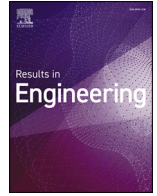






ELSEVIER

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: [www.sciencedirect.com/journal/results-in-engineering](http://www.sciencedirect.com/journal/results-in-engineering)

# Cyber incident disclosure—lessons from CO<sub>2</sub>e emissions disclosure

Ulrik Franke <sup>a,\*</sup>, Jan Svanberg <sup>b</sup>

<sup>a</sup> Swedish Defence University, Box 278 05, SE-115 93, Stockholm, Sweden

<sup>b</sup> University of Gävle, SE-801 76, Gävle, Sweden

## ARTICLE INFO

### Keywords:

Cybersecurity  
Externalities  
Asymmetric information  
Information disclosure  
Cyber incidents

## ABSTRACT

Modern society depends on IT services, but unfortunately, IT services are not always dependable. Cyber incidents occur all the time, caused by bad design or by bad incentives. To address the latter cause, disclosure of cyber incidents has been proposed. Learning about incidents, buyers will find it worthwhile to select and pay for secure vendors, thus contributing to better overall security. While this logic has solid theoretical foundations in the economics of negative externalities and asymmetric information, the practice of cyber incident disclosure is only just emerging, as is empirical research on its effects. However, valuable lessons might be learned from the literature on the more mature practice of CO<sub>2</sub>e emissions disclosure. Based on the extant literature on CO<sub>2</sub>e emissions disclosure, two hypotheses about cyber incident disclosure are derived: First, it is likely that increased cyber incident disclosure would increase the costs of equity and debt for companies with many and/or severe cyber incidents, and also expose them to shareholder activism as well as to decreasing demand. Second, these effects will be smaller for cyber incident disclosure than the corresponding effects for CO<sub>2</sub>e emissions disclosure. The article is concluded with a discussion of implications and future work.

## 1. Introduction

Modern society is increasingly dependent on IT services. Today, these services underpin our work, leisure, social interaction and cultural experiences, as well as global supply-chains and financial transactions. At its best, digitalisation offers both incremental improvements—things we could do previously become more efficient—and quantum leaps—novel things are made possible for the first time.

Unfortunately, IT services are not always dependable and secure. Cyber incidents, some small, some large, occur all the time. Whether caused by adversarial attacks or by non-adversarial errors, omissions, and accidents, such incidents can have very large consequences; monetary [see, e.g., 1–4] as well as non-monetary [5]. A recent attempt to systematise the knowledge on how to quantify cyber risk is given by Woods and Böhme [6].

Why do such cyber incidents occur? Naturally, this question is often approached from the technical angle. However, cybersecurity is not *only* a technical problem. Cybersecurity problems arise when people use technology in an organisational, legal, and economic setting. No amount of technical solutions can prevent harm if legitimate users, managers, or regulators make bad decisions. Thus, it is futile to try and solve all cybersecurity problems with technology alone—other perspectives such as behavioural science [7], management [8], or law [9] are equally legitimate.

### 1.1. Cybersecurity economics

One such complementary perspective on cybersecurity is economics, as introduced by Anderson and Moore [10] in an influential *Science* article. Security failure is caused “at least as often by bad incentives as by bad design”, they argue, and go on to explain why this is the case: First, in an interconnected world, poor security is a *negative externality*. In other words, if any one actor has poor security, this also poses a risk to other actors. (Think of how malware spreads through networks, or how cloud service providers are single points of failure affecting a multitude of customers.) While it makes sense to invest a bit to protect oneself, it does not make sense to invest enough to protect everyone with whom one interacts, just to see one’s effort undercut by the neglect of someone else. Therefore, it is generally believed that we invest too little in cybersecurity [11].<sup>1</sup>

Second, security suffers because of *asymmetric information*, where vendors may claim that their software and services are secure, but

<sup>1</sup> It should be noted, however, that this is not the whole story. Theoretically, there are models where overinvestment rather than underinvestment in security occurs [12], and empirically it is not clear that firms really do invest too little in cybersecurity [13]. More research is needed to better understand the subtleties of cybersecurity investment and to create mechanisms to funnel investments among interdependent firms to where the money is most useful [14].

\* Corresponding author

E-mail addresses: [ulrik.franke@fhs.se](mailto:ulrik.franke@fhs.se) (U. Franke), [jan.svanberg@hig.se](mailto:jan.svanberg@hig.se) (J. Svanberg).

<https://doi.org/10.1016/j.rineng.2026.110137>

Received 17 April 2025; Received in revised form 7 August 2025; Accepted 16 March 2026

Available online 17 March 2026

2590-1230/© 2026 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

buyers have a hard time verifying such claims. Unable to tell secure from insecure software, buyers are reluctant to pay for security, and in the absence of demand, supply collapses. Thus, argue [Anderson and Moore](#), the software market is a ‘market for lemons’, as famously described by [Akerlof \[15\]](#), who uses the market for used cars to illustrate the troubles of asymmetric information.

### 1.2. Cyber incident disclosure

Such reasoning is not only illuminating, but also practical: it suggests solutions. More precisely, various forms of *information disclosure* have been proposed as an important remedy to the problem of asymmetric information in cybersecurity [\[16,17\]](#). If cyber incidents were regularly disclosed to the general public, the reasoning goes, this would allow customers to distinguish more secure services from less secure ones, creating a demand and a willingness-to-pay entailing a better market offering of secure services. Similarly, if incidents were disclosed to investors and banks, this would limit the availability of equity and debt for insecure companies; if incidents were disclosed to governments, this would enable them to enact and evaluate regulations promoting security; if incidents were disclosed to insurers, this would enable them to reward practices good for security and punish practices bad for security through the pricing of premiums. Thus, while many forms of disclosure are conceptually possible, they all share a similar basic mechanism which offers some promise to rectify misaligned incentives a bit by making information less asymmetric. At the same time, all kinds of disclosures need to balance the risk that they help cyber-attackers more than cyber-defenders [see, e.g., [18–20](#)].

Recent years have seen the implementation of some such disclosure practices. Most prominently, privacy breach laws, requiring notification to individuals whenever their personal data has been compromised, were enacted throughout the US states starting with California in 2002. Subsequent studies show that reports of breaches have a negative impact on the stock prices of the offending companies [\[21\]](#) and also that the number of data breaches fell after breach notification laws were introduced [\[22,23\]](#).

More recently, the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive) came into force in the EU in 2018. A second iteration of the latter, NIS 2, came into force in most affected countries in 2024 or 2025, though some still lag behind. Both laws introduce similar reporting regimes, where privacy incidents (GDPR) and loss of service incidents (NIS) must be reported to the authorities. (It should also be pointed out that both laws are agnostic about the origin of incidents—unintentional mistakes and deliberate attacks alike must be reported.) While general economic effects of the GDPR have been evaluated [\[24\]](#), the particular effect of the incident reporting still awaits thorough empirical evaluation. Similarly, to the extent of our knowledge, there is no large empirical evaluation of the NIS reporting, though there is evidence suggesting that it suffers from poor data quality [\[25\]](#).

Cyber incident reporting, and more generally cyber risk reporting, also occurs in annual and quarterly reports, news releases, etc., from publicly traded companies. Sometimes, such data has proven useful for research [e.g. [3](#), who use it to estimate breach costs for their regression model], but at the same time, studies indicate that cybersecurity disclosure levels are low [\[26\]](#), that disclosures are not very specific [\[27,28\]](#), and that the language of disclosures makes them difficult to read [\[29\]](#). Systematic reviews typically point out flaws in reporting standards and data quality and call for more mandatory reporting of cyber incidents [\[30\]](#) according to better standards [\[31\]](#).

Thus, while the theory of cyber incident disclosure is well established, the practice is uneven. Some practices, such as privacy breach laws, are mature and their effects well researched [\[22,23\]](#). Other practices, such as the mandatory reporting under GDPR and NIS, have been around for a few years and there is some research [\[25\]](#), but many open questions remain. Yet other practices, such as the new cyber incident

disclosure requirements from the US SEC [\[32\]](#) announced in July 2023 are only just emerging, and empirical research on the effects mostly remains future work, though some evidence is now becoming available [e.g., [33,34](#)]. These gaps in research lead to the research question of this article: *What lessons relevant for cyber incident disclosure can be learned from the literature on CO<sub>2</sub>e emissions<sup>2</sup> disclosure, a much more mature practice?*

### 1.3. Learning from CO<sub>2</sub>e emissions disclosure

The similarity between cyber incidents and pollution is not a new observation—indeed, the analogy comes naturally if the externality perspective on vulnerable systems is adopted. An extensive discussion of the idea is given by [Sales \[9, pp. 1525–1528\]](#). Arguing the case for disclosure, [Moore \[17\]](#) makes an explicit parallel to the US legislation mandating any toxic chemicals released into the environment to be reported and released to the public in the form of the Toxics Release Inventory.<sup>3</sup>

Compared to cyber incidents, the state of the practice when it comes to climate-related disclosures is much more mature and well-researched. Even though some disclosure regimes came into effect only recently (the US Securities and Exchange Commission adopted its latest sets of rules on climate-related disclosures in March 2024 [\[35\]](#)) and others are still preliminary (also in March 2024, the Basel Committee on Banking Supervision closed a public consultation on upcoming climate-related disclosures for the banking sector [\[36\]](#)). But such rules build on years of accumulated experience from voluntary schemes and standards such as those set by the Global Reporting Initiative (GRI), the Carbon Disclosure Project (CDP), the Sustainability Accounting Standards Board, the Task Force on Climate-related Financial Disclosures (TCFD), and the Climate Disclosures Standards Board [\[37\]](#). For cyber incident disclosure, this means that there is much to learn.

The remainder of this article is structured as follows. In [Section 2](#), the literature on CO<sub>2</sub>e emissions disclosure is surveyed. In [Section 3](#), CO<sub>2</sub>e and cybersecurity are systematically contrasted. To avoid oversimplification, similarities and differences are systematically enumerated in [Sections 3.1](#) and [3.2](#), respectively. Weighing similarities and differences, a balanced synthesis is found and the lessons from CO<sub>2</sub>e emissions disclosure are used to form plausible hypotheses about the effects of cyber incident disclosures. [Section 4](#) concludes the article.

## 2. The literature on CO<sub>2</sub>e emissions disclosure

Climate risks have real effects on companies. Some companies, such as farmers and insurers, incur direct costs related to climate change. Others are more indirectly effected, e.g., by policies and regulations enacted to counter climate change, such as emission ceilings and carbon prices [\[38\]](#). All companies, finally, are impacted by technological changes such as increased use of solar panels and electric vehicles.

As companies face changing circumstances, investors face the choice of rebalancing their portfolios, for instance by selling equities in coal and oil, traditional car manufacturing, deforestation etc., and instead buying equities in renewable energy or energy storage. It is widely believed that a transition in financial markets, possibly volatile, is taking place, with a net outflow of capital from climate impacting sectors and companies to climate mitigating sectors and companies [\[39\]](#). In the following, effects on companies are discussed in four areas—cost of equity, cost of credit, shareholder activism, and consumer and procurement behaviour.

<sup>2</sup> Throughout this article, we adopt the common practice of using the term CO<sub>2</sub>e—carbon dioxide equivalent—to denote all greenhouse gas emissions, regardless of their exact chemical composition.

<sup>3</sup> <https://www.epa.gov/tri>

## 2.1. Cost of equity

Institutional investors control a large part of the world's invested capital and they are by far the largest investors in equity. Institutional investors increasingly believe that climate risks impact portfolio firms and that regulatory risks in particular are already material [39]. The effects of disclosing climate impact must therefore be sought in how institutional investors act on this information. For example, Ramelli et al. [40] found that investors react to political risks they perceive as associated with firms' climate strategies. Many institutional investors consider active engagement in portfolio companies to be the better approach to deal with climate risks, but divestment is still a viable option [41]. Institutional investors' avoidance of investment in climate impacting equity causes climate perpetrators to suffer not only the effects of law suits, government punishment, customer boycotts and disrupted production [42], but also the direct impact of higher costs of equity [41]. Some studies indicate that climate impacting companies would have higher cost of equity than other companies and that the climate impacting companies could decrease their cost of equity by improving environmental policies [43]. Other studies find that environmental policies are related to lower downside and overall portfolio risk [44], suggesting that disclosing poor or no environmental policies could increase the downside and risk.

Unless a company is very much a representative of renewable energy or has products and services that clearly indicate that the company is in fact a climate mitigator, if compared to traditional companies, institutional investors are most likely concerned with climate risks when considering ESG (Environmental, Social, Governance) issues in their investment process [45]. This means that investors are not so much looking for good climate performance as they want to avoid climate impacting equities. Such investors shy away from companies with a high climate impact, which means that such companies will typically not be attractive to own for a large fraction of the investor collective [46]. In line with this, some evidence suggests that it does not pay off to seek the strong environmental performers but that it is really profitable to avoid investing in the bad ones. Flammer [47] claims that the responsibilities to the environment have increased to the extent that this exacerbates the punishment of companies that do not take their responsibilities and reduces the rewards for positive environmental initiatives beyond those that are required. A recent study found that the cost of capital for climate impacting firms may be impacted in the range of 8–10 % in countries with high climate awareness after 2015 [41]. In such circumstances, it is not irrational for firms to take action to avoid divestment.

The long-term effects of investor climate mitigation preferences on the cost of equity financing of climate impacting companies is mirrored by short-term negative reactions to bad environmental news [48]. Thus, the long-term effect for many traditional companies (i.e. companies not belonging to the narrow group of environmental innovators) with substantive climate impact is probably an exposure to a higher risk of increased cost of equity.

## 2.2. Cost of debt

There are also likely impacts on a company's cost of debt financing. Greater climate risk should lead to lower firm leverage because the total risk of the company would have to be consistent with investor preferences and the debt market. If climate risks would increase then either companies themselves would decrease their demand for debt and/or lenders would reduce their lending to firms with the greatest climate risks [49]. Another effect would be that banks price climate risks of their loans, which has been the case after the Paris Agreement [50]. Climate impacting companies are rated not only in terms of ESG, which should discredit the climate perpetrators, although that varies with ratings [51,52] because credit ratings and yield spreads take into account CO<sub>2</sub>e emitting firms [38]. There is recent evidence that climate risk disclosure decreases access to finance and increases cost of debt [53]. Ev-

idence also reveals that disclosing poor environmental or social performance that affects ESG ratings increases cost of debt [54]. In conclusion, considering that climate impact is held as the most serious environmental issue of today, it is unlikely that disclosure of poor performance on the climate issue would lead to anything but higher cost of debt for the individual company.

## 2.3. Shareholder activism

A recent survey of large institutional investors found that shareholder activism is the preferred mode of operation for institutional investors in their ambition to reduce portfolio risk and fulfil their fiduciary duty to beneficiaries [39], confirming a previous study that found only 19 % of institutional investors did not engage in their portfolio companies [55]. We therefore expect that companies disclosing a substantial climate impact would have to encounter institutional investors intervention in their board of directors' governance of the company. Their intervention would have a constraining effect on the current manner in which such companies are operated. According to recent research, shareholder activism causes significant decreases of CO<sub>2</sub>e emissions as the most important result [41,56].

## 2.4. Consumer and procurement behaviour

A fourth stakeholder reaction to CO<sub>2</sub>e disclosure is customers shying away from companies they perceive as climate threats. The effects do not have to be large scale protests but can be the outcome of many small purchase decisions made every day by billions of potential customers. Not only other companies, but even consumers react to what companies' accounting discloses. For example, consumers buying medicine consider the profit margin of highly priced products unjustified and tend to avoid them in favour of alternatives produced with more justifiable margins [57]. A similar effect should be expected for CO<sub>2</sub>e disclosure which is the most high-profiled environmental issue of today. Customers, perhaps mostly consumers, may avoid CO<sub>2</sub>e intensive products by shifting diets [58–60], transport behaviour [61,62], household purchasing [63,64], disposal of products [65], and energy use [66]—all of which will impact producers and distributors of products and services.

The customer actions can be more organised boycotts with substantial impacts on companies' reputation when consumers punish irresponsible companies by collectively not buying [67,68]. 42 % of the Fortune 50 and 54 % of Interbrand top 50 have faced boycotts [69] often associated with reduced financial performance [70]. Boycotts of climate intensive businesses appear likely due to the strong commitment among young people to fight climate change. Disclosing CO<sub>2</sub>e to the extent that a business is perceived as a climate unfriendly company could therefore initiate boycotts through consumer movements [71,72]. CO<sub>2</sub>e boycotts would create considerable negative publicity and boycotts damaging brand image [73] causing long-lasting negative perceptions among consumers [74]. The financial effects of boycotts on firm profitability is most likely negative and the effect on shareholders is at least in the short term negative [75].

## 3. Hypotheses on the effects of cyber incident disclosures

Based on the literature review, the research question can now be tentatively answered. First, some similarities and differences between cyber incident and CO<sub>2</sub>e emissions are identified, to facilitate the analysis.

### 3.1. Similarities between cyber incidents and CO<sub>2</sub>e emissions

As pointed out in the introduction, the parallel between cyber incidents and CO<sub>2</sub>e emissions, or pollution in general, is not new. Anderson et al. [16] remark: "Just as a factory belching out smoke into the environment creates a negative externality for people downwind—and indeed for the whole world in the case of global warming—so also people who

connect infected PCs to the Internet create negative externalities in that their machines may emit spam, host phishing sites and distribute illegal content such as crimeware.” (The truth and relevance of this observation is not decreased by the fact that we now to connect all kinds of infected devices besides PCs to the internet—quite the contrary.)

In the following, a number of similarities are made more precise:

- S1** A first similarity is thus that cyber incidents and CO<sub>2</sub>e emissions alike are negative externalities which occur as side-effects in the production of goods. It may be argued that this similarity is overstated—whereas CO<sub>2</sub>e emissions are a necessary chemical consequence of artefacts such as combustion engines or blast furnaces, cyber incidents are not a necessary consequence of internet banking or industrial use of the Internet-of-things. For each cyber incident, some hypothetical countermeasure that would have prevented it can be imagined. However, avoiding cyber incidents *altogether* stretches the imagination too far. That *some* incidents will occur remains an unavoidable side-effect of modern use of information technology in enterprises.
- S2** A second similarity is asymmetric information: buyers cannot easily inspect a product to discover its full CO<sub>2</sub>e footprint or its cybersecurity properties. This requires specialist competence and a potentially costly effort. Third-party vetting or guarantees offered by the vendor are mechanisms that can alleviate this problem, but not solve it altogether [76]. (Indeed, sometimes it is not so much a matter of asymmetric information as of a more fundamental *lack* of information: in the absence of CO<sub>2</sub>e reporting schemes throughout supply chains, even manufacturers and vendors may be ignorant about the CO<sub>2</sub>e footprint of their products; similarly, most if not all products contain cyber vulnerabilities that are initially unknown even to their creators. However, there may still be an asymmetry between sellers and buyers, in that the former are in a better position to investigate what they do not know.)
- S3** A third similarity is that much of the activities entailing cyber incidents and CO<sub>2</sub>e emissions are conducted by companies; many of which are publicly traded, some of which are privately held, but all of which are subject to the market forces of equity and credit. (In addition, of course, in both cases, the activities of government agencies, NGOs, and private individuals also contribute to both CO<sub>2</sub>e emissions and cyber incidents).
- S4** A fourth similarity is an effect mentioned by Akerlof [15, Section IV]: that brand names are an institution counteracting the adverse effects of asymmetric information. Indeed, empirical investigations show that company brands and valuations can suffer from disclosure of cyber incidents [77] or emissions [48]. Such effects give companies with strong brands compelling incentives to avoid cyber incidents and keep emissions low (Anderson et al. [16] mention Microsoft as an example of a strong brand that is improving its security—which is not to say that it could not be further improved). Sometimes entire industries can have similar positive incentives; e.g., the financial industry is very much in the business of trust (think of financial stability and bank-runs) and so works diligently with cybersecurity [see, e.g., 78]. Still, of course, there are limits to this argument: some empirical findings suggest that only the largest and most salient data breaches actually decrease intangible capital such as brand reputation [79]. Furthermore, the evidence is mixed about whether visibly improving cybersecurity through certification [80] or disclosures about investments to regulators [81] is rewarded or punished by the stock market. Limits to S4 are further explored in D4 below.
- S5** A fifth similarity is that there can be a temporal delay between cause and effect: sometimes, the true cost of poor cybersecu-

rity is only revealed in the long run, similar to the true cost of CO<sub>2</sub>e emissions accumulating in the atmosphere. This temporal delay manifests itself in reports of advanced persistent threats being inside targeted networks for months before being discovered [82,83]. There is empirical evidence suggesting that the market reaction is more negative when it takes longer for target firms to discover that the attack, suggesting that such perceived incompetence is punished by the market [84]. It has also been pointed out that startups may deliberately defer security, first aiming to create a viable product, only later making it secure [10]. In the longer run, such a strategy may be costly. Limits to S5 are further explored in D5 below.

- S6** A sixth similarity is that both CO<sub>2</sub>e emissions and cyber incidents occur as the results of complex value chains with many stakeholders involved. It is not *a priori* clear who should report a particular emission, when goods and services are created from other goods and services produced by suppliers, who may themselves be in a similar situation. This complexity also offers opportunities for greenwashing and blame games [85,86]. Similarly, it is not *a priori* clear who should report a particular cyber incident, when IT services are created from other IT services produced by suppliers, who may themselves be in a similar situation. Similarly to greenwashing, this may also offer opportunities for “security-washing”, such as uninformative “boilerplate” disclosures, though its actual prevalence is subject to debate [29,34,87–89]. But here the lesson from CO<sub>2</sub>e emissions is that the *a priori* qualification really matters: After appropriate deliberation, it is perfectly possible to come up with reasonable standards which define cyber incidents more precisely, avoid double-counting and delineate responsibilities. Though such standards may not be perfect, they can be proposed, tried out, and iteratively updated in a way that suggests that in the end they will be good enough to serve their purpose. Eventually, higher maturity and mandatory reporting regimes for CO<sub>2</sub>e emissions have turned out to reduce greenwashing [90,91].

### 3.2. Differences between cyber incidents and CO<sub>2</sub>e emissions

A striking difference concerning the disclosures of cyber incidents and CO<sub>2</sub>e emissions, respectively, is that the latter is a much more mature practice. As pointed out in the introduction, this is an important part of the motivation for this paper. For example, similarity S6 illustrates precisely such a difference of maturity. However, this gap is contingent, and may indeed be closed over the coming years, if disclosure of cyber incidents becomes a more frequent practice. This is why S6 is listed as a similarity—the differences are contingent, but the similarity is fundamental.

Thus, it is more interesting to consider differences of a more fundamental nature, not likely to ever be closed. In the following, a few such are listed.

- D1** A first difference is that whereas CO<sub>2</sub>e emissions are essentially only negative externalities, cybersecurity has an element of positive externality as well, as pointed out by Sales [9]: whenever a company invests in making its systems more secure, it also makes those systems less accessible as an attack vector against someone else. A more secure system at company A becomes less prone to spread malware to company B.
- D2** A second difference is that there is a stochastic element to cybersecurity that is not present in CO<sub>2</sub>e emissions. Whereas running a certain industrial process in a certain way results in certain emission levels, running certain business processes in information systems of a certain cybersecurity level results in an *uncertain* number of cyber incidents of *uncertain* severity. While cybersecurity laggards are more probable to experience severe incidents,

they may still be lucky. Conversely, while cybersecurity leaders are less probable to experience severe incidents, they may still be unlucky. This stochastic element is an important part of the appeal of *cyber insurance*, a mechanism allowing risk sharing across a large population of insureds, evening out precisely this stochastic element [see, e.g., 92–94]. Importantly, this stochastic element also highlights the importance of distinguishing between studies of the effects of disclosing (i) cybersecurity investments and (ii) cyber incidents. For CO<sub>2</sub>e, an investment in proven technology to reduce emissions is equivalent to a reduction in emissions, but for cyber incidents, an expensive investment is no guarantee of fewer incidents. This helps explain why even though there are studies indicating that lender reactions to cyber incidents are negative [95,96], studies of stock market reactions to visible cybersecurity investments show mixed results [80,81]. The stochastic nature of cyber events by its very nature makes the data noisy and difficult to interpret. In particular, it is difficult to accurately estimate the statistical properties of very rare events [97]. Furthermore, the outcomes of such statistical analyses are sensitive to assumptions. Carfora and Orlando [98] offer an instructive example, demonstrating how the same data on probabilities and consequences of breaches can be modelled in many different ways, resulting in different risk assessments. This is particularly important to understand when using simulations for cybersecurity decision-making [99].

**D3** A third difference, mentioned in the introduction, is the existence of the attacker: cyber incident disclosures risk helping cyber-attackers more than cyber-defenders. There is no corresponding risk with CO<sub>2</sub>e emissions disclosures. In particular, with respect to cyber incident disclosures, it has been claimed that “[i]f Registrants’ disclosures contain sufficient information to be meaningful for investors, disclosures almost certainly will have to contain information of value to Adversaries seeking reconnaissance data that will facilitate a breach or enhance its ability to exploit a cyber-vulnerability” [18]. Such worries get some support from studies showing that software vulnerabilities are increasingly attacked after they are disclosed [100] or after a patch becomes available [101]. But on the other hand, incident disclosure is different from vulnerability disclosure in that much less information is needed for market actors to be able to react compared to what is needed for vendors to write patches. Thus, it may be that the potential negative effects of incident disclosure are smaller than the potential negative effects of vulnerability disclosure. However, it is very difficult ascertain whether the positive or the negative effect—the help to attackers or the help to defenders—dominates. Indeed, what is probably the best theoretical investigation, by Ross Anderson, shows that under idealized circumstances, the two effects are exactly equal [102]. Thus, the only way to find out is to carefully look at the particular case at hand and try to work out the net effect. It is important to remember, though, that not all cyber incidents involve adversarial attackers—many are just the result of non-adversarial errors, omissions, and accidents. In the attacker respect, such incidents are more similar to CO<sub>2</sub>e emissions.

**D4** A fourth difference, and a contrast to similarity S4 about brand names suffering, is related to market concentration. If strong brands suffer more from embarrassing CO<sub>2</sub>e emissions disclosures, and as a result work harder to bring those emissions down, then from a CO<sub>2</sub>e perspective, it would be good if those strong brands grew to obtain even greater market shares. (Of course, from other perspectives such as consumer prices, this may nevertheless be bad.) However, because of the existence of strategically behaving attackers, the analogous proposition for cybersecurity does not hold. If strong brands suffer more from embar-

rassing cyber incident disclosures, and as a result work harder to prevent those incidents, then from a cybersecurity perspective, it would still be an *open question* whether overall security would improve by those brands obtaining even greater market shares. While work to prevent incidents may improve, convincing arguments have been made that increased market concentration may increase the total volume of systemic cyber risk as attackers can focus their efforts on a few high-value targets, so that diversity of systems, software and firms becomes a virtue in its own right (see Geer et al. [103]; Franke and Hoxell [104] formalise one of their arguments mathematically). Similarly, disclosure requirements may themselves inadvertently encourage homogenization, e.g., through compliance with standardized security frameworks, and thus entail less diversity in security practices. By these arguments, paradoxically, a diverse market of lesser brands may be better than an oligopoly of stronger brands, even if the lesser brands are less conscious and conscientious about their cybersecurity than the stronger brands, and a diversity of security practices may be better than widespread conformity to best practice. As with respect to D3, what is preferable here must be a case-by-case assessment, not something to be determined once and for all *a priori*.

**D5** Similarity S5 is about temporal delays between cause and effect. However, as pointed out above, this similarity only holds sometimes. Whereas the adverse effects of CO<sub>2</sub>e emissions only become evident in the long run, the effects of poor cybersecurity practices are sometimes immediately felt, but sometimes only become evident after a while.

### 3.3. Hypotheses

Following the enumerations of similarities and differences, two hypotheses about the effects of cyber incident disclosures can be formed:

**H1** A first hypothesis is that, qualitatively, all the effects listed in Section 2 can be expected to hold for cyber incident disclosure as well. In other words, it is likely that increased cyber incident disclosure would increase the costs of equity and debt for companies with many and/or severe cyber incidents, and also expose them to shareholder activism as well as to decreasing demand.

The arguments for this hypothesis are the similarities S1–S6, as well as some empirical evidence. Whereas early empirical studies were conducted using data on cyberattacks and loans from before the advent of mandatory disclosure [95,96], more recently, the staggered passing of mandatory data breach disclosure laws across the US states has enabled more detailed studies of how this affects the cost of debt. Agarwal et al. [33] find that such laws lead to an increase in the cost of debt for firms affected. As for shareholder activism related to cyber incidents, no empirical evidence has been found—exploring this relationship is listed by Chuah et al. [105, Table 4] as a suggestion for future research.

A general argument against this hypothesis is the phenomenon of *disclosure fatigue* [106], where a large number of breach reports overwhelm observers, with ever decreasing effects on actual behaviour. With respect to investors, Charoen and Khern-am-nuai [107] indeed find the negative stock market reaction to data breach announcements to be smaller in recent years than in the past decade. With respect to consumers, Markos et al. [108] report some evidence that consumers consider incidents “a new reality” and “something we will get used to”, but put the details of desensitization—especially differences between medical data breaches and other industries—on their agenda for future research. However, it is clear that reactions to incidents vary across industries, whether with respect to cost of debt [33] or consumer attitudes [108].

Thus, while the impacts may look different in different industries, in general, H1 is expected to hold.

H2 A second hypothesis is that, quantitatively, the effects listed in H1 will be *smaller* for cyber incident disclosure than the corresponding effects for CO<sub>2</sub>e emissions disclosure.

The arguments for H2 are:

- By D1, cybersecurity is a less clear-cut case of negative externality than CO<sub>2</sub>e emissions. With this different problem structure, the effects of disclosure can be expected to be smaller.
- By D2, the information value of disclosure is smaller for cyber incidents than for CO<sub>2</sub>e emissions. In particular, time-series of disclosed figures will be subject to the phenomenon of regression toward the mean, and it would thus be unwise for investors to pay too much attention to any individual disclosed figures. Similarly, since the same data can be modelled in many different ways [98], it may be unwise to pay too much attention to any particular model unless there are very good reasons for it. These difficulties may dilute the impact of disclosure on investors.
- By D3, some disclosures are counterproductive, helping attackers more than defenders. Unfortunately, it is not obvious which disclosures are which, nor whether the *net* effect in a particular case at hand is positive or negative. Thus, *ceteris paribus*, the overall positive effects of cyber incident disclosure can be expected to be smaller than those of CO<sub>2</sub>e disclosure, where this complication is absent.

Conversely, there are also arguments against H2:

- By D4, brands are a less effective counteracting institution against the adverse effects of asymmetric information for cybersecurity than for CO<sub>2</sub>e emissions. Thus, disclosure may, relatively, be more important for cybersecurity.
- By D5, the effects of poor cybersecurity are sometimes more immediate than those of CO<sub>2</sub>e emissions. Thus, disclosure of (some types of) cyber incidents might have greater effects than disclosure of CO<sub>2</sub>e emissions. However, delayed discovery of advanced persistent threats suggests that such immediacy is far from always the case, removing some force from this counterargument.

On a balance, the arguments for H2 are assessed to outweigh those against. More precisely, the effects in the arguments from D1, D2, and D3 are considered stronger and more certain than the effects in the arguments from D4 and D5.

#### 4. Conclusions

CO<sub>2</sub>e emissions and poor cybersecurity share some common characteristics; most importantly that they impose negative externalities on others and are subject to asymmetric information. As a result, disclosure of CO<sub>2</sub>e emissions and cyber incidents, respectively, have been proposed as partial remedies to some of the resulting problems.

Of the two disclosure practices, CO<sub>2</sub>e emissions disclosure is the more mature, with a plethora of reporting initiatives backed by an ever-growing number of important stock exchanges and regulators. Comparatively, cyber incident disclosure is in its infancy. Laws such as the NIS Directive and GDPR in the EU and the cyber disclosure rules mandated by the US Securities and Exchange Commission were enacted only recently. Thus, empirical research on the effects of cyber incident disclosure is only just emerging.

This article has investigated what lessons relevant for cyber incident disclosure can be learned from the literature on the more mature practice of CO<sub>2</sub>e emissions disclosure. Based on the analysis of the extant literature, two hypotheses seem plausible: First, that it is likely that increased cyber incident disclosure would increase the costs of equity and debt for companies with many and/or severe cyber incidents, and also expose them to shareholder activism as well as to decreasing demand. Second, that these effects will be *smaller* for cyber incident disclosure than the corresponding effects for CO<sub>2</sub>e emissions disclosure.

Clearly, these hypotheses call for further future investigation. As cyber incident disclosure schemes mature and more data becomes available, it will be interesting to test the hypotheses developed empirically, and thus learn more about what can, and cannot, be achieved by such disclosures. However, the second hypothesis also has more practical relevance: if indeed the power of cyber incident disclosure is limited compared to that of CO<sub>2</sub>e emissions disclosure, this is an invitation to design and implement complementary measures to counter the adverse effects of negative externalities and asymmetric information in the cyber realm. One such measure would be to increase existing disclosure. Some disclosure regimes, such as those mandated by GDPR and NIS in the EU, only require disclosure to the relevant government agencies, not to the public. This may unnecessarily limit the positive effects. Another measure would be to think creatively about who sets disclosure requirements. Not only governments can do so, but many other actors, such as stock exchanges, banks, insurers, and anyone buying products could potentially declare that firms need to publicly disclose cyber incidents in order to have their shares traded, get loans, get insurance, sell their products, etc. Surely, many other complementary measures can be imagined. However, as a final lesson from the literature on CO<sub>2</sub>e emission reduction, we should also learn that it is possible to use randomized controlled trials to make policy as effective as possible [see, e.g., 109–111]. The power of such trials should be borne in mind when developing and experimenting with cybersecurity policy in general and incident disclosure regimes in particular.

#### CRedit authorship contribution statement

**Ulrik Franke:** Writing – review & editing, Writing – original draft, Investigation, Conceptualization; **Jan Svanberg:** Writing – review & editing, Writing – original draft, Investigation, Conceptualization.

#### Data availability

No data was used for the research described in the article.

#### Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

#### Acknowledgements and disclosures

This work was supported by Länsförsäkringsgruppens Forsknings- & Utvecklingsfond, agreement no. P4/18 (U. Franke) and agreement no. P8/18 (J. Svanberg).

#### References

- [1] S. Romanosky, Examining the costs and causes of cyber incidents, *J. Cybersecur.* 2 (2) (2016) 121–135. <https://doi.org/10.1093/cybsec/tyw001>
- [2] M. Eling, J. Wirfs, What are the actual costs of cyber risk events?, *Eur. J. Oper. Res.* 272 (3) (2019) 1109–1119. <https://doi.org/10.1016/j.ejor.2018.07.021>
- [3] O.I. Poyraz, M. Canan, M. McShane, C.A. Pinto, T.S. Cotter, Cyber assets at risk: monetary impact of US personally identifiable information mega data breaches, *Geneva Paper. Risk Insurance—Issues Practice* 45 (4) (2020) 616–638. <https://doi.org/10.1057/s41288-020-00185-4>
- [4] U. Franke, IT Service outage cost: case study and implications for cyber insurance, *Geneva Paper. Risk Insurance—Issues Practice* 45 (4) (2020) 760–784. <https://doi.org/10.1057/s41288-020-00177-4>
- [5] I. Agrafiotis, J.R.C. Nurse, M. Goldsmith, S. Creese, D. Upton, A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate, *J. Cybersecur.* 4 (1) (2018) ty006. <https://doi.org/10.1093/cybsec/ty006>
- [6] D.W. Woods, R. Böhme, SoK: Quantifying cyber risk, in: 2021IEEE Symposium on Security and Privacy (SP), 2021, pp. 211–228. <https://doi.org/10.1109/SP40001.2021.00053>
- [7] B. Lebek, J. Uffen, M. Neumann, B. Hohler, M.H. Breitner, Information security awareness and behavior: a theory-based literature review, *Manag. Res. Rev.* (2014). <https://doi.org/10.1108/MRR-04-2013-0085>

- [8] A. Dutta, K. McCrohan, Management's role in information security in a cyber economy, *Calif. Manag. Rev.* 45 (1) (2002) 67–87. <https://doi.org/10.2307/41166154>
- [9] N.A. Sales, *Regulating cyber-security*, *Northwest Univ. Law Rev.* 107 (4) (2012) 1503–1568.
- [10] R. Anderson, T. Moore, The economics of information security, *Science* 314 (5799) (2006) 610–613. <https://doi.org/10.1126/science.1130992>
- [11] L.A. Gordon, M.P. Loeb, W. Lucyshyn, L. Zhou, et al., Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model, *J. Inf. Secur.* 6 (01) (2014) 24. <https://doi.org/10.4236/jis.2015.61003>
- [12] D. Acemoglu, A. Malekian, A. Ozdaglar, Network security and contagion, *J. Econ. Theory* 166 (2016) 536–585. <https://doi.org/10.1016/j.jet.2016.09.009>
- [13] M. Dinkova, R. El-Dardiry, B. Overvest, Should firms invest more in cyber-security?, *Small Bus. Econ.* 63 (1) (2024) 21–50. <https://doi.org/10.1007/s11187-023-00803-0>
- [14] U. Franke, A. Orlando, Interdependent cyber risk and the role of insurers, *Res. Econ.* 79 (3) (2025) 101059. <https://doi.org/10.1016/j.rie.2025.101059>
- [15] G.A. Akerlof, The market for “Lemons”: quality uncertainty and the market mechanism, *Q. J. Econ.* 84 (3) (1970) 488–500. <https://doi.org/10.2307/1879431>
- [16] R. Anderson, R. Böhme, R. Clayton, T. Moore, Security economics and European policy, in: N. Pohlmann, H. Reimer, W. Schneider (Eds.), *ISSE 2008 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2008 Conference*, Vieweg+Teubner, Wiesbaden, 2009, pp. 57–76. [https://doi.org/10.1007/978-3-8348-9283-6\\_6](https://doi.org/10.1007/978-3-8348-9283-6_6)
- [17] T. Moore, The economics of cybersecurity: principles and policy options, *Int. J. Crit. Infrastruct. Prot.* 3 (3–4) (2010) 103–117. <https://doi.org/10.1016/j.ijcip.2010.10.002>
- [18] R.L. Trope, S.J. Hughes, The SEC Staff's cybersecurity disclosure guidance: will it help investors or cyber-thieves more, *Bus. Law Today* (2011) 1–4. <https://www.jstor.org/stable/businesslawtoday.2011.12.04>
- [19] A. Albakri, E. Boiten, R. De Lemos, Risks of sharing cyber incident information, in: *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–10. <https://doi.org/10.1145/3230833.3233284>
- [20] S. Schmitz-Berndt, S. Schiffner, Don't tell them now (or at all)—responsible disclosure of security incidents under NIS directive and GDPR, *Int. Rev. Law Comput. Technol.* (2021) 1–15. <https://doi.org/10.1080/13600869.2021.1885103>
- [21] A. Acquisti, A. Friedman, R. Telang, Is there a cost to privacy breaches? an event study, *ICIS 2006 Proc.* (2006) 94.
- [22] S. Romanosky, R. Telang, A. Acquisti, Do data breach disclosure laws reduce identity theft?, *J. Policy Anal. Manag.* 30 (2) (2011) 256–286. <https://doi.org/10.1002/pam.20567>
- [23] A. Kesari, Do data breach notification laws reduce medical identity theft? evidence from consumer complaints data, *J. Empir. Leg. Stud.* 19 (4) (2022) 1222–1252. <https://doi.org/10.1111/jels.12331>
- [24] G. Aridor, Y.-K. Che, T. Salz, The economic consequences of data privacy regulation: Empirical evidence from GDPR, 2020. National Bureau of Economic Research working paper No. 26900. <https://doi.org/10.3386/w26900>
- [25] U. Franke, J. Turell, I. Johansson, The cost of incidents in essential services—data from Swedish NIS reporting, in: *16th International Conference on Critical Information Infrastructures Security (CRITIS 2021)*, Springer, 2021. [https://doi.org/10.1007/978-3-030-93200-8\\_7](https://doi.org/10.1007/978-3-030-93200-8_7)
- [26] S. Héroux, A. Fortin, Cybersecurity disclosure by the companies on the S&P/TSX 60 index, *Account. Perspect.* 19 (2) (2020) 73–100. <https://doi.org/10.1111/1911-3838.12220>
- [27] E. Eijkelenboom, B. Nieuwesteeg, An analysis of cybersecurity in Dutch annual reports of listed companies, *Comput. Law Secur. Rev.* 40 (2021) 105513. <https://doi.org/10.1016/j.clsr.2020.105513>
- [28] M. Firoozi, S. Mohsni, Cybersecurity disclosure in the banking industry: a comparative study, *Int. J. Disclosure Governance* 20 (4) (2023) 451–477. <https://doi.org/10.1057/s41310-023-00190-8>
- [29] L. Gao, T.G. Calderon, F. Tang, Public companies' cybersecurity risk disclosures, *Int. J. Account. Inf. Syst.* 38 (2020) 100468. <https://doi.org/10.1016/j.accinf.2020.100468>
- [30] F. Cremer, B. Sheehan, M. Fortmann, A.N. Kia, M. Mullins, F. Murphy, S. Materne, Cyber risk and cybersecurity: a systematic review of data availability, *Geneva Paper. Risk Insurance-Iss. Pract.* 47 (3) (2022) 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- [31] L.G. Schaffner, P. Tettamanzi, M. Murgolo, Cyber security and risk disclosure: a literature review for theory and practice, in: *WISP 2023 Proceedings*, 6., 2023. <https://aisel.aisnet.org/wisp2023/6>
- [32] SEC, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, 2023, (<https://www.sec.gov/news/press-release/2023-139>).
- [33] N. Agarwal, S. Agarwal, C. Chatterjee, Data breach notification laws and the cost of private debt, *Brit. Account. Rev.* (2024) 101518. <https://doi.org/10.1016/j.bar.2024.101518>
- [34] M. Adams, T. Moore, How informative are cybersecurity risk disclosures? empirical analysis of breached firms, *Comput. Secur.* (2025). In press.
- [35] SEC, SEC Adopts Rules to Enhance and Standardize Climate-Related Disclosures for Investors, 2024, (<https://www.sec.gov/newsroom/press-releases/2024-31>).
- [36] Basel Committee on Banking Supervision, Disclosure of climate-related financial risks, 2023, (<https://www.bis.org/bcb/publ/d560.htm>).
- [37] *Economist*, Corporate climate reporting: telling all, *The Economist* 438 (9236) (2021) 55–56. March 13.
- [38] L. Seltzer, L.T. Starks, Q. Zhu, Climate regulatory risks and corporate bonds, 2022. National Bureau of Economic Research working paper No. 29994. <https://doi.org/10.3386/w29994>
- [39] P. Krueger, Z. Sautner, L.T. Starks, The importance of climate risks for institutional investors, *Rev. Financ. Stud.* 33 (3) (2020) 1067–1111. <https://doi.org/10.1093/rfs/hhz137>
- [40] S. Ramelli, A.F. Wagner, R. Zeckhauser, A. Ziegler, et al., Stock price rewards to climate saints and sinners: Evidence from the Trump election, 2018. National Bureau of Economic Research working paper No. 25310. <https://doi.org/10.3386/w25310>
- [41] D. Choi, Z. Gao, W. Jiang, Global Carbon Divestment and Firms' Actions, 2020, Available at SSRN. <https://doi.org/10.2139/ssrn.3589952>
- [42] R. Bénabou, J. Tirole, Individual and corporate social responsibility, *Economica* 77 (305) (2010) 1–19. <https://doi.org/10.1111/j.1468-0335.2009.00843.x>
- [43] S. El Ghoul, O. Guedhami, H. Kim, K. Park, Corporate environmental responsibility and the cost of capital: international evidence, *J. Bus. Ethic.* 149 (2) (2018) 335–361. <https://doi.org/10.1007/s10551-015-3005-6>
- [44] A.G.F. Hoepner, I. Oikonomou, Z. Sautner, L.T. Starks, X.Y. Zhou, ESG Shareholder engagement and downside risk, *Rev. Financ. Stud.* 28 (2) (2024) 483–510. <https://doi.org/10.1093/rof/rfad034>
- [45] A. Amel-Zadeh, G. Serafeim, Why and how investors use ESG information: evidence from a global survey, *Financ. Anal. J.* 74 (3) (2018) 87–103. <https://doi.org/10.2469/faj.v74.n3.2>
- [46] J.R. Nofsinger, J. Sulaeman, A. Varma, Institutional investors and corporate social responsibility, *J. Corp. Finance* 58 (2019) 700–725. <https://doi.org/10.1016/j.jcorpfin.2019.07.012>
- [47] C. Flammer, Corporate social responsibility and shareholder reaction: the environmental awareness of investors, *Acad. Manag. J.* 56 (3) (2013) 758–781. <https://doi.org/10.5465/amj.2011.0744>
- [48] B. Cui, P. Docherty, Stock price overreaction to ESG controversies, 2020, Available at SSRN. <https://doi.org/10.2139/ssrn.3559915>
- [49] E. Ginglinger, Q. Moreau, Climate risk and capital structure, *Manag. Sci.* 69 (12) (2023) 7492–7516. <https://doi.org/10.1287/mnsc.2023.4952>
- [50] K. de Greiff, M.D. Delis, S. Ongena, Being Stranded on the Carbon Bubble? Climate Policy Risk and the Pricing of Bank Loans, 2018, CEPR Discussion Paper No. DP12928, available at SSRN, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3178099](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3178099).
- [51] F. Berg, J.F. Kölbl, R. Rigobon, Aggregate confusion: the divergence of ESG ratings, *Rev. Financ. Stud.* 26 (6) (2022) 1315–1344. <https://doi.org/10.1093/rof/rfac033>
- [52] S. Drempeic, C. Klein, B. Zwergel, The influence of firm size on the ESG score: corporate sustainability ratings under review, *J. Bus. Ethic.* (2019) 1–28. <https://doi.org/10.1007/s10551-019-04164-1>
- [53] G. Kling, U. Volz, V. Murinde, S. Ayas, The impact of climate vulnerability on firms' cost of capital and access to finance, *World Dev.* 137 (2021) 105131. <https://doi.org/10.1016/J.WORLDDEV.2020.105131>
- [54] N. Apergis, T. Poufina, A. Antonopoulos, ESG Scores and cost of debt, *Energy Econ.* 112 (2022) 106186. <https://doi.org/10.1016/J.ENERECO.2022.106186>
- [55] J.A. McCahery, Z. Sautner, L.T. Starks, Behind the scenes: the corporate governance preferences of institutional investors, *J. Finance* 71 (6) (2016) 2905–2932. <https://doi.org/10.1111/jofi.12393>
- [56] P. Bolton, M. Kacperczyk, Do investors care about carbon risk?, 2020, National Bureau of Economic Research working paper No. 26968. <https://doi.org/10.3386/w26968>
- [57] Y. Tian, H. Zhou, From bottom line to consumers' mind: the framing effects of accounting information, *Account. Org. Soc.* 43 (2015) 56–66. <https://doi.org/10.1016/j.aos.2015.04.003>
- [58] P. Alexander, C. Brown, A. Arneith, J. Finnigan, M.D.A. Rounsevell, Human appropriation of land for food: the role of diet, *Global Environ. Change* 41 (2016) 88–98. <https://doi.org/10.1016/j.gloenvcha.2016.09.005>
- [59] D.A. Coley, E. Goodliffe, J. Macdiarmid, The embodied energy of food: the role of diet, *Energy Policy* 26 (6) (1998) 455–459. [https://doi.org/10.1016/S0301-4215\(97\)00159-6](https://doi.org/10.1016/S0301-4215(97)00159-6)
- [60] M. Springmann, D. Mason-D'Croz, S. Robinson, K. Wiebe, H.C.J. Godfray, M. Rayner, P. Scarborough, Mitigation potential and global health impacts from emissions pricing of food commodities, *Nat. Clim. Chang* 7 (1) (2017) 69–74. <https://doi.org/10.1038/nclimate3155>
- [61] A. Roth, T. Käberger, Making transport systems sustainable, *J. Clean. Prod.* 10 (4) (2002) 361–371. [https://doi.org/10.1016/S0959-6526\(01\)00052-X](https://doi.org/10.1016/S0959-6526(01)00052-X)
- [62] L.A. Greening, Effects of human behavior on aggregate carbon intensity of personal transportation: comparison of 10 OECD countries for the period 1970–1993, *Energy Econ.* 26 (1) (2004) 1–30. <https://doi.org/10.1016/j.eneco.2003.05.001>
- [63] S. Bin, H. Dowlatabadi, Consumer lifestyle approach to US energy use and the related CO<sub>2</sub> emissions, *Energy Policy* 33 (2) (2005) 197–208. [https://doi.org/10.1016/S0301-4215\(03\)00210-6](https://doi.org/10.1016/S0301-4215(03)00210-6)
- [64] R. Duarte, K. Feng, K. Hubacek, J. Sánchez-Chóliz, C. Sarasa, L. Sun, Modeling the carbon consequences of pro-environmental consumer behavior, *Appl. Energy* 184 (2016) 1207–1216. <https://doi.org/10.1016/j.apenergy.2015.09.101>
- [65] A. Beylot, S. Vaxelaire, J. Villeneuve, Reducing gaseous emissions and resource consumption embodied in french final demand: how much can waste policies contribute?, *J. Ind. Ecol.* 20 (4) (2016) 905–916. <https://doi.org/10.1111/jiec.12318>
- [66] R. McKenna, L. Hofmann, E. Merkel, W. Fichtner, N. Strachan, Analysing socio-economic diversity and scaling effects on residential electricity load profiles in the context of low carbon technology uptake, *Energy Policy* 97 (2016) 13–26. <https://doi.org/10.1016/j.enpol.2016.06.042>
- [67] S. Grappi, S. Romani, R.P. Bagozzi, Consumer response to corporate irresponsible behavior: moral emotions and virtues, *J. Bus. Res.* 66 (10) (2013) 1814–1821. <https://doi.org/10.1016/j.jbusres.2013.02.002>

- [68] J. Lindenmeier, C. Schleer, D. Pricl, Consumer outrage: emotional reactions to unethical corporate behavior, *J. Bus. Res.* 65 (9) (2012) 1364–1373. <https://doi.org/10.1016/j.jbusres.2011.09.022>
- [69] J.G. Klein, N.C. Smith, A. John, Why we boycott: consumer motivations for boycott participation, *J. Mark.* 68 (3) (2004) 92–109. <https://doi.org/10.1509/jmkg.68.3.92.34770>
- [70] C. Kang, F. Germann, R. Grewal, Washing away your sins? corporate social responsibility, corporate social irresponsibility, and firm performance, *J. Mark.* 80 (2) (2016) 59–79. <https://doi.org/10.1509/jm.15.0324>
- [71] L.B. Glickman, The strike in the temple of consumption: consumer activism and twentieth-century American political culture, *J. Am. Hist.* 88 (1) (2001) 99–128. <https://doi.org/10.2307/2674920>
- [72] R.V. Kozinets, J.M. Handelman, Adversaries of consumption: consumer movements, activism, and ideology, *J. Consum. Res.* 31 (3) (2004) 691–704. <https://doi.org/10.1086/425104>
- [73] M.S.W. Lee, J. Motion, D. Conroy, Anti-consumption and brand avoidance, *J. Bus. Res.* 62 (2) (2009) 169–180. <https://doi.org/10.1016/j.jbusres.2008.01.024>
- [74] S.T. Fiske, Attention and weight in person perception: the impact of negative and extreme behavior, *J. Pers. Soc. Psychol.* 38 (6) (1980) 889. <https://doi.org/10.1037/0022-3514.38.6.889>
- [75] R.E. White, D.D. Kare, The impact of consumer boycotts on the stock prices of target firms, *J. Appl. Bus. Res. (JABR)* 6 (2) (1990) 63–71. <https://doi.org/10.19030/jabr.v6i2.6306>
- [76] D.W. Woods, A.C. Simpson, Cyber-warranties as a quality signal for information security products, in: *International Conference on Decision and Game Theory for Security*, Springer, 2018, pp. 22–37. [https://doi.org/10.1007/978-3-030-01554-1\\_2](https://doi.org/10.1007/978-3-030-01554-1_2)
- [77] A. Bharadwaj, M. Keil, M. Mähring, Effects of information technology failures on the market value of firms, *J. Strategic Inf. Syst.* 18 (2) (2009) 66–79. <https://doi.org/10.1016/j.jsis.2009.04.001>
- [78] S. Varga, J. Brynielsson, U. Franke, Cyber-threat perception and risk management in the Swedish financial sector, *Comput. Secur.* 105 (2021). <https://doi.org/10.1016/j.cose.2021.102239>
- [79] C.A. Makridis, Do data breaches damage reputation? evidence from 45 companies between 2002 and 2018, *J. Cybersecur.* 7 (1) (2021) tyab021. <https://doi.org/10.1093/cybsec/tyab022>
- [80] D.D. Malliouris, A. Simpson, The stock market impact of information security investments: the case of security standards, in: *Workshop on the Economics of Information Security (WEIS 2019)*, 2019. <https://ora.ox.ac.uk/objects/uuid:5de5f4cb-5fcb-46bb-9cd3-d13817d27e05>
- [81] T. Havakhor, M.S. Rahman, T. Zhang, Cybersecurity investments and the cost of capital, in: *Workshop on the Economics of Information Security (WEIS 2020)*, 2020. <https://weis2020.econinfocsec.org/wp-content/uploads/sites/8/2020/06/weis20-final16.pdf>
- [82] A. Bushby, How deception can change cyber security defences, *Comput. Fraud Secur.* 2019 (1) (2019) 12–14. [https://doi.org/10.1016/S1361-3723\(19\)30008-9](https://doi.org/10.1016/S1361-3723(19)30008-9)
- [83] A. Bates, W.U. Hassan, Can data provenance put an end to the data breach?, *IEEE Secur. Priv.* 17 (4) (2019) 88–93. <https://doi.org/10.1109/MSEC.2019.2913693>
- [84] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, R.M. Stulz, What is the impact of successful cyberattacks on target firms?, 2018, National Bureau of Economic Research working paper No. 24409. <https://doi.org/10.3386/w24409>
- [85] M. Pizzetti, L. Gatti, P. Seele, Firms talk, suppliers walk: analyzing the locus of greenwashing in the blame game and introducing ‘vicarious greenwashing’, *J. Bus. Ethic.* 170 (1) (2021) 21–38. <https://doi.org/10.1007/s10551-019-04406-2>
- [86] A. Inês, A. Diniz, A.C. Moreira, A review of greenwashing and supply chain management: challenges ahead, *Clean. Environ. Syst.* 11 (2023) 100136. <https://doi.org/10.1016/j.cesys.2023.100136>
- [87] J.L. Campbell, H. Chen, D.S. Dhaliwal, H.-m. Lu, L.B. Steele, The information content of mandatory risk factor disclosures in corporate filings, *Rev. Account. Stud.* 19 (1) (2014) 396–455. <https://doi.org/10.1007/s11142-013-9258-3>
- [88] K.K. Nelson, A.C. Pritchard, Carrot or stick? the shift from voluntary to mandatory disclosure of risk factors, *J. Empir. Leg. Stud.* 13 (2) (2016) 266–297. <https://doi.org/10.1111/jels.12115>
- [89] H. Li, W.G. No, T. Wang, SEC’s cybersecurity disclosure guidance and disclosed cybersecurity risk factors, *Int. J. Account. Inf. Syst.* 30 (2018) 40–55. <https://doi.org/10.1016/j.accinf.2018.06.003>
- [90] A.J. Mateo-Márquez, J.M. González-González, C. Zamora-Ramírez, An international empirical study of greenwashing and voluntary carbon disclosure, *J. Clean. Prod.* 363 (2022) 132567. <https://doi.org/10.1016/j.jclepro.2022.132567>
- [91] N.H. Luu, C. Le, H.N. Luu, D.T.K. Nguyen, Does mandatory greenhouse gas emissions reporting program deter corporate greenwashing?, *J. Environ. Manage.* 373 (2025) 123740. <https://doi.org/10.1016/j.jenvman.2024.123740>
- [92] OECD, Enhancing the Role of Insurance in Cyber Risk Management, OECD, 2017. <https://doi.org/10.1787/9789264282148-en>
- [93] D. Woods, A. Simpson, Policy measures and cyber insurance: a framework, *J. Cyber Policy* 2 (2) (2017) 209–226. <https://doi.org/10.1080/23738871.2017.13609>
- [94] U. Franke, The cyber insurance market in Sweden, *Comput. Secur.* 68 (2017) 130–144. <https://doi.org/10.1016/j.cose.2017.04.010>
- [95] A. Sheneman, Cybersecurity risk and the cost of debt, 2017, Available at SSRN. <https://doi.org/10.2139/ssrn.3406217>
- [96] A. Sheneman, Contagion or competitive effects?: Lenders’ response to peer firm cyberattacks, in: *Workshop on the Economics of Information Security (WEIS 2022)*, 2022. <https://weis2022.econinfocsec.org/wp-content/uploads/sites/10/2022/06/weis22-sheneman.pdf>
- [97] B. Edwards, S. Hofmeyr, S. Forrest, Hype and heavy tails: a closer look at data breaches, *J. Cybersecur.* 2 (1) (2016) 3–14. <https://doi.org/10.1093/cybsec/tyw003>
- [98] M.F. Carfora, A. Orlando, Quantile based risk measures in cyber security, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), IEEE, 2019, pp. 1–4. <https://doi.org/10.1109/CyberSA.2019.8899431>
- [99] M. Kianpour, U. Franke, The use of simulations in economic cybersecurity decision-making, *J. Cybersecur.* 11 (1) (2025) tyaf003. <https://doi.org/10.1093/cybsec/tyaf003>
- [100] L. Bilge, T. Dumitras, Before we knew it: an empirical study of zero-day attacks in the real world, in: *Proceedings of the 2012ACM Conference on Computer and Communications Security*, 2012, pp. 833–844. <https://doi.org/10.1145/2382196.2382284>
- [101] A. Arora, A. Nandkumar, R. Telang, Does information security attack frequency increase with vulnerability disclosure? an empirical analysis, *Inf. Syst. Front.* 8 (5) (2006) 350–362. <https://doi.org/10.1007/s10796-006-9012-5>
- [102] R. Anderson, Open and closed systems are equivalent (that is, in an ideal world), in: J. Feller, B. Fitzgerald, S.A. Hissam, K.R. Huff (Eds.), *Perspectives on Free and Open Source Software*, MIT Press, 2007, pp. 127–142. <https://ieeexplore.ieee.org/abstract/document/6277068>
- [103] D. Geer, E. Jardine, E. Leverett, On market concentration and cybersecurity risk, *J. Cyber Policy* 5 (1) (2020) 9–29. <https://doi.org/10.1080/23738871.2020.1728355>
- [104] U. Franke, A. Hoxell, Observable cyber risk on Cournot oligopoly data storage markets, *Risks* 8 (119) (2020). <https://doi.org/10.3390/risks8040119>
- [105] K. Chuah, M.R. DesJardine, M. Goranova, W.J. Henisz, Shareholder activism research: a system-level view, *Acad. Manag. Annals.* 18 (1) (2024) 82–120. <https://doi.org/10.5465/annals.2022.0069>
- [106] B. Nieuwesteeg, M. Faure, An analysis of the effectiveness of the EU data breach notification obligation, *Comput. Law Secur. Rev.* 34 (6) (2018) 1232–1246. <https://doi.org/10.1016/j.clsr.2018.05.026>
- [107] D. Charoen, W. Khern-am-nuai, Revisiting the (disappearing) cost of data breach disclosures, *Digit. Policy Regul. Governance* 27 (1) (2025) 37–55. <https://doi.org/10.1108/DPRG-02-2024-0033>
- [108] E. Markos, P. Peña, L.I. Labrecque, K. Swani, Are data breaches the new norm? exploring data breach trends, consumer sentiment, and responses to security invasions, *J. Consum. Affair.* 57 (3) (2023) 1089–1119. <https://doi.org/10.1111/joca.12554>
- [109] J. Burwen, D.I. Levine, A rapid assessment randomized-controlled trial of improved cookstoves in rural Ghana, *Energy Sustain. Dev.* 16 (3) (2012) 328–338. <https://doi.org/10.1016/j.esd.2012.04.001>
- [110] M. Cornelius, K.C. Armel, K. Hoffman, L. Allen, S.W. Bryson, M. Desai, T.N. Robinson, Increasing energy- and greenhouse gas-saving behaviors among adolescents: a school-based cluster-randomized controlled trial, *Energy Effic.* 7 (2) (2014) 217–242. <https://doi.org/10.1007/s12053-013-9219-5>
- [111] S. Wynes, K.A. Nicholas, J. Zhao, S.D. Donner, Measuring what works: quantifying greenhouse gas emission reductions of behavioural interventions to reduce driving, meat consumption, and household energy use, *Environ. Res. Lett.* 13 (11) (2018) 113002. <https://doi.org/10.1088/1748-9326/aae5d7>