Harnessing Market Incentives to Improve Cybersecurity Outcomes for Firms and Consumers

Policy Briefing | November 2023

Dr Wing Man Wynne Lam (University of Edinburgh)
Dr Jacob Seifert (University of Leicester)

*'In order to establish long-lasting change in how businesses manage their cyber risk and improve their resilience levels, there remains a need to stimulate **market incentives**. Market drivers that could normalise investment in cyber security across the economy and lead companies to feel compelled to take up effective cyber risk management, such as strong consumer pressure and competitive advantage, **have not yet formed in many sectors or across the economy**. While harder forms of **government intervention**, including legislation, can be a useful tool to drive behavioural change from above, stimulating market incentives in parallel will ensure businesses themselves prioritise cyber resilience, and that practice continues to adapt to evolving threats.'*

HM Government, 2022 Cyber Security Incentives and Regulation Review (emphasis added)

About the research

The global costs of cyber-attacks are predicted to exceed $10 trillion annually by 2025.[1] These costs underline the challenge that governments and regulators face in promoting the innovative potential of digital markets while also ensuring that consumers and firms are not exposed to excessive cyber-risks. Mitigating these risks through robust IT systems and practices requires firms to make ongoing investments in cybersecurity and to adopt new technologies that are capable of addressing evolving cyber-threats.[2]

Our research supports the view that firms typically underinvest in security and under-adopt secure technologies. Addressing these **market failures** is complicated by the interlinked nature of firms' decision making in digital markets, however. In these markets, firms' decisions with respect to protecting consumer data cannot be separated from their **data sharing** choices and their broader **competitive efforts** to capture market share.

Our work shows that regulatory interventions must take this broader market context into account. **Narrowly conceived cyber-regulations can backfire** and harm consumers if the effects of changes in cyber-investment on firms' data sharing choices and wider competitive behaviour are not taken into consideration.

Policy recommendations

1. **Underinvestment** in cybersecurity and **under-adoption** of secure hardware are prevalent. Effective regulatory interventions to correct these market failures must take the **wider market context** into account.

2. Policies that **incentivise secure hardware adoption** should be tailored to reflect the **competitiveness** of the final product market in which firms are competing.

3. **Minimum cybersecurity standards** should be accompanied by increased safeguards on firms' **data sharing** practices, since higher mandated security levels can lead to reduced data privacy.

4. **Raising consumer awareness** can be effective in increasing firms' cybersecurity investments but might also impact **data sharing** decisions and undermine consumer privacy.

5. The **data governance framework** in the form of **data ethics** and **responsible innovation** rules, as well as technical requirements on **data anonymisation**, **encryption** and **interoperability** can improve market failures. Interventions must, however, be **context-specific**.

Main insights

Economic analysis based on game theoretic modelling is an important complement to the computer science perspective on cybersecurity. It provides a set of tools that allow us to study the **market-generated incentives** underlying firms' decisions to protect the sensitive consumer data they control. These decisions include both the ongoing level of investment that a firm should commit to cybersecurity measures, as well as its one-off decision to adopt or not adopt a new and more secure piece of hardware.

Understanding these incentives requires the **market context** in which a firm's business decisions are made to be accurately captured: protecting consumer data is only one dimension of a firm's business strategy that, overall, aims to **maximise shareholder returns**.

In digital markets, the cybersecurity problem is linked to **data privacy** in the sense that a firm will typically have to decide on the scope of its data sharing agreements at the same time as it decides on its approach to safeguarding consumer data. Moreover, a firm will consider the implications of any decisions it makes with respect to either cybersecurity or data privacy (data sharing) on its **competitive position** vis-à-vis its rival firms (Figure 1).

What is a market failure?

What does it mean, in this context, to say that a market failure with respect to a firm's cybersecurity practices (or any other business decision) has occurred? If we say that a firm underinvests in cybersecurity, what is the benchmark relative to which it underinvests? **Is more investment always better?**

In order to determine whether or not a market failure has occurred, we consider the following hypothetical scenario. We ask what the firm's decisions would have been, were its objective not to maximise its own profits but instead to maximise **social welfare**, defined as the sum of the total benefits enjoyed by firms and consumers in this market.

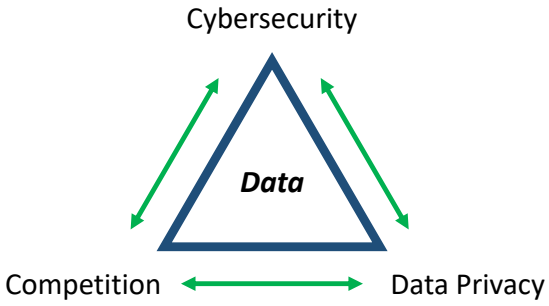


Figure 1. The market context

A market failure occurs whenever a firm's (or a group of firms') profit-maximising decisions fall short of or exceed those that maximise the wellbeing of society as a whole. An important benefit of applying economic research methods to the cybersecurity field is that **they allow us to analyse this benchmark of the social optimum formally**. This is the basis for identifying market failures and for studying suitable policy interventions to remedy them.

Market failures and interventions

Our research shows that **market failures with respect to cybersecurity are prevalent**: firms' ongoing investments in cybersecurity tend to fall short of socially optimal levels, and firms may not adopt secure hardware to a sufficient extent. The main question for policy is therefore: how can firms' privately optimal decisions in these areas be brought into line with those that maximise the wellbeing of society as a whole?

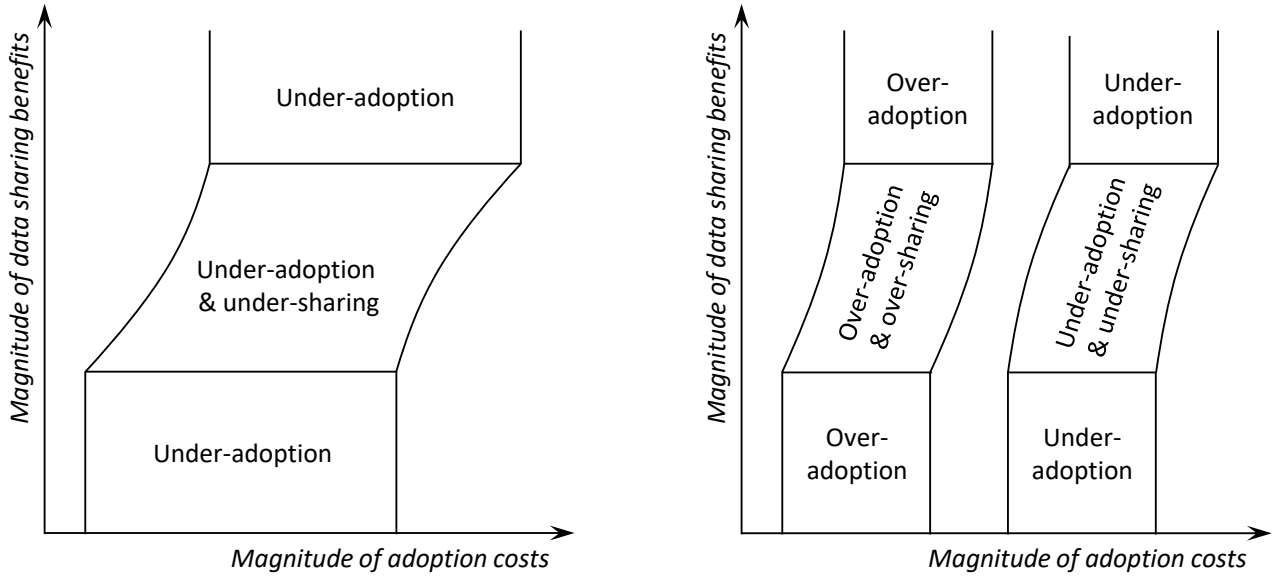
We show that improving social welfare by addressing these cybersecurity market failures must take the business context described above into account. **Even if firms' cybersecurity efforts are insufficient, policies that focus too narrowly on cybersecurity can make society worse off**.

For example, when firms underinvest in cybersecurity, mandating a higher **minimum standard of security** can be an appealing policy choice. This underlies the objective of the UK Government to "look at ways in which we can increase the number of companies achieving Cyber Essentials certification", for example.[3] This is where the market context, and particularly the interactions between cybersecurity and data privacy, must be considered. Our work shows that **privacy and security tend to be negatively related**, in the sense that firms tend to share data more widely as the extent of their security protections increases. The reason is that, the more effective a firm's security measures become, the better protected it is against incremental cyber-threats that accompany the more widespread sharing of consumer

data. Therefore mandating higher security standards can have the unintended side effect of incentivising data sharing. **Higher security standards can even lead to lower social welfare as a result of socially excessive data sharing that is induced by the standard itself**. In that sense, it is crucial that minimum security standards are accompanied by safeguards on firms' data sharing practices (*Recommendation 3*).

Similarly, **promoting consumer awareness** can make firms more accountable in terms of their use of consumer data. We show that, when firms cannot be held fully liable for the cyber-damages that consumers suffer as the result of a cyber-attack,[4] increasing consumer awareness of the residual cyber-risks they face leads to an increase in a firm's security investment levels. Nonetheless, this increase in investment does not necessarily translate into an increase in social welfare, since more knowledgeable consumers are also deterred from engaging with the firm at all. This market shrinking effect implies that consumer education policies actually lower social welfare unless they cause the firm to reduce the extent of its data sharing as a means of retaining customers. In that sense, **an increase in security cannot always be equated with an increase in social welfare**. This is an example of a policy targeting cybersecurity, namely consumer education, that succeeds in improving social welfare only as a result of the indirect effects that it exerts on data sharing (*Recommendation 4*).

Finally, our work shows that cybersecurity market failures depend on the **intensity of competition** in the final product market. When competition is less intense, such that consumers are relatively unresponsive to small price differences between firms, a firm's incentive to adopt secure hardware as part of a strategy of market expansion is also limited. By contrast, when demand is highly responsive to small differentials in price, firms can compete over the adoption of secure hardware to such an extent as to generate over-adoption in some cases (Figure 2). This over- or under-adoption of secure hardware can translate into over- or under-sharing of consumer data, respectively, again as a result of the negative relationship between data privacy and security described above.



(a) Low intensity of competition (b) High intensity of competition

Figure 2. Market failures and the intensity of competition in the final product market

Figure 2 (b) highlights that under-adoption of secure hardware is not the only market failure that can occur. In highly competitive markets, the competitive advantage that more secure hardware confers, namely the mitigation of cyber-risks that accompany an expansionary market strategy, can lead to the over-adoption of such technologies in the sense that there is excessive duplication. **Therefore the nature of market failures in the secure hardware adoption context depends on the intensity of competition in the final product market** (*Recommendation 2*). It also follows that promoting the intensity of competition within an existing market structure can be a means of addressing market failures related to the under-adoption of secure hardware. On the other hand, we also show that changes to the market structure itself in favour of increased competition can reduce secure hardware adoption incentives.

Given the links between data sharing and cybersecurity described above, efforts to mitigate the under-adoption (or over-adoption) problem need not be limited to policies that impact the intensity of competition or alter the costs of adoption in a direct way. Policies that affect adoption costs directly include **fines for non-adoption**, **subsidies** as well as broader reputational costs of non-adoption that relate to **data ethics** and **responsible innovation rules**.

Instead, policies that target the magnitude of the benefits that firms derive from sharing data also affect their hardware adoption incentives, and therefore the nature of the market failures identified above. Policies in this category include **technical requirements on data anonymisation, encryption and interoperability**, for example, as well as **taxes on the profits derived from data sharing**.

Overall, it is important to recognise that there are cases in which increases in security, reflected here in the extent to which firms adopt secure hardware, do not lead to improvements in social welfare. Regulatory interventions must therefore be carefully targeted to reflect the relevant market context, including the competitiveness of the final product market in which firms are competing (*Recommendation 5*).

Notes

[1] World Economic Forum, 2023, see https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/.

[2] A particular example of a new technology with the potential to substantially reshape the security landscape is the capability architecture that underlies the UK Digital Security by Design challenge, see https://www.dsbd.tech/.

[3] See 2022 Cyber Security Incentives and Regulation Review. https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review

[4] A related policy intervention involves increasing firms' liability in the event of a cyber-attack. In keeping with the discussion in this section, we show that increasing firms' liability increases security investments, but decreases social welfare unless the firm is deterred from sharing data.

Further information

Lam, W.M.W. and Seifert, J. (2021). Regulatory Interactions and the Design of Optimal Cybersecurity Policies. *ESRC Digital Security by Design Social Science (Discribe) Hub+ Commissioned Report*. https://static1.squarespace.com/static/5f8ebbc01b92bb238509b354/t/618cf3a82f816f66d11dd4cc/1636627370520/Lam+Seifert+Final+Project+Report.pdf

Lam, W.M.W. and Seifert, J. (2023). Regulating Data Privacy and Cybersecurity. *Journal of Industrial Economics*, 71 (1), 143-175. https://doi.org/10.1111/joie.12316

Lam, W.M.W. and Seifert, J. (2023). Secure Hardware Adoption in the Open Data Context. *ESRC Discribe Hub+ Commissioned Report*. https://www.discribehub.org/s/Final-Report-Lam-Seifert.pdf

Lam, W.M.W. and Seifert, J. (2023). Competition, Data Sharing and Secure Hardware Adoption. *Working Paper*, available on request from the authors (see contact details below).

Contact the researchers

Dr Jacob Seifert, University of Leicester. jacob.seifert@leicester.ac.uk

Dr Wing Man Wynne Lam, University of Edinburgh. wynne.lam@ed.ac.uk

discribe