Empirically Evaluating the Effect of Cybersecurity Precautions on Incidents in Israeli Enterprises

Neil Gandal
Berglas School of Economics
Tel Aviv University, Israel
gandal@post.tau.ac.il

Tyler Moore
School of Cyber Studies
The University of Tulsa, USA
tyler-moore@utulsa.edu

Michael Riordan
Department of Economics
Columbia University, USA
mhr21@columbia.edu

Noa Barnir
Berglas School of Economics
Tel Aviv University, Israel
noabarnir@gmail.com

Abstract

Empirical evidence that connects firm investment in cybersecurity defenses to the likelihood of being attacked has been very hard to come by. The Israel National Cyber Directorate (INCD) and the Israeli Central Bureau of Statistics (CBS) recently surveyed Israeli firms about their ICT operations including cyber defenses and attacks. Using the survey, in this paper, we empirically examine whether security precautions adopted by firms do in fact reduce the chances of being attacked. We find that using four basic security precautions reduces the probability of experiencing a cyber incident from 69% to 21%.

1 Introduction

Cybersecurity is widely recognized as essential to the functioning of modern economies. Firms and governments are spending ever greater sums on countermeasures designed to mitigate risks, yet we know surprisingly little about which of these investments, if any, reduce the risk of experiencing a cyber incident, and by how much. Estimates of the financial harm resulting from successful attacks vary by multiple orders of magnitude, when they are available at all. And the threats organizations face are often highly correlated, since a single attack can affect hundreds or thousands of firms that utilize the same vulnerable components.

Why is this? Firms focus on frameworks such as NIST CSF, COBIT and ISO 27001 that emphasize the process of implementing various controls, without regard to their effectiveness. By codifying best practices, the frameworks steer organizations to measure their compliance to the framework rather than the effectiveness of security achieved. This is understandable since the relationship between making security investments and avoiding cyber incidents depends on multiple factors, including target value and attacker strategy, each of which exhibits randomness. Consequently, drawing conclusions from a single firm's experience is quite problematic.

The paper is an empirical examination of how security precautions undertaken by enterprises affect the likelihood of experiencing a cyber incident. This paper uses a remarkably detailed firm-level data

Workshop on the Economics of Information Security (WEIS) 2022, Tulsa, Oklahoma, USA, June 21–22, 2022

set from an ICT use and cybersecurity survey that was undertaken in 2020-2021 by the Israel National Cyber Directorate (INCD) and the Israeli Central Bureau of Statistics (CBS). In our assessment, this is by far the most comprehensive firm-level cybersecurity survey ever undertaken at a national level.

A huge problem with empirical work on this topic is that the timing of security investments is unknown. Indeed, as shown in Table 2, the survey data we examine exhibits a positive correlation between investment in security precautions and incidents. This is because many such investments are made *ex post*, i.e., after a firm has suffered a cyberattack/incident. Thus, there is an endogeneity issue.

The survey enables us to overcome this obstacle and examine the relationship between security precautions undertaken by enterprises and the likelihood of experiencing a cyber incident because the survey asked two key questions:

- Is your enterprise aware of the cyber directives and instructions (e.g. the Cyber Defense Methodology for an Organization) published by the Israeli National Cyber Directorate (INCD)?
- For those enterprises that were aware of the cyber directives and instructions, a follow up question was asked about whether there was full implementation of the directives.

The CBS received responses to the 2020 survey from firms beginning in July 2020 and ending in April 2021. The survey specifically asks the following: "Did your enterprise have to handle any cyber security attacks over the past 12 months."

Since the document was issued in June 2017, it is very likely that firms for the most part became aware of the document and responded to it (by implementing or not implementing the guidelines) prior to the 12 month period (2019-2020) for which incidents were reported in the survey. This is because implementation of he four basic cybersecurity precautions we employ in this paper is simple and fairly straightforward and takes a relatively short amount of time. (See below for the four basic precautions.)

These two questions above thus address the timing issue of when precautions were undertaken and enable the use of the second question as an instrumental variable. In other words, firms that implemented the directives thus took security precautions did so prior to the 2019–2020. We interpret the instrument as an indicator of whether the organization is alert and intentionally vigilant to risks of cyber attacks. Empirically, this variable works as an instrument for security precautions since it is positively correlated with different measures of security precautions and negatively correlated with incidents.

When we run a (probit) regression of security precautions and firm characteristics on whether the firm experienced a cyber incident, without instrumenting for precautions, we find that the estimated coefficient on security precautions is (not surprisingly) positive and statistically significant. This is because many firms likely adopted security measures after suffering a cyber incident. Once we instrument for security precautions using the "implementation" variable, the estimated coefficient on security precautions is negative and statistically significant. This means that employing precautions indeed reduces the probability of suffering a cyber security incident.

We find that use of four basic cybersecurity precautions significantly reduces the likelihood of experiencing a cyber incident for Israeli firms. The following are the four basic cybersecurity precautions.

- Strong password policy (e.g. periodical password reset, minimum password length policy, requiring combination of letters, numbers and characters)
- Keeping systems up-to-date per manufacturer's recommendation, or at a more frequent rate
- Having multiple updated backup copies, with one offsite and usually offline
- Means of detecting and responding to malware at endpoints and servers (e.g. antivirus system)

Our results are probably biased downward, that is employing the four basic security controls is

A specification test concludes that the instrument is indeed exogenous.

The survey asks specifically about twenty different precautions.See Figure 3.

more likely to reduce incidents than we estimate. This is because, like all surveys, the CBS survey relies on self-reports of cyber incidents. Thus firms that are less invested in cybersecurity may not even be aware that they have suffered such an attempt.

Overall in our data set (993 firms), 46 percent suffered a cybersecurity incident in the twelve months preceding the 2020-2021 survey. To get some sense of the magnitude of the results, for firms with significant revenues and firms with a large number of workers, but without a significant Internet presence and not in high risk industries, the use of four key basic security precautions reduces the probability of a cybersecurity incident from 69% to 21%. These differences are large and suggest that firms that employ these four important basic security precautions greatly reduce the risk of suffering a security incident.

2 Background and Prior Work

Few would dispute that cyber risk is a very serious problem for the global economy and for society. But there is a "disconnect" between acknowledgement of the problem and action to address the problem. What is the relationship between vulnerabilities, preventive measures, and security incidents, like being targeted by ransomware or experiencing a data breach? Surprisingly little is known about the relationship among these variables, and even less is known at the micro level, that is, at the level of the firm.

One key reason why this knowledge gap exists is that the firms themselves do not try to measure these relationships. Based on semi-structured interviews with 40 executives in charge of cybersecurity, Moore et al. found that, broadly speaking, organizations do not compute return on investment (ROI) by measuring the reduction in expected losses from experiencing incidents due to the adoption of security controls [4]. Instead, most companies had adopted frameworks of one kind (e.g., the NIST Cybersecurity Framework, COBIT, SANS Critical Controls). These frameworks enumerate available controls and levels that can be achieved by adopting them. While the frameworks direct investments, they do not explicitly evaluate how taking particular precautions affects the security level of their organization, and ultimately whether those precautions make a breach less likely to occur.

But why would organizations spend huge sums on defenses without determining how such spending improves their security level? It turns out it can be very hard to establish how and whether investments in security controls successfully stop attacks.

First, there is an inherent information asymmetry about the quality of security products and services [1, 2]. This makes it difficult for firms to determine what defenses are more effective, which makes establishing the link between security investment and outcomes that much harder to establish. Second, the relationship between spending on security controls and expected losses is not direct. Instead, it is mediated by multiple factors, including the effectiveness of controls, varying attacker effort, and the value of a target. Third, we lack reliable estimates of the costs resulting from cyber attacks.

Fortunately, the research community and industry have begun to fill in some of these gaps. For a comprehensive theoretical treatment, we refer the reader to Woods and Böhme's theoretical systemization [6]; we describe some of the most relevant work here. Liu et al. gather publicly-observable data on organizations' network misconfigurations and then construct a classifier to predict whether a data breach is subsequently reported. Surprisingly, these crude external measures of security levels were found to be predictive of subsequent adverse outcomes [3]. Sarabi et al. [5] employed a similar approach, but gathered additional data on business sectors and breach types in order to identify the

Very similar results (73% vs. 20%) are obtained when we use "whether the firm employed more than mean number of cyber security precautions of other firms in the data set" as the cyber security precautions variable.

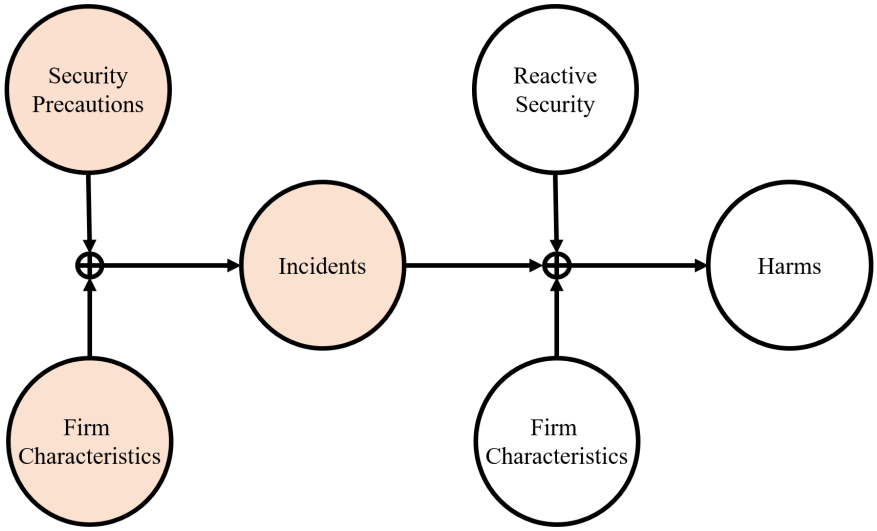

Figure 1: Causal model relating security precautions to incidents and harms [6] (shaded circles indicate the relationships evaluated in this paper).

relative risk of incidents for different industries. Furthermore, a number of risk-rating services have appeared (e.g., offerings from SecurityScorecard, QuadMetrics, and BitSight) that commercialize the results found by researchers.

These cases showed that, while the metrics can often predict breaches, the underlying causal factors remain unknown. In other words, we are beginning to learn more about the relationship between the security level and the likelihood of experiencing a breach, but we do not know *why* observable external metrics are associated with subsequently experiencing a breach. Without having established causality, it is not known whether taking concrete steps to improve security would actually reduce risk (and by how much), or if some other unobservable factor is actually driving differences in risk.

Our paper takes a step towards establishing a causal link between cybersecurity investments and outcomes. We follow an adaptation of the causal model presented by Woods and Böhme [6] and laid out in Figure 1. The survey questions cover the relationships identified by the shaded circles. The survey reports characteristics of Israeli firms, the security precautions they claim to adopt, and the experience of cybersecurity incidents. While the survey does include questions about the harms resulting from incidents (as represented in the unshaded right half of the figure), we do not consider them in this paper.

3 Dataset Description

In 2020-2021, the Israeli National Cyber Directorate (INCD), in conjunction with the Israeli Central Bureau of Statistics (CBS) constructed and implemented the most comprehensive survey regarding cybersecurity even undertaken at the level of the firm. The survey, entitled "Survey of Information and Communication Technologies Usage and Cyber Security in Businesses 2020", includes detailed questions about the types of security controls adopted by organizations and whether cybersecurity attacks experienced, as well as questions about Internet use, ecommerce, and other firms characteristics.

The survey population is drawn from the 29 825 Israeli private sector businesses with more than 10 employees, excluding the following industries: agriculture, finance, diamonds, public and local

10.8 Did your enterprise have to handle any cyber security attacks over the past 12 months? (Handling an attack can be with or without damage or loss to the enterprise. An attack can be financial, image related or as a breach of employees' privacy)
Please check ✓ all relevant answers: ***(Incident)***

	Yes – with damage or loss	Yes – without damage or loss	No
10.8.1 Attempts to deny access to the enterprises' data and communication systems (e.g. ransomware*), failure of software or hardware			
10.8.2 Attempts to destroy or corrupt data (e.g. inserting malware or unauthorized access)			
10.8.3 Attempts to expose classified information (e.g. pharming,* phishing,* actions of employees, whether unintentional or malicious)			

Figure 2: Sample survey question dealing with cyber incidents experienced by the firm.

administration, education, health, households and non-governmental organizations. 2 500 of these firms received the survey, of which 2 020 (81%) responded. Firms were selected at random in layers by industry, corporate structure (multinational and domestic), and firm size.

The survey was conducted from July 2020 to March 2021, referring to business activity in 2020. The carefully constructed survey is remarkable, not only because of the number of firms that have responded, but also for the incredibly important detailed information security questions within. In our assessment, this is the most comprehensive (national) survey ever undertaken.

One of the authors (Barnir) accessed anonymized survey response data in a secure room at the Central Bureau of Statistics. Data remains with the CBS; only the outputs of the statistical scripts that were cleared for public disclosure are available to authors.

A key question is whether the firm had to handle any cyber attacks (or incidents) in the past 12 months. Figure 2 shows how the question was asked in the survey.

Additionally, firms were asked whether any of twenty different security precautions were implemented by the enterprise? (For each measure, the firm needs to answer yes or no.) See Figure 3.

We also have extensive data on firm characteristics including size, ICT use, and industry. Thus for firm characteristics, we will evaluate how technological dependence, employee headcount, industry headcount, ecommerce presence, etc. affects susceptibility to compromise. This is important because we will be able to shed light on (for example) which sectors are more likely to be targeted and successfully compromised.

Given the rich data and the availability of an exogenous instrumental variable, the INCD/CBS survey enables us to measure the impact of firm characteristics (FC) and security precautions (P)) on the likelihood of compromise/incidents (I).

Global Statistics from INCD/CBS Survey Fully 993 firms indicated that they were aware of the directives and instructions from the INCD. These firms comprise our dataset for analysis. We now report some global statistics before we formally begin to analyze the data.

- 46% of the enterprises reported that they had to handle a cyberattack or incident in the last twelve months.
- Among firms with 250 or more employees, 55% reported that they hand to handle a cyberattack

10.5 Which of the following security measures has been implemented by the enterprise? Please check √ the appropriate answer in each row.

		Yes	No
10.5.1	Strong password policy (e.g. periodical password reset, minimum password length policy, requiring combination of letters, numbers and characters)		
10.5.2	Keeping systems up-to-date per manufacturer's recommendation, or at a more frequent rate		
10.5.3	Biometric identifiers (e.g. fingerprint, facial or voice recognition)		
10.5.4	Data, files and email encryption		
10.5.5	Having multiple updated backup copies, with one offsite and usually offline		
10.5.6	Control over access to enterprises' network, by user filtering		
10.5.7	The enterprise has a virtual private network (VPN) to transfer data safely through public domains		
10.5.8	Conducting a periodic survey on cyber security risks		
10.5.9	Security checks (e.g. system invasion attempts, warning system checks, security procedure assessments, etc.)		
10.5.10	Means of detecting and responding to malware at endpoints and servers (e.g. antivirus system)		
10.5.11	File typing of attachments (e.g. DOC, DOCX, PDF) to be accepted from outside the enterprise ("Whitelist")		
10.5.12	Authentication of Sender ID (DMARC) for handling spam		
10.5.13	Security protection services for the enterprises' email systems, including: detecting and responding to spam and malware (e.g. SEG, Mail Relay)		
10.5.14	URL filtering by means of firewall, Secure Web Gateway (SWG) or cloud-based security software		
10.5.15	User malware download prevention (e.g. Firewall, SWG – Secure Web Gateway) or cloud-based security software		
10.5.16	Use of Multi Factor Authentication		
10.5.17	Periodic recovery tests to ensure proper recovery if needed		
10.5.18	Use of operating systems and applications which are under full manufacturer's support (not in "end of life" state)		
10.5.19	Specifications regarding disaster recovery protocols (e.g. RTO, RPO)		
10.5.20	Cyber insurance		

Figure 3: Sample survey question dealing with security precautions adopted by the firm.

or incident in the last twelve months.

- There is a particularly high incidence of cyberattacks in high-tech industries: 57% of the firms defined to be high-tech had to handle a cyberattack in the last twelve months. Given the prominence of the high-tech sector in the Israeli economy (and the US economy as well), this is particularly striking and raises concerns.
- Twenty security measures were listed in the survey. The security measures that were implemented most often were the ones that are very inexpensive to employ, such as adopting a strong password policy (93% of firms).
- Small (10–49 employees) and medium-size firms (50–249 employees) implemented on average significantly fewer of the twenty security measures than did the large firms.

4 Regression Analysis

We estimate probit regressions with a binary response variable equal to one if the firm experienced an incident and zero otherwise. In other words, the dependent (or response) variable is a dummy variable that takes on the value one if the firm suffered a cyber incident and zero otherwise.

Since we have data on incidents, firm characteristics, and security precautions, we can estimate the model shown in the left side (shaded circles) of the diagram in Figure 1. The observation is at the level of the firm.

4.1 Mapping Survey Responses to Variables

Independent variables include the following:

- Did the firm employ the four basic security precautions below (yes/no):
  - Strong password policy (e.g. periodical password reset, minimum password length policy, requiring combination of letters, numbers and characters)
  - Keeping systems up-to-date per manufacturer's recommendation, or at a more frequent rate
  - Having multiple updated backup copies, with one offsite and usually offline
  - Means of detecting and responding to malware at endpoints and servers (e.g. antivirus system)
- Small Firm is a dummy variable that takes on the value one if the firm has 10-49 employees and zero otherwise.
- Medium-size firm is a dummy variable that takes on the value one if the firm has 50-249 employees and zero otherwise.
- Large firm is a dummy variable that takes on the value one if the firm has 250 or more employees and zero otherwise.
- Low Revenue is a dummy variable that takes on the value one if the firm's income is below 19 million shekels and zero otherwise.
- Medium Revenue is a dummy variable that takes on the value one if the firm's income is 19-133 million and zero otherwise.
- High Revenue is a dummy variable that takes on the value one if the firm's income is above 133 million shekels and zero otherwise.
- Dummy variables for each of the six sectors:
  - Mining and quarrying, Manufacturing, Electricity and water supply
  - Construction, Transportation and storage, Postal and courier activities, and Accommodation and food activities
  - Trade
  - Information and communication
  - Real estate activities, Administrative and support service activities
  - Professional, scientific and technical activities
- High-tech is a is a dummy variable that takes on the value one if the firm is in the high-tech sector and zero otherwise.
- Ecommerce is a dummy variable that takes on the value one if during 2019 the enterprise received orders for goods or services placed via a website or "app" and zero otherwise
- Cloud is a dummy variable that takes on the value one if the enterprise purchases any cloud computing services used over the internet (including membership, pay by use or any other payment agreement) and zero otherwise
- International is a dummy variable that takes on the value one if the firm is international and zero otherwise.
- Website is a dummy variable that takes on the value one if the enterprise (including the company group) use information about visitors' behavior on its website (e.g. clicks, items viewed) for improving user experience and zero otherwise

Summary data on these variables appear in the appendix in Table 3.

4.2 Estimation and Results

We now estimate the relationship between incidents (the dependent variable) and firm characteristics, Internet use, and (precautionary) choices (security measures) made by the firm in stage 1.

Since the precautions are endogenous, we address the issue by using an appropriate exogenous instrument. Fortunately we have an exogenous instrument for security precautions from the survey: The instrument is "implementation" which is a dummy variable that takes on the value one for those enterprises that report awareness of the cyber directives and instructions and full implementation of the directives. The variable takes on the value zero for those enterprises that were aware of the cyber directives and instructions, but either did not implement them at all, or only partially implemented them.

Of the 993 firms in the sample that were aware of the cyber directives and instructions, 384 (or 39% percent) fully implemented the cyber directives and instructions. Table 2 shows that the implementation variable is positively correlated with the variable we use for security precautions and negatively correlated with incidents.

Additionally and importantly, Figure 4 shows that firms that (i) implemented the directives and employed the four basic security precautions have a lower probability of a cyber incident than firms that (ii) did not implement the directives and employed the four basic security precautions. Further, the figure shows that for firms that did not implement the directives and did not employ the basic controls, there is no difference in the probability of a cyber incident.

Taken together, this provides evidence that the instrument is a good indicator of whether the organization is alert and intentionally vigilant to the risks of cyber attacks.

The results from the probit regressions are shown in Table 1. In the first regression for each of the two different variables for cybersecurity precautions, we do not instrument for the cybersecurity precaution variable. Table 1 shows that in such a case, the estimated coefficient on cybersecurity precautions is positive and statistically significant. Obviously, that does not mean that taking precautions leads to incidents, but rather that those who suffered breaches/incidents were likely to install precautions following an incident. This illustrates the "endogeneity" problem. This is why we need to run an instrumental variable regression.

In the second regression for each of the two different variables for cybersecurity precautions, we do instrument for the cybersecurity precaution variable using the implementation variable. Table 1 shows that in such a case, the estimated coefficient on cybersecurity precautions in negative and statistically significant. This means that other things being equal, employing security precautions reduces the probability of a cybersecurity incident.

Additionally, Table 1 shows that high-tech firms, international firms, firms that use cloud services, and firms that use information about visitors' behavior on its website are more likely to suffer an incident than other firms - and that the effects are statistically significant.

We can use the coefficient estimates on security measures from the Instrumental Variable (IV) probit regressions to get some sense of the difference in the estimated probability of suffering an incident for firms that employ controls vs. firms that do not employ controls. We find the following:

Additional summary data by industry and firm size are shown in Table 4 and Table 5.

Further, a specification test shows that the instrument is indeed exogenous.

For firms that engage in e-commerce, the estimated coefficient is nearly statistically significant.

- For firms with significant revenues and firms with a large number of workers, but are not international firms or high-tech firms, and do not have a "significant Internet presence" the use of four key basic security precautions reduces the probability of a cybersecurity incident from 69% to 21%. These differences are large and suggest that firms that employ four important basic security precautions greatly reduce the risk of suffering a security incident.
- For firms with significant revenues and firms with a large number of workers and with the highest risks of an incident (high-tech firms, international firms, and firms with a significant Internet presence), the use of all four basic security controls reduces the probability of a cybersecurity incident from 94% to 70%.

These differences are large and suggest that firms that employing four important basic security precautions or more than the mean number of security precautions greatly reduces the risk of suffering a security incident.

5 Further Discussion

These findings have public policy implications since we provide the first empirical estimate of how increased security precautions reduce the likelihood of experiencing cybersecurity incidents. While cybersecurity experts have long recommended "best practices" for securing organizations, until now such proclamations have lacked a solid empirical basis.

Of course, more work is needed to corroborate these findings and strengthen the empirical evidence linking investment cybersecurity defenses to experiencing attacks. As good as these survey questions are, it would be desirable to collect additional evidence such as direct observations of security control implementation and experiencing attacks. Such "triangulation" would strengthen the connection between cyber investment and secure outcomes.

Additionally, more work is needed to connect the experience of cybersecurity incidents with the harm they cause (i.e., the right side of the causal model in Figure 1). Establishing such connections is hard for many reasons, including that fewer firms suffer harmful attacks and most cannot readily quantify the harms imposed.

Our results also shed light on what precautions firms should take as well as what data should be gathered moving forward. This can in turn guide firms as they consider how best to spend their limited cybersecurity budgets. This is critical because while "reactive security" measures following incidents are more common, less is done in terms of taking preventative (i.e., ex-ante) security measures.

Finally, Israel is country with an advanced cyber economy that can serve as a useful case study to inform future efforts in larger economies like the United States.

Acknowledgements

We thank Itai Benartzi, Iddo Bar Noy, Yael Lederman, Daniel Roash, and the Israeli National Cyber Directorate (INCD) as well as the Central Bureau of Statistics for their helpful suggestions and coop-

Firms without a 'significant Internet presence" do not use cloud services, do not engage in ecommerce, and do not use information about visitors' behavior on its website.

Similar results (54% vs. 19%) are obtained when we use "whether the firm employed more than mean number of cyber security precautions of other firms in the data set" as the cyber security precautions variable.

Very similar results (93% vs. 69%) are obtained when we use "whether the firm employed more than mean number of cyber security precautions of other firms in the data set" as the cyber security precautions variable.

eration in conducting this research. We gratefully acknowledge support from the US National Science Foundation Award No. 2147505.

References

[1] R. Anderson. Why information security is hard - an economic perspective. In *Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01)*, New Orleans, LA, Dec. 2001.

[2] R. Anderson and T. Moore. The economics of information security. *Science*, 314(5799):610–613, Oct. 2006.

[3] Y. Liu, A. Sarabi, J. Zhang, P. Naghizadeh, M. Karir, M. Bailey, and M. Liu. Cloudy with a chance of breach: Forecasting cyber security incidents. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 1009–1024, Washington, D.C., 2015. USENIX Association.

[4] T. Moore, S. Dynes, and F. Chang. Identifying how firms manage cybersecurity investment. In *15th Workshop on the Economics of Information Security (WEIS)*, 2016.

[5] A. Sarabi, P. Naghizadeh, Y. Liu, and M. Liu. Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, 2(1):15–28, 2016.

[6] D. W. Woods and R. Böhme. Sok: Quantifying cyber risk. In *2021 2021 IEEE Symposium on Security and Privacy (S&P)*, pages 909–926, Los Alamitos, CA, USA, may 2021. IEEE Computer Society.

A Appendix

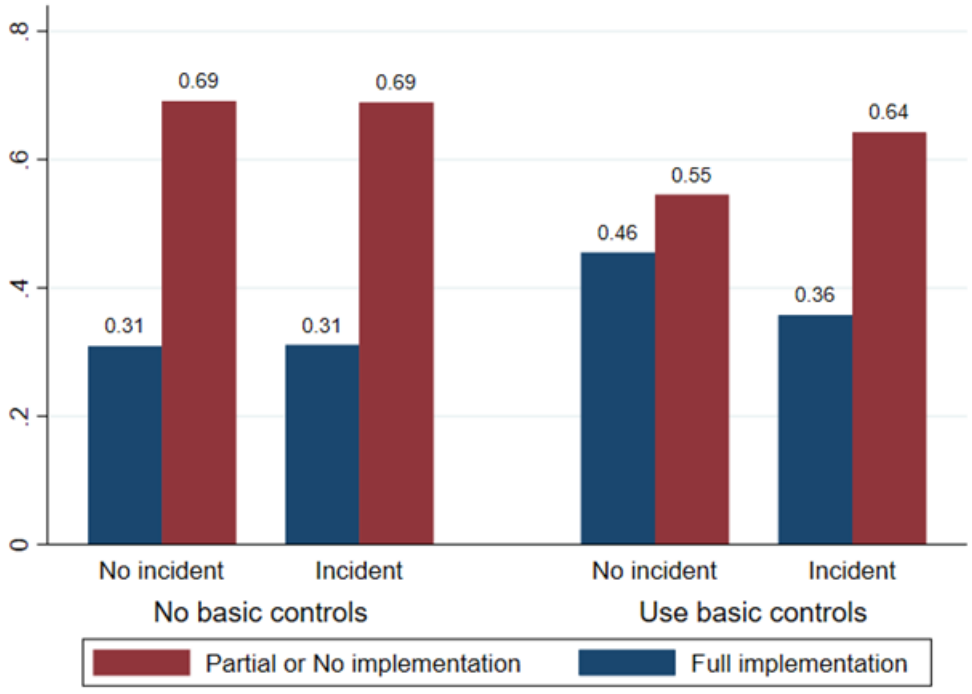

Figure 4: Incidents by use of basic controls and implementation of directives

	Basic controls	
	Probit	**IV probit**
	(1)	(2)
Security Measures	0.247**	-1.308*
	(0.105)	(0.715)
Medium revenue	0.088	0.202
	(0.144)	(0.138)
High revenue	0.338**	0.493***
	(0.160)	(0.150)
Medium-size firm	0.132	0.0978
	(0.124)	(0.119)
Large firm	0.159	0.0963
	(0.140)	(0.137)
High-tech	0.214	0.218*
	(0.132)	(0.124)
International firm	0.259***	0.290***
	(0.09)	(0.085)
Manufacturing industry	0.306**	0.272**
	(0.135)	(0.133)
Trade industry	0.014	0.089
	(0.156)	(0.147)
Information and communication industry	0.088	0.109
	(0.192)	(0.177)
Administrative and support service activities industry	-0.006	0.159
	(0.181)	(0.183)
Professional, scientific and technical activities industry	0.187	0.182
	(0.192)	(0.179)
Cloud	0.263***	0.214**
	(0.099)	(0.104)
Website	0.214**	0.270***
	(0.09)	(0.083)
E-commerce	0.203*	0.082
	(0.115)	(0.130)
Observations	993	993

*Significant at 10%; **significant at 5%; ***significant at 1%

Table 1: Regression Results

	Full implementation	Incident	Basic security measures
Full implementation	1		
Incident	-0.069	1	
Basic security measures	0.082	0.112	1

Table 2: Correlations between key variables.

	Full implementation	Partial or no implementation		
Incident	0.42	0.49		
	(0.49)	(0.5)		
Number of controls	15.8	14.7		
	(4)	(4.1)		
Average revenue of low revenue firms	8.29	9.42		
	(5.12)	(5.41)		
Average revenue of medium revenue firms	59.6	66.7		
	(31.175)	(35.131)		
Average revenue of high revenue firms	1280.4	897		
	(3113.98)	(1255.32)		
Average employees in small-size firms	24.96	26.28		
	(11.68)	(10.75)		
Average employees in medium-size firms	119.86	122.86		
	(53.41)	(58.49)		
Average employees in large-size firms	1394.42	1041.34		
	(2399.52)	(1278.9)		
High-tech	0.24	0.25		
	(0.43)	(0.43)		
International firm	0.41	0.47		
	(0.49)	(0.5)		
Manufacturing industry	0.35	0.42		
	(0.48)	(0.49)		
Construction or Food activities industry	0.15	0.14		
	(0.36)	(0.35)		
Trade industry	0.14	0.15		
	(0.35)	(0.36)		
Information & communication industry	0.16	0.13		
	(0.37)	(0.34)		
Real estate, Administrative activities industry	0.11	0.08		
	(0.32)	(0.27)		
Professional, scientific and technical industry	0.09	0.08		
	(0.28)	(0.27)		
Cloud	0.73	0.76		
	(0.45)	(0.43)		
Website	0.42	0.46		
	(0.49)	(0.5)		
E-commerce	0.2	0.2		
	(0.4)	(0.4)		
Observations	384	609		

Table 3: Summary Statistics by implementation of directives (std. dev. in parentheses)

Industy	Incident	Use basic controls	Average number of controls	International	Cloud	Website	E-commerce
Manufacturing	0.52	0.79	15.14	0.54	0.72	0.38	0.14
Construction, Food activities	0.38	0.74	14.24	0.33	0.69	0.38	0.33
Trade	0.41	0.80	14.80	0.31	0.76	0.61	0.42
Information & Communication	0.52	0.82	16.68	0.56	0.84	0.61	0.18
Real estate, Administrative	0.37	0.86	14.62	0.32	0.73	0.43	0.07
Professional,scientific activities	0.42	0.75	15.15	0.40	0.78	0.27	0.04

Table 4: Descriptive Statistics by Industry

Company size	Incident	Use basic controls	Average number of controls	International	Cloud	Website	E-commerce
Small	0.32	0.73	13.62	0.27	0.65	0.32	0.11
Medium	0.46	0.78	15.02	0.43	0.75	0.37	0.15
Large	0.55	0.83	16.22	0.58	0.81	0.58	0.29

Table 5: Descriptive Statistics by Firm Size