.011)
Offered IT-training to IT-specialists in 2016 (=1)			-0.023	(0.026)	0.016	(0.024)	0.009	(0.032)		
Offered IT-training to other employees in 2016 (=1)			0.054**	(0.023)	0.051**	(0.023)	0.020	(0.028)		
sector = 2, Energy & Water supply	-0.028	(0.047)	0.007	(0.053)	0.033	(0.073)	0.048	(0.079)	-0.001	(0.030)
sector = 3, Construction	0.009	(0.030)	0.049	(0.034)	0.083*	(0.049)	0.101*	(0.061)	0.044**	(0.020)
sector = 4, Wholesale and retail trade	0.008	(0.019)	0.030	(0.025)	-0.008	(0.030)	-0.016	(0.042)	0.007	(0.013)
sector = 5, Transportation and storage	-0.036	(0.024)	0.045	(0.031)	-0.067	(0.044)	0.035	(0.053)	-0.013	(0.017)
sector = 6, Accommodation and food serving	-0.056*	(0.030)	-0.028	(0.039)	-0.026	(0.053)	-0.220**	(0.101)	-0.065***	(0.022)
sector = 7, Information and communication	-0.038	(0.026)	-0.049*	(0.030)	-0.091**	(0.039)	-0.122*	(0.063)	-0.053***	(0.016)
sector = 8, Financial	-0.016	(0.043)	-0.034	(0.053)	-0.055	(0.077)	0.072	(0.087)	-0.030	(0.029)
sector = 9, Real estate	0.078*	(0.043)	0.003	(0.070)	-0.000	(0.093)	0.029	(0.107)	0.047	(0.032)
sector = 10, Other specialised business services	0.036*	(0.021)	0.025	(0.024)	0.024	(0.035)	0.000	(0.051)	0.025*	(0.014)
sector = 11, Renting and other business support	-0.023	(0.025)	-0.024	(0.028)	0.028	(0.030)	0.029	(0.042)	-0.014	(0.015)
sector = 12, Healthcare	0.006	(0.027)	0.030	(0.034)	0.149***	(0.046)	0.124***	(0.038)	0.037**	(0.016)
Observations	5,219		4,579		2,679		1,651		14,128	
R-squared	0.118		0.105		0.097		0.062		0.169	
Joint significance security measures (p-value)	0.000		0.000		0.000		0.006		0.000	
Joint significance sector dummies (p-value)	0.019		0.111		0.002		0.002		0.000	
Joint significance innovation variables (p-value)	0.000		0.000		0.000		0.111		0.000	
Joint significance maturity dummies (p-value)	0.000		0.000		0.000		0.021		0.000	

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Not all questions were asked to all firms, hence the empty cells. The estimations of the total sample take this into account. Alternative maturity level refers to the count of security measures divided into four levels. Reference categories: Low maturity level, security ppatching (category: not applicable), sector 1 (industry).

Table 12: Estimated profitability by firm size (all coefficients, alternative maturity level)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Dependent variable	Micro		Small		Medium		Large		All	
Profitability in 2016: Net income/ Net revenue	coeff.	se	coeff.	se	coeff.	se	coeff.	se	coeff.	se
Maturity level: Medium low	-0.007	(0.010)	-0.001	(0.005)	0.008	(0.007)	0.019	(0.012)	-0.000	(0.004)
Maturity level: Medium high	-0.016	(0.012)	0.007	(0.006)	0.001	(0.008)	0.006	(0.011)	-0.001	(0.005)
Maturity level: High	0.027*	(0.015)	0.009	(0.008)	0.017*	(0.009)	0.012	(0.013)	0.012**	(0.005)
log(firm size)	0.008*	(0.005)	-0.003	(0.002)	-0.008***	(0.002)	-0.004	(0.002)	-0.003***	(0.001)
Orders received via website or app (=1)	-0.024***	(0.009)	-0.004	(0.005)	-0.006	(0.006)	-0.004	(0.010)	-0.009**	(0.004)
Security patching: automatic (=1)	-0.014	(0.012)	-0.007	(0.006)	0.002	(0.008)	-0.001	(0.010)	-0.006	(0.005)
Security patching: manually (=1)	-0.005	(0.013)	-0.001	(0.006)	0.007	(0.009)	-0.013	(0.011)	-0.002	(0.005)
Product innovation in 2016 (=1)	-0.009	(0.011)	-0.001	(0.006)	0.003	(0.007)	0.013	(0.011)	0.001	(0.004)
Process innovation in 2016 (=1)	0.009	(0.012)	-0.001	(0.006)	-0.010*	(0.006)	-0.002	(0.011)	-0.002	(0.004)
Supply chain management system used (=1)			-0.004	(0.006)	0.000	(0.006)	0.001	(0.009)		
CRM used (=1)			-0.004	(0.005)	0.008	(0.006)	-0.000	(0.009)		
ERP software used (=1)			-0.000	(0.005)	-0.000	(0.007)	-0.019*	(0.010)		
Offered IT-training to IT-specialists in 2016 (=1)			-0.004	(0.008)	0.006	(0.007)	0.019	(0.011)		
Offered IT-training to other employees in 2016 (=1)			0.006	(0.007)	0.001	(0.007)	0.004	(0.010)		
sector = 2, Energy & Water supply	-0.006	(0.036)	-0.019	(0.018)	0.026	(0.026)	-0.023	(0.024)	-0.009	(0.014)
sector = 3, Construction	0.014	(0.017)	-0.018**	(0.008)	-0.024**	(0.010)	-0.002	(0.016)	-0.009	(0.006)
sector = 4, Wholesale and retail trade	-0.011	(0.011)	-0.018***	(0.006)	-0.015*	(0.008)	-0.017	(0.014)	-0.016***	(0.004)
sector = 5, Transportation and storage	0.016	(0.017)	-0.005	(0.008)	-0.026**	(0.011)	-0.000	(0.014)	-0.003	(0.006)
sector = 6, Accommodation and food serving	-0.092**	(0.045)	0.007	(0.013)	0.011	(0.017)	-0.034	(0.046)	-0.005	(0.011)
sector = 7, Information and communication	-0.015	(0.015)	0.006	(0.009)	-0.001	(0.012)	-0.028	(0.030)	-0.002	(0.006)
sector = 10, Other specialised business services	0.010	(0.013)	0.005	(0.007)	0.009	(0.010)	-0.024	(0.022)	0.006	(0.006)
sector = 11, Renting and other business support	0.009	(0.014)	-0.014*	(0.007)	-0.014	(0.009)	0.002	(0.015)	-0.006	(0.005)
sector = 12, Healthcare	0.050**	(0.024)	0.022*	(0.013)	0.000	(0.016)	-0.039**	(0.019)	0.006	(0.009)
Observations	2,014		3,329		1,777		738		7,858	
R-squared	0.021		0.013		0.028		0.042		0.008	
Joint significance maturity levels (p-value)	0.035		0.365		0.143		0.322		0.022	
Joint significance patching vars (p-value)	0.359		0.284		0.553		0.333		0.232	
Joint significance sector dummies (p-value)	0.034		0.000		0.016		0.107		0.002	

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Alternative maturity level refers to the count of security measures divided into four levels. Same reference categories apply as in previous specifications.

Table 13: Estimated probabilities for different types of incidents (full sample)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Dependent variables:	Data leaks				Data destr.				System failure			
Type of incident (binary)	breach		internal		IT		attack		IT		attack	
	coeff.	se	coeff.	se	coeff.	se	coeff.	se	coeff.	se	coeff.	se
Maturity level: Medium low	-0.004	(0.003)	-0.010***	(0.004)	0.004	(0.006)	-0.001	(0.006)	0.032***	(0.010)	0.000	(0.007)
Maturity level: Medium high	-0.007*	(0.004)	-0.015***	(0.005)	0.006	(0.007)	0.019**	(0.009)	0.088***	(0.012)	0.030***	(0.009)
Maturity level: High	0.021***	(0.006)	0.030***	(0.007)	0.009	(0.009)	-0.010	(0.010)	0.033**	(0.014)	0.043***	(0.011)
log (firm size)	0.004***	(0.001)	0.017***	(0.001)	0.010***	(0.002)	0.030***	(0.002)	0.043***	(0.003)	0.019***	(0.002)
Orders received via website or app (=1)	0.017***	(0.004)	0.023***	(0.005)	0.023***	(0.007)	0.025***	(0.008)	0.075***	(0.011)	0.060***	(0.008)
Security patching: automatic (=1)	0.002	(0.003)	0.005	(0.004)	0.031***	(0.005)	0.032***	(0.006)	0.159***	(0.010)	0.030***	(0.007)
Security patching: manually (=1)	0.004	(0.004)	0.010**	(0.004)	0.040***	(0.006)	0.060***	(0.007)	0.197***	(0.011)	0.052***	(0.008)
Product innovation in 2016 (=1)	0.014***	(0.004)	0.025***	(0.006)	0.019***	(0.007)	0.019**	(0.009)	0.057***	(0.012)	0.031***	(0.009)
Process innovation in 2016 (=1)	0.000	(0.004)	0.014***	(0.005)	0.038***	(0.007)	0.044***	(0.008)	0.059***	(0.012)	0.035***	(0.009)
sector = 2, Energy & Water supply	0.022*	(0.014)	0.055***	(0.017)	0.027	(0.020)	0.014	(0.023)	-0.010	(0.031)	-0.009	(0.022)
sector = 3, Construction	0.004	(0.006)	0.019**	(0.008)	0.021*	(0.012)	0.045***	(0.015)	0.014	(0.020)	0.022	(0.014)
sector = 4, Wholesale and retail trade	0.006	(0.004)	0.014***	(0.005)	-0.004	(0.008)	-0.013	(0.009)	0.002	(0.013)	0.002	(0.009)
sector = 5, Transportation and storage	0.006	(0.006)	0.010	(0.006)	0.008	(0.010)	0.003	(0.012)	-0.010	(0.017)	-0.026**	(0.011)
sector = 6, Accommodation and food serv.	-0.000	(0.007)	0.007	(0.008)	0.000	(0.012)	-0.037***	(0.013)	-0.046**	(0.021)	-0.044***	(0.013)
sector = 7, Information and communic.	-0.004	(0.005)	0.015**	(0.007)	-0.010	(0.010)	-0.064***	(0.010)	-0.050***	(0.016)	-0.006	(0.012)
sector = 8, Financial	0.007	(0.011)	0.035**	(0.015)	-0.028*	(0.015)	-0.013	(0.020)	-0.035	(0.029)	0.001	(0.021)
sector = 9, Real estate	-0.002	(0.009)	0.044***	(0.015)	0.007	(0.019)	-0.010	(0.021)	0.031	(0.033)	-0.018	(0.021)
sector = 10, Other spec. bus. services	0.007	(0.004)	0.035***	(0.006)	0.010	(0.008)	-0.009	(0.009)	0.018	(0.014)	0.008	(0.010)
sector = 11, Renting and other bus. supp.	0.009*	(0.005)	0.002	(0.006)	-0.008	(0.009)	-0.041***	(0.010)	-0.011	(0.015)	0.005	(0.011)
sector = 12, Healthcare	0.003	(0.005)	0.082***	(0.009)	-0.020**	(0.009)	-0.032***	(0.011)	0.040**	(0.017)	-0.028**	(0.011)
Observations	14,128		14,128		14,128		14,128		14,128		14,128	
R-squared	0.014		0.062		0.027		0.062		0.106		0.051	
Joint signif. maturity dummies (p-value)	0.000		0.000		0.697		0.028		0.000		0.000	
Joint signif. patching vars (p-value)	0.567		0.067		0.000		0.000		0.000		0.000	
Joint signif. sector dummies (p-value)	0.431		0.000		0.012		0.000		0.000		0.000	
Joint signif. innovation vars (p-value)	0.001		0.000		0.000		0.000		0.000		0.000	

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1
Notes: Data destr. refers to data destruction and mutilation. Questions on ICT training and software use were not asked to all firms and are hence excluded from this analysis. Reference categories: low maturity level, security patching (category: not applicable), sector 1.