SERIES:
Research Insights for Investment Professionals

ISSUE: NO. 3 | DATE: JULY, 2026

CYBER RISK AND CORPORATE RESILIENCE

A practitioner-focused synthesis of original research

Luc Renneboog, Jasmin Gider, Tal Strauss

EXECUTIVE SUMMARY

Using 14,261 cyber incidents across nearly two decades (2005–2023), we provide an empirical study of cyber vulnerability among publicly-traded U.S. firms, drawing on a rich dataset of publicly observable indicators: financial data, SSL certificate records, bug bounty programs, cyber-hygiene indicators from regulatory filings, executive and governance data, and detailed incident records. For investment professionals, cyber risk remains hard to price because it is still treated largely as a binary ESG/governance checkbox rather than a quantifiable, firm-specific risk factor. The core difficulty is measurement: which firms are more exposed, which protective measures work? This study addresses that gap. We identify firm-level drivers of cyber risk, examine the effectiveness of protective measures and regulatory interventions, and build a machine-learning model for cyber exposure. Three results stand out. (i) Prior incidents are the strongest predictor of future events: firms with past incidents face an approximately six-fold higher likelihood of subsequent attacks, indicating that vulnerability is persistent and clusters at the firm level rather than reflecting one-off security lapses. (ii) Exposure is sector-dependent: finance, hospitality, and business services are materially riskier than metals, petroleum, or traditional manufacturing, and larger firms are more exposed, as target attractiveness outweighs their defensive resource advantage. (iii) Using regulatory shocks that force security upgrades, we document that mandated protection reduces subsequent incidents, consistent with firms underinvesting because of agency costs and unpriced externalities. Among voluntary protective measures, bug bounty programs stand out, reducing incident risk by roughly 42.5%. The practical benefit is a set of externally observable, verifiable signals, which investors can incorporate into pricing, factor models, and stewardship, rather than relying on corporate disclosure narratives.

Key Takeaways for Investment Professionals

- Treat prior incidents as a primary risk signal.
- Score cyber risk on a scale – sector baseline plus firm-specific exposure – instead of ticking a compliance box.
- Reward verifiable governance and protection, not policy narrative.
- Separate negligence-driven from externally-driven incidents, to isolate management failures from external attacks.

CFA Society Netherlands

ABOUT THE VBA RESERVES The research in this series is funded through the VBA reserves of CFA Society Netherlands. These reserves were created following the merger between VBA Beleggingsprofessionals and CFA Society Netherlands and are dedicated to supporting initiatives that promote knowledge and professional practice related to investment analysis, portfolio management, financial issues, and related disciplines. Through this funding, the Society aims to contribute to practitioner-oriented research and knowledge sharing for the development of the investment profession in the Netherlands.

WHY THIS RESEARCH MATTERS NOW

Cyber risk presents material, priced exposure that investment professionals can no longer treat as a disclosure checkbox. Estimates put the global cost of cybercrime at roughly USD 11 trillion in 2023, estimated to exceed USD 24 trillion by 2027. Three structural shifts make this theme timely. First, the regulatory information environment has changed: the SEC's 2023 rules require U.S. registrants to disclose material cyber incidents on Form 8-K within four business days and to disclose risk management, strategy, and governance annually for fiscal years ending on or after December 2023, while DORA (Digital Operational Resilience Act) entered into force across the EU in January 2025, alongside uneven NIS2 (Network and Information Security 2 Directive) transposition, creating both a structural break in disclosure quality and persistent cross-border information asymmetries. Second, much of existing academic evidence has been constrained to small samples (from primarily the Privacy Rights Clearinghouse) without firm-level measures of exposure and protection, leaving the determinants of resilience largely unidentified. Third, current practice still treats cyber as a binary indicator within ESG/governance scores rather than a quantifiable, persistent, and partly manageable risk gradient. Ignoring this gap exposes portfolios to mispriced tail risk and repeat-breach concentration, while stewardship misses verifiable governance levers, such as dedicated C-level roles, board attention, bug bounty programs, which can reduce incident probabilities.

Relevance in Today's Context

- Cybercrime is a macro-scale, growing exposure.
- The disclosure regime has changed structurally.
- Treating cyber as a binary ESG/governance flag, instead of a quantifiable, persistent and partly manageable risk factor, leads to mis-pricing.

RESEARCH QUESTION AND APPROACH

We ask which firm-level characteristics drive cyber vulnerability and whether security investments reduce the incidence of cyber events. Prior work is constrained by small samples (largely the Privacy Rights Clearinghouse), missing firm-specific exposure and protection measures, and endogeneity. We address these gaps with a new dataset and a causal design.

Our sample covers 14,261 cyber incidents at publicly traded U.S. firms (2005–2023), each detailing perpetrator type, compromised assets, records and individuals affected, attack type, and financial damages. Many firms report multiple incidents per year. The annual count of firms reporting at least one incident has risen sharply.

To identify correlates of vulnerability, we assemble externally observable characteristics – from several novel databases, built via scraping, textual analysis, or hand-collection: classical firm variables (size, profitability, leverage, age, Tobin's Q, R&D); governance (cybersecurity roles and committees, top-management education and experience); exposure (data intensity, retail apps and their success, API services, AI patents); and protection (bug bounty programs, SSL certificate management, cyber hygiene, cyber standards). We model incident occurrence as a function of a common time trend, industry, firm and governance characteristics, and exposure and protection.

What This Research Does (and Does Not) Show

- Past breaches are a strong signal.
- Certain industries (hospitality, retail, finance, services), size, and data asset exposure raise risk; profitability and institutional ownership reduce it.
- Governance structure matters.
- Correlation does not imply causation: The empirical design in our work goes beyond measuring a correlation between cyber vulnerability and corporate cyber protection, which could just reflect strong exposure, and allows for a causal interpretation of the effect of protection on cyber risk.

Because more-exposed firms adopt stronger protection, we break this endogeneity using regulatory shocks that force security upgrades: staggered state breach-notification laws (with a stringency score), Google's Certificate Transparency initiative (2014/2015), nine NIST/critical-infrastructure events (2009–2020), and supply-chain shocks (the WannaCry, and NotPetya cyberattacks affecting a host of related firms). Mandated upgrades reduce subsequent incidents, consistent with underinvestment from agency costs and unpriced externalities.

Finally, an XGBoost model trained on 110,000 firm-years (2005–2017) and tested on ~34,000 (2018–2023), with a time-based split to avoid look-ahead bias, yields a meaningful signal (51% precision, 38% recall at the optimal threshold). A SHAP (SHapley Additive exPlanations) analysis across 309 variables attributes 71% of predictive power to firm characteristics, 12% to board/management, 11% to exposure, and 6% to protection; top predictors are firm size, prior incidents, governance roles, sales volatility, SSL characteristics, and industry, with nonlinear, heterogeneous effects.

APPLICATIONS FOR INVESTMENT PROFESSIONALS

The research suggests a number of practical implications for investment professionals.

Sector allocation. The research quantifies which sectors might carry structurally elevated cyber exposure. Finance, hospitality, and business services are materially riskier; metals, petroleum, and traditional manufacturing are not. For thematic funds, this provides an empirical basis for cyber-adjusted return expectations by industry, rather than relying on generic ratings that often treat cyber as a binary disclosure checkbox rather than a priced risk gradient.

Factor model augmentation. The research suggests a set of externally observable factors that help identify firm-level cyber exposure. The findings also support the notion of persistence of cyber vulnerability. Hence, models can be improved by incorporating historical incident frequencies and incident-type severity weights as a standalone risk factor or as an overlay on quality/governance factors.

Risk management integration. The dataset assembled in the study distinguishes perpetrator types (external hackers, insiders, accidental data loss, physical theft) and attack vectors (ransomware, phishing, misconfiguration, supply-chain compromise). This granularity allows investors to separate incidents that reflect genuine failures of management from incidents that occur despite reasonable protective effort.

Digital exposure and attack-surface screening. The study operationalizes cyber exposure through several externally observable proxies that investors can construct independently of corporate disclosure. Web presence, Application Programming Interface (API) intensity, mobile-app installation volumes, top-app-developer status, and Artificial Intelligence (AI)-related patenting all correlate positively and, in most cases, statistically significantly with subsequent incidents. These measures are inexpensive to construct at scale from public sources (domain registries, app-store metadata, patent databases, and API directories) and offer a firm-level attack-surface score that complements the standard financial fundamentals used in equity research.

Practical Use Cases

- Consider cyber risk by sector. Finance, hospitality, and business services carry structurally elevated risk; metals, petroleum, and traditional manufacturing do not.
- Augment factor models with persistency-based signal. Prior breaches strongly predict future events.
- Screen on governance structure, not just policy disclosure. Dedicated C-level data/security roles, board security committees, and adoption of cybersecurity standards materially lower breach probability.
- Reward investment into verifiable corporate protection.
- Separate negligence from external attacks in risk management scoring. Incident-type and perpetrator data isolate management-driven failures from externally-driven events, sharpening cyber signals in governance scores.

CONCLUSIONS AND NEXT STEPS

Cyber risk is firm-specific, persistent, and at least partially manageable. Externally observable indicators – prior events, dedicated C-level roles, board oversight, SSL certificate hygiene, bug bounty programs, and adoption of recognised standards – carry meaningful signals for future events and can be incorporated into risk and stewardship processes today. Causal evidence from regulatory shocks confirms that mandated protection upgrades reduce subsequent events, consistent with underinvestment driven by agency costs and unpriced externalities. This strengthens the case for active engagement on cyber governance and for differentiating issuers on verifiable protection rather than narrative.

Several caveats bear on how these results should be used. The estimates are lower bounds on the true rate of incidents. The analysis relies on publicly observable events, and a substantial share of cyber incidents remains confidential, particularly outside the U.S. where mandatory disclosure is uneven and only partially enforced. Firms may also under-report cybersecurity investment to avoid signaling vulnerabilities to attackers or to competitors, biasing observed protection measures downward. Reported damages exclude third-party externalities and indirect costs (reputational losses, foregone business, reduced operational flexibility, increased cost of capital, higher premia for cyber insurance, and litigation) that are inherently hard to quantify. The distinction between negligence-driven and externally driven incidents depends on attribution that is imperfect at the time of disclosure and often revised later.

Several directions are promising for both academic research and investment practice. First, augmenting public indicators with proprietary firm-level data (security spending, incident logs, audit findings) would sharpen protection and breach detection. Second, partnering with cyber insurers would provide claims data on non-public events, addressing under-reporting directly. Third, the SEC's 2023 disclosure rules create a structural break enabling reassessment of pricing, persistence, and protection effects. Fourth, extending the framework to private firms and to SMEs is essential for credit and private-market investors and for policymakers concerned with systemic risk transmission.

Points for Professional Discussion

- How should portfolio managersinvestment professionals price the persistence finding,: as a tilt away from repeat-breach firms, or as an engagement opportunity where governance reform is credibly underway?
- How should the SEC's post-2023 disclosure regime reshape both fundamental analysis of U.S. issuers and the way investors push for comparable transparency in other jurisdictions?
- Which verifiable protective actions (bug bounty programs, formal standards adoption, board committees, dedicated cyber roles) should stewardship teams prioritize in engagement, and at what point should absence of these actions become a voting or divestment trigger?
- To what extent should credit analysts and rating methodologies incorporate the persistence of cyber vulnerability into loss-given-default and probability-of-default assumptions?

About the Original Research

This summary is based on the following original research paper:

- **Title:** Cyber Risk and Resilience in U.S. Public Firms
- **Authors:** Luc Renneboog, Jasmin Gider, Tal Strauss
- **Affiliation(s):** Tilburg University, ECGI, European Central Bank
- **Publication:** Working Paper, Chapter of PhD Thesis of Tal Strauss (under supervision of L. Renneboog and J. Gider)
- **Full paper available at:** Cyber Risk, Regulation, and Firm Resilience