DISCUSSION PAPER SERIES

DP17605

EMPIRICALLY EVALUATING THE EFFECT OF SECURITY PRECAUTIONS ON CYBER INCIDENTS

Neil Gandal, Tyler Moore, Michael Riordan and Noa Barnir

INDUSTRIAL ORGANIZATION

CEPR

ISSN 0265-8003

EMPIRICALLY EVALUATING THE EFFECT OF SECURITY PRECAUTIONS ON CYBER INCIDENTS

Neil Gandal, Tyler Moore, Michael Riordan and Noa Barnir

Discussion Paper DP17605
Published 25 October 2022
Submitted 23 October 2022

Centre for Economic Policy Research
33 Great Sutton Street, London EC1V 0DX, UK
Tel: +44 (0)20 7183 8801
www.cepr.org

This Discussion Paper is issued under the auspices of the Centre's research programmes:

- Industrial Organization

Any opinions expressed here are those of the author(s) and not those of the Centre for Economic Policy Research. Research disseminated by CEPR may include views on policy, but the Centre itself takes no institutional policy positions.

The Centre for Economic Policy Research was established in 1983 as an educational charity, to promote independent analysis and public discussion of open economies and the relations among them. It is pluralist and non-partisan, bringing economic research to bear on the analysis of medium- and long-run policy questions.

These Discussion Papers often represent preliminary or incomplete work, circulated to encourage discussion and comment. Citation and use of such a paper should take account of its provisional character.

EMPIRICALLY EVALUATING THE EFFECT OF SECURITY PRECAUTIONS ON CYBER INCIDENTS

Abstract

To the best of our knowledge, there is no econometric evidence to show that firm investment in cybersecurity defenses reduces the likelihood of a cyber incident. Instead, the available data often 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 cyber incident. 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 cyber incidents. We overcome the endogeneity "obstacle" using an instrumental variable drawn from questions about a cybersecurity directive. The resulting regressions enable us to examine the causal relationship between security precautions potentially undertaken by enterprises and the likelihood of experiencing a cyber incident. Once suitably instrumented, we find robust evidence that increased adoption of security controls does in fact reduce the likelihood of experiencing a cyber incident or breach.

JEL Classification: D22

Keywords: Empirical

Neil Gandal - gandal@tauex.tau.ac.il
Tel Aviv University and CEPR

Tyler Moore - tyler-moore@utulsa.edu
Tandy School of Computer Science, The University of Tulsa

Michael Riordan - mhr21@columbia.edu
Columbia University

Noa Barnir - noabarnir@gmail.com
Tel Aviv University

Empirically Evaluating the Effect of Security Precautions on Cyber Incidents

Neil Gandal
Berglas School of Economics
Tel Aviv University, Israel
gandal@tauex.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

October 3, 2022

Abstract

To the best of our knowledge, there is no econometric evidence to show that firm investment in cybersecurity defenses reduces the likelihood of a cyber incident. Instead, the available data often 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 cyber incident. 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 cyber incidents. We overcome the endogeneity "obstacle" using an instrumental variable drawn from questions about a cybersecurity directive. The resulting regressions enable us to examine the causal relationship between security precautions potentially undertaken by enterprises and the likelihood of experiencing a cyber incident. Once suitably instrumented, we find robust evidence that increased adoption of security controls does in fact reduce the likelihood of experiencing a cyber incident or breach.

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. There is no econometric evidence showing that firm investment in cybersecurity defenses reduces the likelihood of a cyber incident.In this paper, we leverage a dataset gathered by the Israeli Central Bureau of Statistics (CBS) at the behest of the Israeli National Cyber Directorate (INCD). Our objective is to empirically examine how security precautions undertaken by enterprises affect the likelihood of experiencing a cyber incident. We use a remarkably detailed firm-level data set from an ICT use and cybersecurity survey undertaken in 2020-2021 by the INCD and CBS. In our assessment, this is by far the most comprehensive firm-level cybersecurity survey ever undertaken at a national level. We utilize this dataset to establish, for the first time, a causal link between firm-level cybersecurity investments and outcomes (i.e., whether firms experience incidents or breaches).

In addition to the value of the findings themselves, we hope that this may serve as motivation and guide to efforts such as the Bureau of Cyber Statistics recommended by the Cyberspace Solarium Commission.[1] Establishing an empirical basis for cybersecurity could improve the efficiency of future investments, which have been growing steadily in recent years with little to show for it. The results presented here should be complemented by new efforts to study cybersecurity effectiveness, such as additional surveys and field experiments.

1.1 Solving the Endogeneity Problem

A huge problem with empirical work on this topic is that the timing of security investments is unknown. Indeed, 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 cyber incident. Thus, there is an endogeneity issue.

The survey enables us to overcome this obstacle and examine the causal relationship between security precautions potentially 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)? (The directives were published in 2017.)
- 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 2017 "directives" document is more than 140 pages long. We interpret a "yes" response to implementation to mean that the firm is alert and intentionally vigilant to risks of cyber attacks.[2] 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."[3] Hence, the twelve month period for reporting security incidents was no earlier than 2019.

The survey asks specifically about twenty different precautions and the firms need to answer "yes" or "no" for each measure. See Figure 1. It is very likely that, other things being equal, firms that implemented the directives, employed more security precautions prior to the 12 month period for reporting incidents than firms that did not implement the directives. For robustness purposes, we also examined six "basic" cybersecurity precautions that are very easy to immediately employ - and the results were qualitatively unchanged. The 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.

Empirically, the "implementation of the directives variable" works as an instrument for security precautions for the following reasons:

- It is positively correlated with the number of security precautions and whether the firm employed all six basic security measures. Additionally, the implementation variable is negatively correlated with incidents.

[1] Indeed, this is why the Cyberspace Solarium Commission recommended the establishment of a Bureau of Cyber Statistics charged with "collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policymaking" [5]. To begin to answer such questions empirically, a broader population sample is needed. As we wait for such an effort to materialize, it is instructive to begin to answer these questions with suitable data from other sources.

[2] Of the 993 firms that answered yes to being aware of the directives (and hence are included in our data set), 46 percent had to handle a cybersecurity incident in the twelve months preceding the 2020-2021 survey.

[3] We interpret "handling" security incidents to mean that the attack was successful, i.e., there was a breach or incident.

- On average, firms in the data set employed 15 security precautions. For firms that employed more than 15 precautions and implemented the directives, there was a lower likelihood of a security incident (47%) than firms that employed more than 15 precautions, but did not implement the directives (59%). This addresses the timing issue. Further, for firms that employed less than 15 security measures, there is a smaller difference in the probability of a cyber incident between (i) firms that implemented the directives (28%) and (ii) firms that did not implement the directives (33%).
- Additionally, for firms that employed all six basic security measures and implemented the directives, there was a much lower likelihood of a security incident (47%) than there was for firms that employed all six basic security measures but did not implement the directives (65%). Again, this addresses the timing issue. Further, for firms that did not employ all six basic security measures, there is virtually little difference in the probability of a cyber incident between (i) firms that implemented the directives (38%) and (ii) firms that did not implement the directives (41%).
- All of this suggests that the instrument empirically resolves the timing issue. We discuss this in more detail when we conduct the estimation.

1.2 Our Results

When we run a regression of whether the firm had to handle a cyber incident on the number of security precautions and firm and industry characteristics without instrumenting for precautions, we find that the estimated coefficient on the security precautions is (not surprisingly) positive and statistically significant. This is because many firms likely adopted the security measures after suffering a cyber incident and/or were attractive targets for attackers. Once we instrument for the number of security precautions employed by the firm (using the "implementation" variable as the instrument), the estimated coefficient on security precautions is negative and statistically significant. This means that employing more security precautions indeed reduces the probability of suffering a cyber security incident.

Further, when we use the six basic cybersecurity precautions as the security variable, the results are qualitatively unchanged. When we run a regression of whether the firm had to handle a cyber incident on whether the firm employed all six basic security precautions and firm and industry characteristics, without instrumenting for precautions, we find that the estimated coefficient on the security precautions is positive and statistically significant. Again, once we instrument for the six basic security precautions employed by the firm (using the "implementation" variable as the instrument), the estimated coefficient on the basic security precautions is negative and statistically significant. Thus the use of the six basic security measures significantly reduces the likelihood of experiencing a cyber incident for Israeli firms.

Importantly, in our regressions, we include many (control) variables that take into account the attractiveness of the target to attackers. These variable include firm size (both revenues and employees), as well as dummy variables for high-tech firms, firms that use cloud services, firms in high-risk industries, and firms that use information about visitors' behavior on its website. The estimated coefficients on these variables are positive and statistically significant as well.

We find that for 'large" firms with significant revenues using cloud services (the riskiest firms), using 18 out of 20 security precautions rather than 13 security precautions reduces the probability of experiencing a cyber incident from 81% to 58%. Using an alternative measure for security, we find that for 'large" firms with significant revenues using ecommerce and cloud services, using all six basic security precautions reduces the probability of experiencing a cyber incident from 80% to

42%.[4] [5] Perhaps more important than the statistical significance and the economic importance (a large reduction in the probability of a successful attack) is the proof of concept. That is, overcoming the timing issue enables researchers to measure how a stronger security posture reduces security incidents that firms need to handle.

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 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. This should not come as a surprise, given that cybersecurity has long suffered from market failures that undermine the effectiveness of defensive investments [1,2]. Information asymmetries are rife. Firms cannot easily discern whether the technological controls they purchase are effective. Additionally, the relationship between investment in security controls and incidents depends on other factors as well, including firm characteristics and attacker effort.

Hence, as Moore et al. [7] found, firms often simply adopt frameworks of one kind (e.g., the NIST Cybersecurity Framework, COBIT, SANS Critical Controls). While the frameworks direct investments, they do not explicitly evaluate how taking precautions affects the security level of their organization, and ultimately whether those precautions make a breach less likely to occur.

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 systematization [11]. We describe the most relevant empirical work here. Liu et al. gather publicly-observable data on organizations' network misconfigurations and data on observed malicious activities originating from a network (e.g., spam and phishing) to construct a classifier to predict whether a data breach is subsequently reported. These crude external measures of security levels were found to be predictive of subsequent adverse outcomes [6]. Sarabi et al. [10] employed a similar approach, but gathered additional data on business sectors and breach types in order to identify the relative risk of incidents for different industries. Nagle et al. identified a correlation between a firm's network exposure (as measured by counting the number of open ports) and the incidence of botnet-related activity on that network [8].[6]

Our research is very different. We are interested in the causal relationship between security precautions undertaken by firms and outcomes (i.e., incidents). We thus estimate a causal model, where ex-ante firm investment in security precautions and firm characteristics (including attractiveness to attackers) affect the likelihood of experiencing a security incident. The survey questions cover these variables. 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

[4] For firms that employed all six basic security precautions, the average number of security measures employed is 18, while for firms that did not employ all six basic security precautions, the average number of security measures employed is 13. On average, firms employed 15 out of 20 security precautions.

[5] Of course, we are not identifying causal effects of particular security precautions, but rather indicators of security posture. That is, we are testing whether a stronger security posture (as measured by security precautions in the analysis) reduces security incidents that firms need to handle.

[6] Furthermore, a number of risk-rating services have appeared (e.g., offerings from SecurityScorecard, QuadMetrics, and BitSight) that commercialize the results found by researchers.

the harms resulting from incidents, only about ten percent of the firms that had to handle a cyber security incident indicated that they suffered harm. [7] Hence, we cannot examine them in this paper.

3 Data

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 ever 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 the firm had to handle a cyber security attack, as well as questions about Internet use, ecommerce, and other firms characteristics.

The survey population is representative and is drawn from the 29 825 Israeli private sector businesses with more than 10 employees, excluding the following industries: agriculture, finance, education and health.[8] 2 500 of these firms received the survey, of which 2 020 (81%) responded. This very high response rate is because the survey was an official "state" survey and firms were required to complete it. Firms were selected at random in layers by industry, corporate structure (multinational and domestic), and firm size in order to mirror the Israeli economy.

The survey was conducted from July 2020 to March 2021. 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 from the security questions within. In our assessment, this is the most comprehensive (national) survey ever undertaken.[9]

4 Key Summary Statistics

Fully 993 firms indicated that they were aware of the directives and instructions from the INCD. These firms comprise our dataset for analysis. Of the 993 firms in the sample that were aware of the cyber directives and instructions, 384 (or 39% percent) replied that they fully implemented the cyber directives and instructions.[10]

Another key variable is whether the firm had to handle any cyber attacks (or incidents) in the past 12 months. The specific question in the survey was "Did your organization have to handle any cyber security attacks in the past 12 months?"[11] Answering "yes" (regardless of whether there was damage) means the variable "incident" takes on the value one.[12] Overall, 46% of the enterprises reported that they had to handle a cyber attack or incident in the last twelve months.

37 percent of the firms in the data base employed all six basic controls. On average, firms employed 15 of the 20 security measures covered by the survey. Firms were asked whether any of twenty different

[7] It is likely that the small parentage is because it is typically hard for firms to estimate the costs associated with a cyber incident.

[8] These industries are excluded because they are not overseen by the INCD. Finance firms in Israel are very strictly regulated regarding cybersecurity.

[9] We 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.

[10] These numbers suggest that the firms took the survey seriously and to a large extent answered honestly. One might have expected virtually all firms to indicate that they were aware of the survey and had implemented the directives. Again, this is likely due to the fact that the survey was an official state survey.

[11] As noted earlier, it is very reasonable to assume that "handling" security incidents means that the attack was successful, i.e., there was a breach or incident.

[12] As noted above, most firms did not fill in information on damages, and it is not an easy task to calculate such damages.

security precautions were employed by the enterprise? (For each measure, the firm needs to answer yes or no.) See Figure 1.

We also have extensive data on firm characteristics including size, ICT use, and industry.

Incidents vary significantly by firm characteristics. Many large firms with significant revenues and many employees, firms in high-risk industries, and with a significant Internet presence have had to handle a cyber incident: More than 80 percent of these firms had to handle a cyber attack in the last twelve months. These firms are attractive targets to attackers and we control for them using variables that measure the attractiveness of targets to attackers. 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. Small firms with relatively low income without a significant Internet presence suffered far fewer cyber incidents. 20% of these firms had to handle a cyber attack in the last twelve months. Descriptive statistics on all of the variables used in the analysis appear in the appendix in Table 1.[13]

5 Regression Analysis

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 and security precautions on the likelihood of compromise/incidents. The observation is at the level of the firm.

5.1 Endogeneity and our Instrumental Variable

As discussed in the introduction, a huge problem with empirical work on this topic is that the timing of security investments is unknown. Indeed, the survey data we examine exhibits a positive correlation between whether the firm employed the six basic security precautions and incidents. This is because many such investments are made *ex post*, i.e., after a firm has suffered a cyber incident. Thus, there is an endogeneity issue.

We address the endogeneity issue with an instrumental variable regression. Fortunately, we are able to construct an appropriate instrument for security precautions from the survey data. The instrumental variable is “implementation” which is a dummy variable that takes on the value one for those enterprises that report both awareness and full implementation of cyber directives and instructions with reference to a government guidance document. The instrumental variable takes on the value zero for those enterprises that reported awareness of the government guidance document, but did not implement them at all or reported only partial implementation.[14]

Since the guidance document referred to the survey was issued in June 2017, it is very likely that firms for the most part became aware of it and responded to it (either employing or not employing basic security precautions) prior to the 12 month period for which incidents were reported in the survey (2019-2020). This means that other things being equal, firms that implemented the directives likely employed more security measures before the period of the survey than firms that did not implement the directives.

The guidance document is more than 140 pages long, and we do not interpret a “yes” response to implementation questions necessarily to mean that the firm literally followed all of the detailed directives and instructions in the document. We hypothesize only that a firm that implemented the directives was more likely to have adopted more security measures prior to the relevant period in the survey than firms that did not implement the directives.

[13] All figures and appendices are in the appendix.

[14] The possible responses to the implementation variable were full implementation, partial implementation, or no implementation.

We interpret the instrumental variable as an indicator of “vigilance”, an unobserved characteristic of the firm. A more vigilant firm is one that is aware and concerned about cybersecurity threats. Our basic hypothesis supporting the instrumental variable approach is that a more vigilant firm is more likely to be an early adopter of security precautions to discourage or thwart attacks. Furthermore, since both vigilance and the implementation responses were unobservable to potential attackers, these variables presumably are uncorrelated with attacks conditional on the adoption of the basic security precautions and observed characteristics of the firm.

Like most instruments, we doubt that our instrumental variable is a perfect one, because some firms in the sample could have become aware of the guidance document and implemented its directives and instructions in response to suffering a cyber incident. Intuitively, this imperfection is likely to bias our estimate of the effect of security precautions on incidents toward zero. Using Nevo and Rosen’s [9] analysis of “imperfect instruments”, we show that this is indeed the case. Consequently, we think our quantitative estimate of the effect of basic security precautions on preventing incidents is conservative.

The instrument works empirically for the following reasons.

- The implementation variable is positively correlated with the variables we use for security precautions and negatively correlated with incidents.
- For firms that employed more than 15 precautions and implemented the directives, there was a lower likelihood of a security incident (47%) than firms that employed more than 15 precautions, but did not implement the directives (59%). This addresses the timing issue. The former set of firms were thus more likely to employ security measures before an attack. Further, for firms that employed less than 15 security measures, there is a smaller difference in the probability of a cyber incident between (i) firms that implemented the directives (28%) and (ii) firms that did not implement the directives (33%).
- Of the firms that employed all six basic controls, 174 implemented the directives while 188 did not implement the directives. As Figure 2 shows, firms that (i) employed the six basic security precautions and implemented the directives have a lower probability of a cyber incident (47%) than firms that (ii) employed the six basic security precautions, but did not implement the directives (65%). This again addresses the timing issue. The former set of firms were thus more likely to employ the six basic security measures before a cyber incident. Further, the figure shows that for firms that did not employ all six basic security measures, there is little difference in the probability of a cyber incident between (i) firms that implemented the directives (38%) and (ii) firms that did not implement the directives (41%).

The following are the six 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
- Employing two-factor authentication
- Means of detecting and responding to malware at endpoints and servers (e.g. antivirus system)
- Use of operating systems and applications which are under full manufacturer’s support (not in ”end of life” state)
- Data, files and email encryption

As noted above, 37 percent of the firms in the data set employed all six of the basic security precautions. These six precautions were selected because they are quite basic and easy to implement.

5.2 Mapping Survey Responses to Variables

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.

The primary independent variable of interest is security precaution. For robustness, we use two different measurements (and consequently, two regressions):

- First Regression: How many of the twenty security precautions did the firm employ?
- Second Regression: Did the firm employ the six basic security precautions? (yes/no):

We include additional independent (control) variables that take into account the attractiveness of the target. These exogenous variables include firm size (revenues and employees), as well as dummy variables for high-tech firms, firms that use cloud services, firms in high-risk industries, and firms that use information about visitors' behavior on its website. The estimated coefficients on these variables are statistically significant as well. These other independent variables are defined as follows:

- Firm size and firm revenue variables:
  - Large firm is a dummy variable that takes on the value one if the firm has 250 or more employees and zero otherwise.
  - High Revenue is a dummy variable that takes on the value one if the firm's income is above 400 million shekels and zero otherwise.
- High risk (of attack) industry is a dummy variable that takes on the value one if the firm is in one of the following high-risk industries:[15]
  - Mining and quarrying, Manufacturing, Electricity, water supply and Information and communication (these industries handle more cyber cyber attacks than other industries)
- 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.
- 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.

5.3 Estimation and Results

We now estimate the relationship between incidents (the dependent variable) and firm characteristics, Internet use, and the precautionary security posture of the firm. We use two alternative specifications measuring a firm's security posture: the number of security controls (from the list specified in the survey) adopted by the firm, or whether all of six basic controls were adopted by the firm.

Following the empirical "conventional wisdom" (Angrist [3] and Angrist and Pischke [4]), we estimate linear regressions with robust standard errors. In the first case, we do not instrument for our security precautions variable. In the second case, we estimate linear instrumental variable regressions. In the case of our first specification, where the security measure is the number of controls, using an IV probit yields virtually identical results. In the case of our second specification, where the security measure is a dummy variable itself, an IV probit is not appropriate – and linear models are always employed. See Angrist [3] for more details.

[15] Our results are virtually unchanged if we exclude this variable from the regressions.

The results from the regressions are shown in Table 2. In the first regression for each specification, we do not instrument for the cybersecurity precaution variable. Table 2 shows that in both specifications, 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 firms more prone to attack are more likely to adopt precautions, or those who suffer an incident might install controls following the incident. These possibilities illustrates the "endogeneity" problem, and are why we need to run an instrumental variable regression.

In the second regression for each specification, we instrument for our security posture variable using the implementation variable discussed in Section 5.1. Table 2 shows that in such a case, for both specifications, the estimated coefficient on cybersecurity precautions is negative and statistically significant with a p-value of 0.09.[16]

Additionally, like most instruments, we doubt that our instrumental variable is a perfect one, because some firms in the sample could have become aware of the guidance document and implemented its directives and instructions in response to suffering a cyber incident. Intuitively, this imperfection is likely to bias our estimate of the effect of security precautions on incidents toward zero. Using the Nevo and Rosen [9] analysis of "imperfect instruments", this is indeed the case for our data.[17] Consequently, we think our quantitative estimate of the effect of basic security precautions on preventing incidents is conservative. We thus conclude that, other things equal, a stronger security posture reduces the frequency of cybersecurity incidents.

Importantly, in our regressions, we include many (control) variables that take into account the attractiveness of the target. These variable include firm size, revenues, employees, as well as dummy variables for high-tech firms, firms that use cloud services, firms in high-risk industries, and firms that use information about visitors' behavior on its website. The estimated coefficients on these variables are positive and statistically significant. In particular, Table 2 shows that large firms with many employees and significant revenues, firms in high-risk industries, high-tech 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. This all makes sense, since firms with such characteristics are attractive targets to attackers.

Furthermore, the first stage regressions of the endogenous security variables on the instrument (and all other variables in the IV regressions) shows that for both specifications, the instrument is indeed statistically significant in explaining our security variables. See table 3.

We can use the coefficient estimates on security measures from the Instrumental Variable (IV) regressions to get some sense of the difference in the estimated probability of suffering an incident using both specifications.

- To get some sense of the magnitude of the results and compare the two specifications, note that for firms that employed all six basic security precautions, the average number of security measures employed is 18, while for firms that did not employ all six basic security precautions, the average number of security measures employed is 13. (Recall that on average, firms employed 15 out of 20 security precautions.)
- Using the first specification and our estimates, we find that for 'large" firms with significant revenues using ecommerce and cloud services (the riskiest firms), using 18 out of 20 security

[16] Further, for both IV specifications, a one-tailed test rejects the the null hypothesis that the coefficient on security precautions is non-negative with p-values below 0.05.

[17] Using Nevo and Rosen [9], our instrumental variable estimate will be biased toward zero if the Covariance of $\tilde{x}$ and our instrument is greater than zero, where $\tilde{x}$ are the residuals from an OLS regression of our endogenous variable on all other right hand variables (all of which are exogenous). This is indeed the case for both specifications. Hence, the true coefficient is more negative than our estimate in both regressions.

precautions rather than 13 security precautions reduces the probability of experiencing a cyber incident from 81% to 58%.[18]

- Using the second specification and our estimates, we find that for 'large" firms with significant revenues using ecommerce and cloud services, using all six basic security precautions reduces the probability of experiencing a cyber incident from 80% to 42%.
- Thus both specifications give fairly similar results.

6 Concluding Remarks

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. Of course, more work is needed to corroborate these findings and strengthen the empirical evidence linking investment cybersecurity defenses to experiencing cyber incidents. As good as these survey questions are, it would be desirable to collect additional evidence such as direct observations of security control employment 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. Establishing such connections is hard for many reasons, primarily because most firms cannot readily quantify the harms/costs. Finally, Israel is a 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, Analia Schlosser, and the Israeli National Cyber Directorate (INCD) as well as the Central Bureau of Statistics, and participants at the 21st Workshop on the Economics of Information Security (WEIS) for their helpful suggestions and cooperation in conducting this research. We gratefully acknowledge support from the US National Science Foundation (NSF) Award No. 2147505 and the US Israel Binational Science Foundation (BSF) Award No. 2016622 and Award No. 2021711.

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] J. Angrist. Estimation of limited dependent variable models with dummy endogenous regressors: Simple strategies for empirical practice. *: Journal of Business and Economic Statistics*, 19(1):2–16, 2001.

[18] Running an IV Probit regression, using 18 out of 20 security precautions rather than 13 security precautions reduces the probability of experiencing a cyber incident from 76% to 58%.

[4] J. Angrist and J.-S. Pischke. Mostly harmless econometrics: An empiricist's companion. 2009, Princeton University Press.

[5] A. King and M. Gallagher. United States Cyberspace Solarium Commission Final Report, March 2020. https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.p

[6] 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.

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

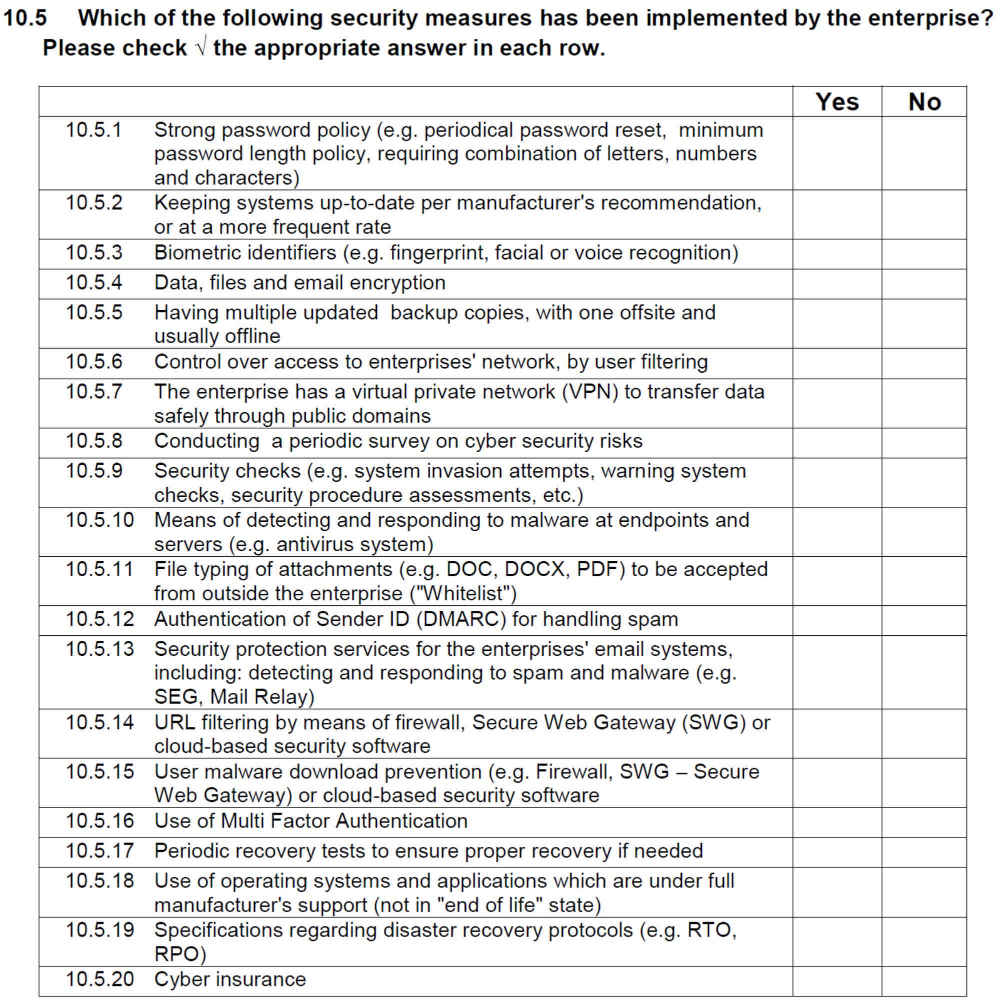
[8] F. Nagle, S. Ransbotham, and G. Westerman. The effects of security management on security events. In *Workshop on the Economics of Information Security*, 2017.

[9] A. Nevo and A. Rosen. Identification with imperfect instruments. *: The Review of Economics and Statistics*, 94(3):659–671, 2012.

[10] 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.

[11] 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.

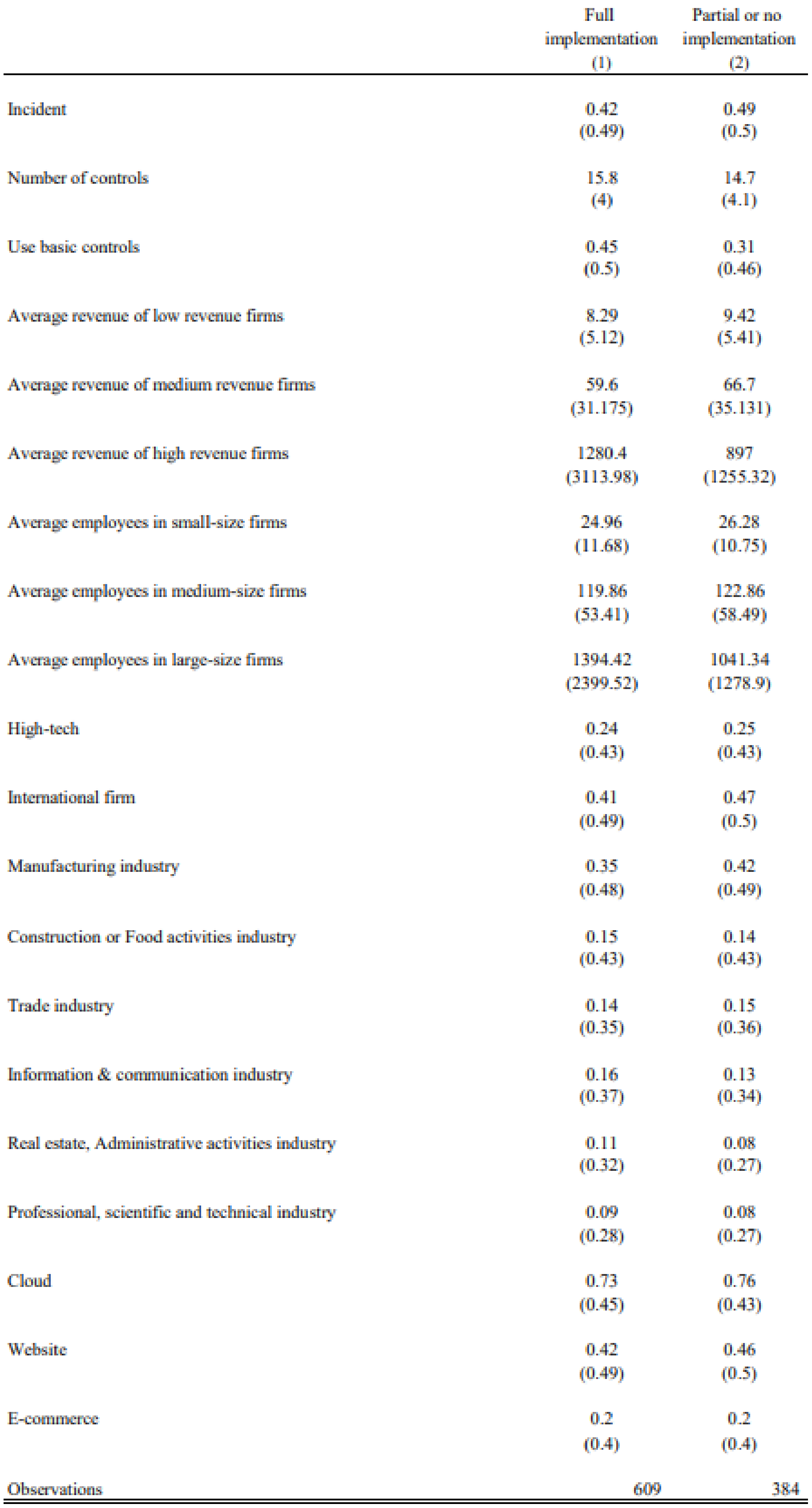
A Appendix



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 1: Survey question dealing with security precautions adopted by the firm.



	Full implementation (1)	Partial or no implementation (2)
Incident	0.42 (0.49)	0.49 (0.5)
Number of controls	15.8 (4)	14.7 (4.1)
Use basic controls	0.45 (0.5)	0.31 (0.46)
Average revenue of low revenue firms	8.29 (5.12)	9.42 (5.41)
Average revenue of medium revenue firms	59.6 (31.175)	66.7 (35.131)
Average revenue of high revenue firms	1280.4 (3113.98)	897 (1255.32)
Average employees in small-size firms	24.96 (11.68)	26.28 (10.75)
Average employees in medium-size firms	119.86 (53.41)	122.86 (58.49)
Average employees in large-size firms	1394.42 (2399.52)	1041.34 (1278.9)
High-tech	0.24 (0.43)	0.25 (0.43)
International firm	0.41 (0.49)	0.47 (0.5)
Manufacturing industry	0.35 (0.48)	0.42 (0.49)
Construction or Food activities industry	0.15 (0.43)	0.14 (0.43)
Trade industry	0.14 (0.35)	0.15 (0.36)
Information & communication industry	0.16 (0.37)	0.13 (0.34)
Real estate, Administrative activities industry	0.11 (0.32)	0.08 (0.27)
Professional, scientific and technical industry	0.09 (0.28)	0.08 (0.27)
Cloud	0.73 (0.45)	0.76 (0.43)
Website	0.42 (0.49)	0.46 (0.5)
E-commerce	0.2 (0.4)	0.2 (0.4)
Observations	609	384

Table 1: Summary Statistics by implementation of directives (std. dev. in parentheses)

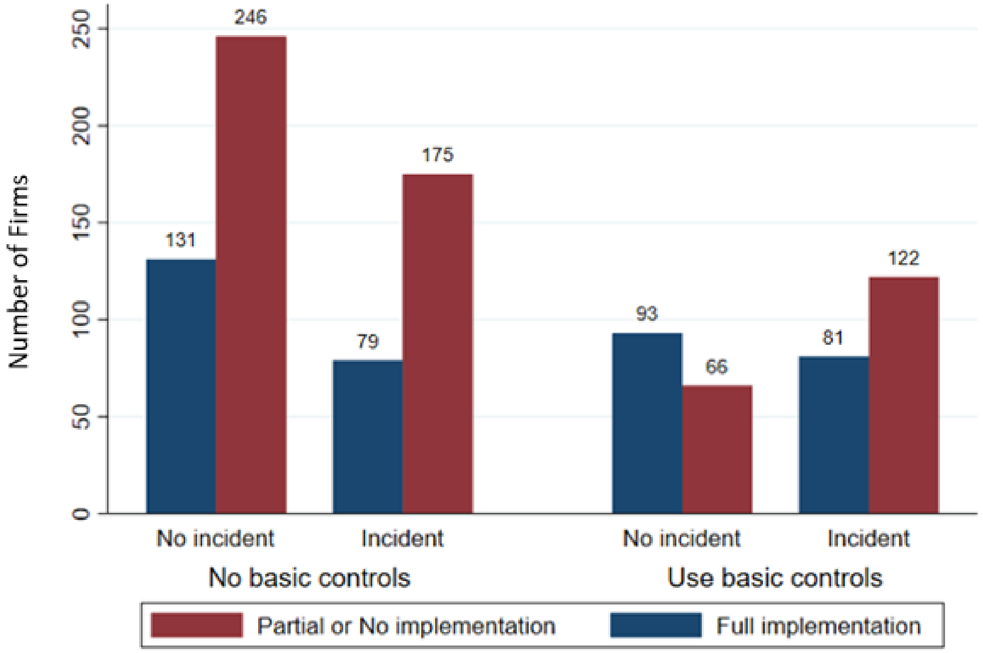
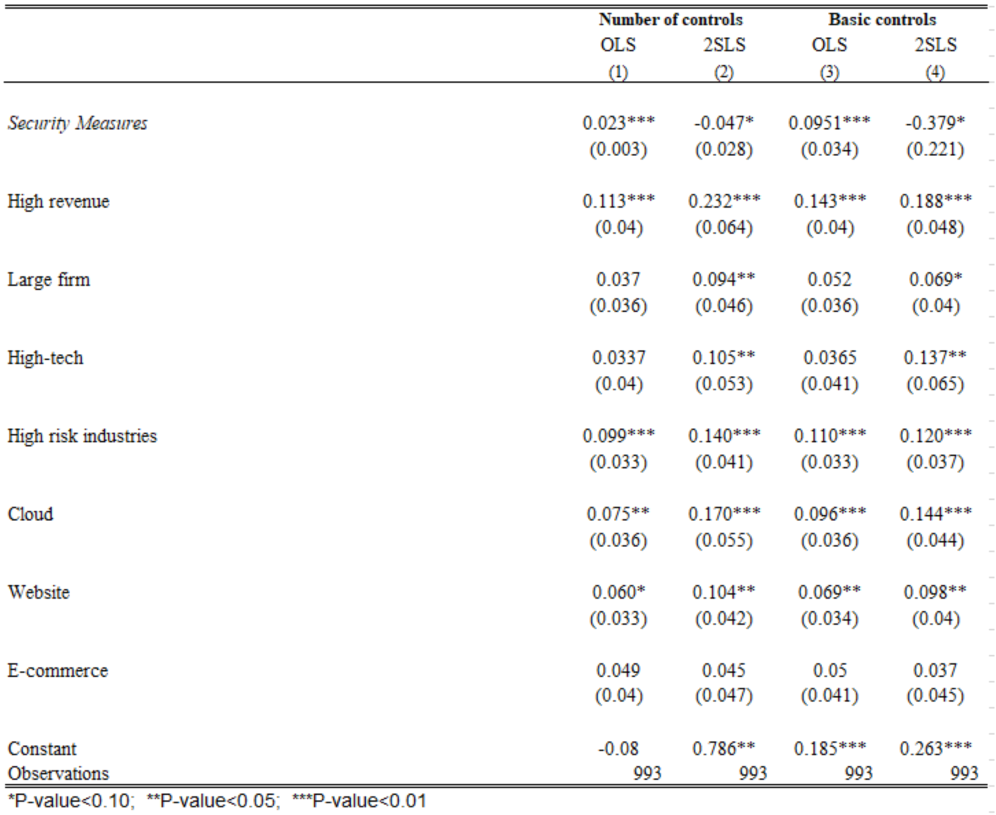


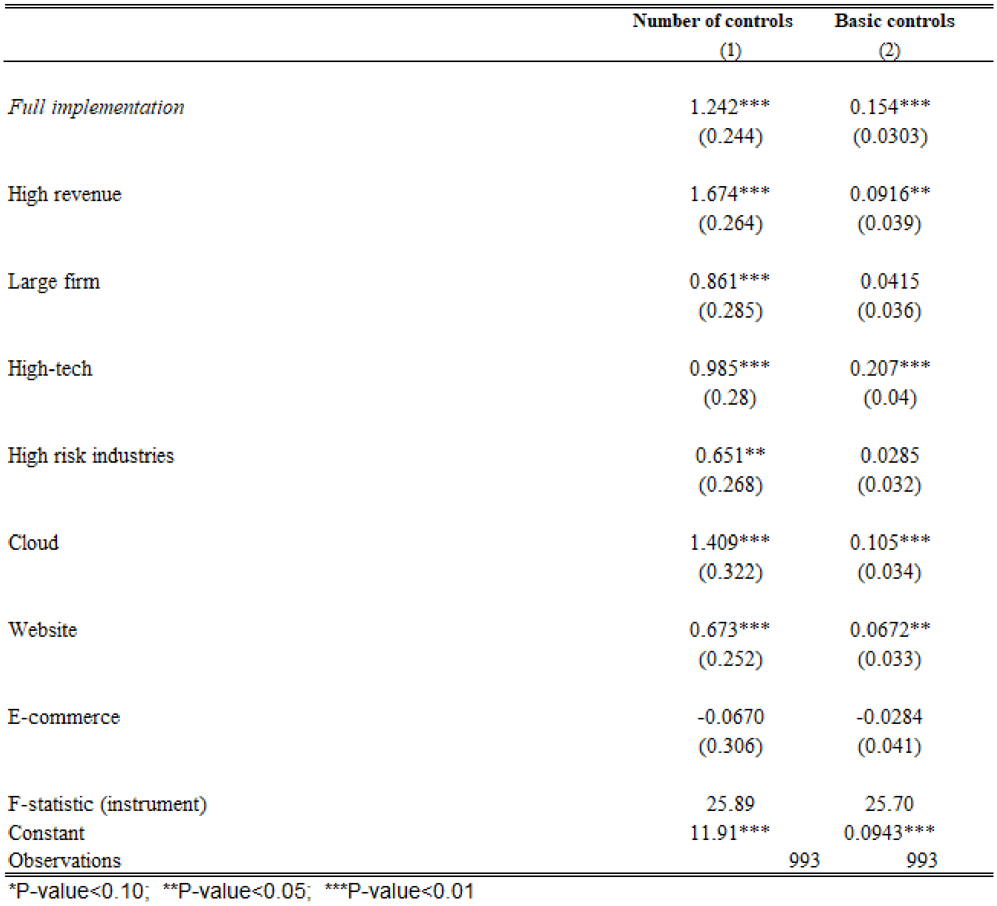
Figure 2: Number of firms with and without security Incidents by use of basic controls and implementation of directives



	Number of controls		Basic controls	
	OLS	2SLS	OLS	2SLS
	(1)	(2)	(3)	(4)
Security Measures	0.023*** (0.003)	-0.047* (0.028)	0.0951*** (0.034)	-0.379* (0.221)
High revenue	0.113*** (0.04)	0.232*** (0.064)	0.143*** (0.04)	0.188*** (0.048)
Large firm	0.037 (0.036)	0.094** (0.046)	0.052 (0.036)	0.069* (0.04)
High-tech	0.0337 (0.04)	0.105** (0.053)	0.0365 (0.041)	0.137** (0.065)
High risk industries	0.099*** (0.033)	0.140*** (0.041)	0.110*** (0.033)	0.120*** (0.037)
Cloud	0.075** (0.036)	0.170*** (0.055)	0.096*** (0.036)	0.144*** (0.044)
Website	0.060* (0.033)	0.104** (0.042)	0.069** (0.034)	0.098** (0.04)
E-commerce	0.049 (0.04)	0.045 (0.047)	0.05 (0.041)	0.037 (0.045)
Constant	-0.08	0.786**	0.185***	0.263***
Observations	993	993	993	993

*P-value<0.10; **P-value<0.05; ***P-value<0.01

Table 2: Regression Results



	Number of controls	Basic controls
	(1)	(2)
Full implementation	1.242***	0.154***
	(0.244)	(0.0303)
High revenue	1.674***	0.0916**
	(0.264)	(0.039)
Large firm	0.861***	0.0415
	(0.285)	(0.036)
High-tech	0.985***	0.207***
	(0.28)	(0.04)
High risk industries	0.651**	0.0285
	(0.268)	(0.032)
Cloud	1.409***	0.105***
	(0.322)	(0.034)
Website	0.673***	0.0672**
	(0.252)	(0.033)
E-commerce	-0.0670	-0.0284
	(0.306)	(0.041)
F-statistic (instrument)	25.89	25.70
Constant	11.91***	0.0943***
Observations	993	993

*P-value<0.10; **P-value<0.05; ***P-value<0.01

Table 3: First stage regression Results