Cyber Extortion and Corporate Vulnerability: Firm-Level Evidence from Ransomware Attacks in Europe *

G. Alfredo Minerva†, Armando Rungi‡, Brandon Levene§

March 20, 2025

Abstract

Ransomware attacks pose unique challenges to firms by encrypting critical data and threatening to leak sensitive information. We assemble a large dataset of European companies, merging balance-sheet information with records of confirmed ransomware incidents. Using propensity score matching, we find that attacked firms exhibit significantly higher costs and a lower liquidity ratio in the year of the attack and in subsequent years. These results suggest that firms' short-term financial buffers are eroded by upfront ransom, remediation, and related costs. Our study is the first to highlight the financial vulnerabilities of non-public European firms facing ransomware, expanding cyber risk research beyond U.S. public companies.

JEL Classification: D22 (Firm Behavior: Empirical Analysis); G32 (Financing Policy; Financial Risk and Risk Management; Capital and Ownership Structure); K42 (Economic Analysis of Crime); O33 (Technological Change: Choices and Consequences; Diffusion Processes);

Keywords: Cyber Risk; Cybersecurity; Firm Performance; Ransomware

*Preliminary and incomplete version. Minerva and Rungi certify that they have no affiliations with or involvement in any organisation or entity that holds a financial interest (such as honoraria, educational grants, participation in speakers' bureaus, membership, employment, consultancies, stock ownership or other equity interests, expert testimony, or patent-licensing arrangements) or a non-financial interest (such as personal or professional relationships, affiliations, knowledge, or beliefs) related to the subject matter or materials discussed in this research project. Levene is an employee of Google, Inc in addition to his employment as an Adjunct Professor at Johns Hopkins University. Neither organization has affiliations with or involvement in any entity that holds a financial interest (such as honoraria, educational grants, participation in speakers' bureaus, membership, employment, consultancies, stock ownership or other equity interests, expert testimony, or patent-licensing arrangements) or a non-financial interest (such as personal or professional relationships, affiliations, knowledge, or beliefs) related to the subject matter or materials discussed in this research project. We thank Emma Neri for outstanding research assistance.

†Department of Economics, University of Bologna, Italy. E-mail: ga.minerva@unibo.it.

‡Laboratory for the Analysis of Complex Economic Systems, IMT School for Advanced Studies Lucca, Italy.

§Alperovitch Institute for Cybersecurity Studies, Johns Hopkins University, Washington DC, United States of America.

1 Introduction

In today's interconnected business environment, companies depend heavily on data collection and the seamless exchange of information. This reliance underscores the critical importance of cybersecurity, as cyber-attacks can significantly disrupt the delivery of goods and services. In response, many European firms have emphasized proactive cybersecurity measures—such as employee training, robust backup procedures, and vendor risk management—to strengthen their resilience. However, especially in the European context, empirical evidence on the exact economic consequences of ransomware attacks remains limited.

Among the cyber threats, ransomware attacks are particularly concerning due to the so-called *double-extortion* strategy: they not only encrypt vital data, rendering it inaccessible, but also threaten to release sensitive information if a ransom is not paid. Ransomware attacks pose both generic and specific risks to firms. The generic risk involves the potential for any company to be targeted by criminal entities seeking ransom payments, contributing to the overarching uncertainty that companies must factor into their strategic planning and risk management frameworks. Additionally, there are specific risks introduced into supplier and buyer relationships. In these bilateral relationships, the need to exchange sensitive information with partners heightens the potential for data breaches, whether perpetrated by the partners or third parties seeking ransom. Such breaches can compromise individual firms and the robustness and resilience of entire supply chains.

This paper aims to evaluate the degree of resilience of firms against ransomware attacks by systematically evaluating firms' performance after being a victim of an attack. We match a firm-level data set with information on ransomware attacks with a large data set with balance sheet information for several million European firms. We then perform propensity score matching to highlight any potential negative effects of ransomware victimization across a variety of corporate outcomes, with respect to unaffected firms. Contrary to much of the existing literature focused on publicly traded firms in the United States, our study is the first to systematically analyze the financial vulnerabilities of non-public European companies, offering new insights into how ransomware affects these less-examined entities.

The economic implications of cyberattacks have attracted significant attention in recent research, reflecting the growing threat these incidents pose to firms' competitiveness and resilience. Anderson and Moore (2009) highlighted the complexity of information security economics by em-

phasizing how the costs of breaches extend beyond direct financial losses to include reputational harm, legal liabilities, and downstream effects on partner firms. In line with this insight, Gordon and Loeb (2002) pointed out that cyber risk management decisions hinge not only on the firm's internal security protocols but also on macro-level considerations such as regulatory frameworks and industry standards. Increasingly sophisticated ransomware operations, which employ "double-extortion" tactics by threatening both data encryption and confidential information leaks, have made it particularly difficult for firms to gauge the full scope of their risk exposure.

Scholars examining the performance implications of cyber incidents suggest that although negative impacts on firm value or stock prices can be swift and pronounced, their long-run persistence often hinges on firm-specific disclosure, governance, and remediation. In a comprehensive study on cybercrime costs, Anderson et al. (2013) argue that while modern cyberattacks (e.g., ransomware) often net only modest direct returns for perpetrators, the indirect losses (e.g., reputational damage, inefficiencies, foregone transactions) and defense expenses (e.g., security products, patching, incident response) can exceed perpetrator gains by an order of magnitude. Kamiya et al. (2021) propose a risk-management model in which successful cyberattacks expose hidden vulnerabilities that undermine investor confidence. Their large-sample tests show severe abnormal returns when personal financial data are compromised, exceeding standard remediation and legal costs. They attribute these outsized losses to reputational damage, with victimized firms tending to bolster board oversight and restrain managerial risk-taking. Corbet and Goodell (2022) analyze the 2021 Colonial Pipeline ransomware incident, uncovering "reputational contagion" extending beyond directly impacted operations. Using GARCH and DCC-GARCH to track volatility and returns, they find competitor firms—though unlinked operationally—suffered heightened volatility and negative price reactions. This broad effect, they argue, stems from investor attention shocks that penalize firms perceived as vulnerable by association, underscoring the power of large-scale cyber events to shape market sentiment and amplify negative spillovers. Crosignani et al. (2023) investigate the 2017 NotPetya attack, showing how it paralyzed major multinationals and imposed disproportionate losses on downstream customers—around four times the attackers'. Impacted customers tapped liquidity reserves and drew more on credit lines if they lacked alternate suppliers or used highly specialized inputs. Eventually, many replaced compromised vendors with security-savvy alternatives, triggering lasting shifts in supply networks. Their evidence underscores how cyber shocks magnify risks beyond targeted firms and reshape supply chains. Florackis et al. (2022) develop

a textual measure of cyber risk from 10-K disclosures, validated via known attacks. They show that high-exposure firms bear systematically higher future returns—around 8% annually—and are more prone to subsequent breaches. The measure correlates with known vulnerabilities, rises over time, and remains robust after controlling for standard firm-level and risk factors. Firms with extensive cyber risk statements underperform during high cyberattack concerns, consistent with investor compensation for intangible, systematic cyber threats. Jamilov et al. (2021) introduce a novel, text-based measure of firm-level cyber risk exposure derived from quarterly earnings call transcripts, covering 13,000 firms across 85 countries (2002–2021). Their computational linguistics approach shows that cyber risk exposure predicts future attacks, affects stock returns, and is priced in equity options. The study also finds that risk spills over across firms and estimates global cyber risk costs exceed $200 billion annually, thereby advancing the literature on quantifying cyber threats and their economic impact.

To summarize, ransomware attacks create immediate cash flow problems for firms, requiring quick spending on ransom, legal fees, and computer investigations even when overall profits remain steady. These attacks can also disrupt supply chains, increasing financial stress. Although fast fixes, backup plans, or cyber insurance may lessen revenue losses, such incidents notably impact firm performance and financial health through short-term cash issues, reputation damage, and supply-chain weaknesses. Using a large dataset of European companies, our research deepens the understanding of these effects and explores how ransomware attacks affect financial outcomes.

2 Data and variables

Our research is carried out thanks to merging two primary data sources.

2.1 Firm-level variables

The main outcomes and covariates are obtained from firm-level balance sheet information for all EU plus UK countries from Orbis by Moody's, over the period 2019-2023. Data were downloaded in June 2024, so that there are fewer balance sheet observations for year 2023. We extract information on a number of variables including operating revenues, value added, the number of workers, total assets, cost of goods sold, firm age, and two financial ratios, the liquidity ratio and the solvency ratio. The liquidity ratio is defined as current assets net of stocks, divided by current liabilities.

The solvency ratio is defined as shareholder funds over total assets multiplied by 100.

2.2 Ransomware attacks

Data on ransomware attacks are provided for research purposes by Camichel Ventures GmbH (2025). The data are sourced from leak or shame sites where ransomware groups publish information about their victims. This practice is part of the double-extortion scheme, which involves both encrypting data and threatening to release confidential information unless a ransom is paid. The dataset contains: victim name (identifies the targeted organization); leak site name (specifies the platform where victim information is posted); timestamps (records the dates when the victim was first and last seen on the leak site). The dataset covers incidents from 2020 to 2023, aligning with the period when operating leak sites became standard in the ransomware business model. We are able to match roughly 600 incidents to firms with balance sheet information in our sample. In Table 1 we report the most common ransomware in terms of number of victims.

[Insert Table 1 about here]

Table 2 presents the country-wise breakdown of firms, showing both the frequency of attacked firms and their percentages within the full sample.

[Insert Table 2 about here]

Table 3 shows the distribution of attacks by the year each firm was first targeted. Note that there are fewer attacked firms in 2023 because, as of our June 2024 data download from Orbis, balance sheet information for that year was available for a more limited number of companies.

[Insert Table 3 about here]

3 Empirical Strategy

Firms are hit by ransomware attacks in different years. We consider the fact of being attacked as an *absorbing* treatment, such that the treatment status over time is a non-decreasing sequence of zeros and then ones if the firm is listed on shame sites.

First of all, we estimate the likelihood that a firm has been treated (i.e., that it has been hit by a ransomware attack and publicly exposed on shame sites either in the current or a previous

year) using a logistic regression on a set of covariates. These covariates include the logs of firm age, lagged size (measured in terms of employment), lagged capital intensity (total assets per employee), lagged value added per worker (a proxy for productivity), as well as country, two-digit industry and year fixed effects. We estimate the following logistic regression model to obtain the propensity score:

$$P(D_{i,j,c,t} = 1 \mid X_{i,j,c,t}) = \frac{\exp(X'_{i,j,c,t}\beta)}{1 + \exp(X'_{i,j,c,t}\beta)}. \tag{1}$$

In this specification, $D_{i,j,c,t}$ is an indicator that firm i in industry j, in country c at time t is treated, $X_{i,j,c,t}$ is the vector of covariates described above.

We then predict the propensity score, which is used to match with five nearest neighbors under common support, and we compare the means between treated and nontreated firms across multiple outcome variables. Specifically, we consider: the log of operating revenue; the log of the cost of goods sold; the liquidity ratio, a measure that reflects a company's capacity to cover its short-term obligations with its most liquid assets; the asset-based solvency ratio, a measure that reflects a firm's ability to meet its long-term obligations using its assets.

4 Results

We show the results of the logistic regression (1) in Table 4.

[Insert Table 4 about here]

We then show the results obtained after matching with the five nearest neighbors using the propensity score predicted after estimating (1).

[Insert Table 5 about here]

After matching, the differences that remain statistically different from zero are the log of costs and the liquidity ratio. In particular, we witness a higher cost of goods sold for attacked firms of the order of 23% (p-value of about 0.045), and a reduction of the liquidity ratio by 0.31 points (p-value well below 0.01). A drop of 0.31 points in the liquidity ratio means that, on average, ransomware-affected firms have about 16% fewer near-cash resources relative to their short-term liabilities than firms that were not attacked (given the control group's average ratio of around 1.96).

In practical terms, it indicates that these firms have a notably smaller financial cushion to cover immediate obligations once inventories are excluded, which can heighten the risk of short-term liquidity pressures following an attack.

Table 6 presents the balancing test results for the main covariates after matching. Specifically, we match each treated firm with five nearest neighbors from the control group based on the propensity score, meaning that the final matched sample includes all treated firms plus up to five controls per treated firm. The results show that differences in means across all variables are small and statistically insignificant (p-values well above 0.05). This indicates that the matching procedure successfully balances the treated and control groups on these covariates, validating our empirical approach and methodological design.

[Insert Table 6 about here]

4.1 Discussion of the Mechanisms

Our estimates indicate a statistically significant positive ATT for firms' costs and a negative ATT for the liquidity ratio, while operating revenues show no decrease. The lack of an observable negative effect on annual revenues suggests that any short-term disruptions are either too brief to appear in yearly data or offset by other firm-level adjustments (e.g., catching up on production, leveraging backup systems, or receiving insurance reimbursements). Below, we propose several mechanisms that could simultaneously raise costs and weaken liquidity ratios, even when annual operating revenues do not change significantly.

Immediate Cash Outflows and Ransom Payments

A direct mechanism arises from ransom payments themselves. Even if ransom demands are negotiated or partially covered by insurance, the cash outlay—whether formal (paying attackers to restore data access) or indirect (legal or consulting fees)—immediately draws down a firm's liquid assets, weakening its short-term liquidity.

Unplanned Expenditures on Recovery and Remediation

Beyond ransom payments, post-attack expenses often include system restoration, forensic investigations, and IT upgrades. These costs must generally be paid up front from liquid resources.

Additional spending on external cybersecurity consultants or overtime for in-house IT staff can also reduce the firm's cash or near-cash assets.

Heightened Reliance on Short-Term Financing

When cyberattacks create liquidity pressures, some firms resort to short-term borrowing to meet immediate obligations. The added debt burden, often at higher interest rates, can erode liquidity by diverting cash flows to interest and principal payments, further weakening short-term financial health.

Insurance Coverage Gaps or Delayed Insurance Payouts

Cyber insurance can mitigate direct financial losses, but coverage gaps and lengthy claim processes can still pressure a firm's short-term liquidity. Firms typically have to pay recovery and remediation costs up front, relying on future reimbursement. Any delay in these reimbursements extends the period during which the firm's liquidity remains under strain.

5 Conclusions

In a large sample of European firms, we show that those that have experienced a ransomware attack face higher costs and a lower liquidity ratio. Our explanation hinges on the occurrence of costly disruptions and unplanned expenditures for attacked firms, that raise costs and drain liquid assets relative to short-term liabilities. Even after matching on a large number of observables, these post-attack effects can persist long enough to cause statistically significant differences between attacked and non-attacked firms.

References

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: Böhme, R. (Ed.), The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg. chapter 12, pp. 265–300.

Anderson, R., Moore, T., 2009. Information security economics–and beyond, in: Advances in Cryptology–CRYPTO 2009, pp. 68–91. Lecture Notes in Computer Science.

Camichel Ventures GmbH, 2025. Enhancing threat detection and incident response capabilities with ecrime.ch. `https://ecrime.ch/whitepaper/`. Whitepaper.

Corbet, S., Goodell, J.W., 2022. The reputational contagion effects of ransomware attacks. Finance Research Letters 47, 102715.

Crosignani, M., Macchiavelli, M., Silva, A.F., 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. Journal of Financial Economics 147, 432–448.

Florackis, C., Louca, C., Michaely, R., Weber, M., 2022. Cybersecurity risk. Review of Financial Studies 36, 351–407.

Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Transactions on Information and System Security (TISSEC) 5, 438–457.

Jamilov, R., Rey, H., Tahoun, A., 2021. The anatomy of cyber risk. Working Paper 28906. National Bureau of Economic Research.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A., Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics 139, 719–749.

Table 1: Leak site distribution of attacked firms found in Orbis

Leak site	Frequency	Percent
LockBit 2.0	83	14.36
Conti	69	11.94
LockBit 3.0	36	6.23
Egregor	24	4.15
AlphVM	22	3.81
Avaddon	21	3.63
Grief	21	3.63
REvil	19	3.29
MAZE	18	3.11
PYSA	16	2.77
BlackBasta	15	2.60
DoppelPaymer	15	2.60
HiveLeaks	14	2.42
BABUK	12	2.08
CL0P	11	1.90
LV	11	1.90
Ragnarok	11	1.90
Vice Society	11	1.90
Other ransomware	149	25.78
Total	578	100.00

Note: The table shows the distribution of leak sites with at least 10 attacked firms.

Table 2: Country distribution of attacked firms and overall sample from Orbis

Country	Frequency of attacked firms	Percent of attacked firms	Frequency in the full sample	Percent in the full sample
Austria	11	1.90	4,578	0.22
Belgium	18	3.11	10,604	0.50
Bulgaria	3	0.52	88,568	4.17
Czech Republic	8	1.38	50,173	2.36
France	83	14.36	65,707	3.10
Germany	68	11.76	28,219	1.33
Hungary	6	1.04	11,334	0.53
Ireland	2	0.35	1,966	0.09
Italy	167	28.89	606,135	28.55
Luxembourg	1	0.17	117	0.01
Poland	11	1.90	112,355	5.29
Portugal	20	3.46	325,850	15.35
Romania	7	1.21	151,246	7.12
Slovenia	2	0.35	37,503	1.77
Spain	110	19.03	614,695	28.95
Sweden	2	0.35	42	0.00
United Kingdom	59	10.21	13,877	0.65
Total	578	100.00	2,122,969	100.00

Note: The table shows the distribution by country of attacked firms for which we are able to find balance sheet information from Orbis, and the distruùibution in the full sample.

Table 3: Distribution of first year of attacks for firms found in Orbis

Year	Frequency	Percent
2020	92	15.92
2021	238	41.18
2022	199	34.43
2023	49	8.48
Total	578	100.00

Note: The table shows the distribution of the first year of attacks.

Table 4: Logistic regression

	(1) Coef/t-stat
Age (log)	0.2542
	(5.50)
Employees at $t-1$ (log)	0.8181
	(45.80)
Capital intensity at $t-1$ (log)	0.1852
	(5.16)
VA per worker at $t-1$ (log)	0.2238
	(4.25)
2-digit NACE dummies	Yes
Country dummies	Yes
Year dummies	Yes
Pseudo-R^2	0.31
Obs.	4,990,238

Note: Dependent variable is $D_{i,j,c,t}$, an indicator equal to one that firm i in industry j, in country c in year t has been hit by a ransomware in year t or before, and zero otherwise.

Table 5: Propensity score matching estimates

Outcome	Sample	Treated	Controls	Difference	S.E.	t-stat
Operating revenue (log)						
	Full sample	17.728	13.304	4.424	0.061	72.05
	Nearest neighbors (ATT)	17.728	17.645	0.082	0.070	1.18
Costs of goods sold (log)						
	Full sample	16.606	12.001	4.605	0.095	48.61
	Nearest neighbors (ATT)	16.606	16.377	0.229	0.114	2.01
Liquidity ratio						
	Full sample	1.648	3.161	-1.513	0.228	-6.65
	Nearest neighbors (ATT)	1.650	1.962	-0.312	0.096	-3.25
Solvency ratio						
	Full sample	39.284	38.669	0.615	1.086	0.57
	Nearest neighbors (ATT)	39.284	40.186	-0.903	0.847	-1.07

Note: The table shows the differences in means between treated and control observations both in the full sample and after matching under common support using 5 nearest neighbors.

Table 6: Balance test for covariates

Variable	Mean (T)	Mean (C)	% Bias	t-stat	p-value	V(T)/V(C)
Age (log)	3.3225	3.3409	-2.3	-0.57	0.568	0.94
Employees at $t-1$ (log)	4.9937	4.9850	0.5	0.10	0.918	0.78
Capital intensity at $t-1$ (log)	12.7400	12.6730	4.5	0.98	0.327	0.94
VA per worker at $t-1$ (log)	11.443	11.450	-0.7	-0.16	0.872	1.07

Note: T is the treated group, C is the control group; V(T)/V(C) is the variance ratio.