Regulatory Interactions and the Design of Optimal Cybersecurity Policies

Final Project Report

Prepared for the Digital Security by
Design Social Science (Discribe) Hub+

July 31, 2021

Wing Man Wynne Lam
University of East Anglia
(wing.m.lam@uea.ac.uk)

Jacob Seifert
University of Leicester
(jacob.seifert@leicester.ac.uk)

Acknowledgements

We thank the Digital Security by Design Social Science (Discribe) Hub+, and particularly Adam Joinson, Joanna Syrda and Nicola Johnson, for their extensive support throughout this project. We are also indebted to all of our interview and workshop participants for their time and valuable insights.

Contents

Executive Summary

This report investigates the design of optimal cybersecurity policies. Our analysis focuses on incentives and explores how regulations can bring the private decisions of profit-maximising firms into line with the objectives of society as a whole. In so doing, we pay explicit attention to important regulatory interactions between cybersecurity, data privacy and competition. This is a crucial part of evaluating the welfare-desirability of any cybersecurity policy: in order to maximise social welfare, regulation must not only correct market failures in the area of cybersecurity but, at the same time, avoid exacerbating market failures in the related areas of data privacy and competition. These areas are intuitively closely connected since the sensitive consumer data that a firm's cybersecurity strategy aims to protect are simultaneously the subject of data sharing agreements between firms (the data privacy issue) and the source of market power for dominant firms in several important sectors (the competition issue).

We approach this question from several methodological directions. Firstly, we discuss the extent to which the UK's existing regulatory framework accounts for relevant interactions. Secondly, we conduct a qualitative analysis of this regulatory landscape, drawing on primary data collected from interviews and workshops. Thirdly, we begin our evaluation of the policy recommendations that emerge from these interviews and workshops by reviewing the existing literature in the area of cybersecurity regulation. Finally, we extend the literature by presenting the results of two original theoretical contributions that, for the first time, incorporate regulatory interactions into the analysis of cybersecurity regulations.

These theoretical results allow us to evaluate in more detail the various policy recommendations that are highlighted by our qualitative analysis. In particular, they suggest that a more prescriptive approach to cybersecurity and data privacy regulation may be needed, and that cybersecurity concerns need to be closely integrated into any competition remedies that are based on compulsory data sharing by dominant firms. The report closes with an overview of some important directions for future research in this area.

List of Abbreviations

AI	Artificial Intelligence
CA 2013	Communications Act 2013
CDEI	Centre for Data Ethics and Innovation
DCMS	Department for Digital, Culture, Media and Sport
DMA	Data & Marketing Association
DPA 2018	Data Protection Act 2018
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IT	Information Technology
NCSC	National Cyber Security Centre
NIS [Regulations]	Network and Information Systems [Regulations]
OECD	Organisation for Economic Co-operation and Development
OES	Operator of Essential Services
PCI DSS	Payment Card Industry Data Security Standard
PECR	Privacy and Electronic Communications Regulations
RDSP	Relevant Digital Service Provider
SYSC	Senior Management Arrangements, Systems and Controls

Part 1

Introduction

The importance of protecting society from online threats is highlighted by the rising cost of cyber-attacks.[1] Cyber-crimes such as espionage, ransomware attacks and financial crime entail not only direct monetary harm but also non-monetary damages in the form of system downtime, reduced efficiency and brand damage. Protecting firms and consumers from these costs relies on the availability of effective technological defences, but also on the incentives of firms to develop and implement these new technologies, and of consumers to adopt secure behaviours with respect to their personal data.

This project takes an economic approach to studying cybersecurity that focuses on incentives. In this context, the motivation for regulation arises whenever the private incentives that the market provides for firms and consumers fail to achieve the goals that society as a whole sets for itself. Market failures of this type are common whenever choices are made by private agents such as profit-maximising firms who do not base their decisions on a consideration of social welfare, which considers not only firm profits but also the well-being of consumers.

Optimal cybersecurity policies align firms' cybersecurity decisions with those that society as a whole prefers. If firms' cybersecurity choices are separate from the remaining aspects of their business strategy, this problem can be viewed in isolation. Typically, however, firms' decisions are interrelated, so that altering a firm's incentives in one dimension, albeit with a view to correcting a market failure, can have unintended welfare consequences if it exacerbates market failures in another dimension.

Interactions of this type are likely to play a significant role in the context of cybersecurity. This is the case because the sensitive data that cybersecurity seeks to protect are, at the same time, the subject of data sharing agreements between firms (the data privacy issue) and also

[1] See Federal Bureau of Investigation (2020); McAfee (2020). The methodology underlying the calculation of cyber-damages is not the focus of this report, but is discussed in DCMS (2020a).

underlie the dominant market position enjoyed by many banks, search engines, online retailers and social media platforms, among others (the competition issue). Our focus on regulatory interactions reflects our objective to incorporate these important relationships between firms' incentives in the cybersecurity, data privacy and competition domains in our investigation of optimal cybersecurity policies.

For the sake of a clear separation between cybersecurity and data privacy, in what follows, we consider cybersecurity to relate to measures seeking to prevent the unintentional dissemination of data through the economy that occurs as a result of a cyber-attack, while data privacy relates to the intentional dissemination of data that occurs when data controlling firms agree to share data with third parties.[2]

In this report, we approach the analysis of regulatory interactions and optimal cybersecurity policies from several methodological directions. Firstly, we review the existing regulatory framework in the UK and discuss the extent to which relevant interactions are already taken into account. We find that this is true to a limited extent, but that important open questions remain in terms of whether cybersecurity and data privacy objectives are co-ordinated sufficiently, and whether cybersecurity and competition objectives merit closer integration, for example in the context of Open Baking.

Secondly, we evaluate the UK framework of digital security regulation by drawing on primary data collected through interviews and workshops. The input collected through these interactions provides an overview of the strengths, weaknesses, opportunities and threats that market participants representing a broad range of professional backgrounds identified in relation to the current system of regulations. Our interviews and workshops also enable us to present a range of specific policy recommendations concerning the future of UK digital security. The types of questions that these policy recommendations address include, for instance, whether a centralised or decentralised approach is likely to be most effective.

Given the large number of policies that were suggested by our interview and workshop participants, it is important to have an objective basis for evaluating the desirability of alternative reform proposals. Economic modelling offers the opportunity to study the welfare consequences of alternative policy reforms in isolation of conflating factors. To that end, our third methodology consists of a review of the academic literature and technical reports in the area of cybersecurity regulation. A number of important contributions in the fields of economics and management demonstrate the value that a theoretical understanding of regulations can have. These relate, for example, to the optimal balance between investments to

[2]This is in keeping with the UK Data Sharing Code of Practice, for example, which defines *privacy information* as the "information that organisations need to provide to individual data subjects about the collection and use [i.e. transfer] of their data".

prevent and mitigate the damage of cyber-attacks.

This review of the existing literature also highlights that the cybersecurity problem has, so far, been studied in isolation of the data privacy and competition issues. To address this gap in the literature, we present the results of two original contributions that, to the best of our knowledge, are the first to account explicitly for regulatory interactions. This game-theoretic modelling work represents the fourth of our methodological approaches. Relating the conclusions of this work back to the input we collected through interviews and workshops, we are able to demonstrate the precise sense in which regulatory co-ordination is needed: regulations such as minimum security standards that unilaterally target cybersecurity can have unintended welfare consequences if firms' decisions in the areas of data privacy are left to be determined by market forces. Moreover, introducing competition can introduce new market failures in the area of cybersecurity.

On the basis of this theoretical work, we draw several policy conclusions with relevance to the UK framework of digital security regulation. In particular, we suggest that a more prescriptive approach to regulation may be needed, and that any pro-competitive measures based on compulsory data sharing, such as Open Banking, should have cybersecurity as a joint objective. Nonetheless, not all the open questions that are raised by our review of existing regulations, our primary data analysis and our review of the existing literature are answered by this work. We therefore also present an overview of some important open questions for research.

The report is structured as follows. Part 2 reviews the existing framework of digital security regulation in the UK. Part 3 presents our qualitative analysis of these regulations, drawing on primary data collected through interviews and workshops. Part 4 reviews the existing academic literature and technical reports, before Part 5 discusses our original game-theoretic modelling work. Part 6 discusses future research directions. Conclusions are presented in Part 7.

Part 2

The UK Regulatory Landscape

There is no single law governing firms' cybersecurity choices.[1] Instead they fall under a variety of legislative instruments that either target cybersecurity in a more limited sense, or that have other objectives such as national security or sectoral regulation as their primary goal.

The approach of these regulations is broadly principles-based rather than prescriptive. This is designed to give the law the flexibility to keep up with the evolving nature of technology and cyber-threats. These regulations also do not intend to make firms immune to cyber-attack, the associated costs generally being seen as unsupportable. Instead, the appropriate level of cybersecurity is governed by a balancing exercise between the costs of implementing a given level of cybersecurity and its benefits in terms of preventing cyber-attacks.

We first discuss the central elements of the UK regulatory framework for digital security: the UK GDPR, the Data Protection Act 2018 and the Network and Information Systems Regulations 2018. We then discuss a number of other relevant pieces of legislation.

2.1 Data Protection Act (2018) and the UK GDPR

The General Data Protection Regulation ((EU) 2016/679) (GDPR) governs the manner in which personal data is collected, shared or otherwise processed. It does so by defining a series of rights held by data subjects and by imposing obligations on controllers and processors.[2]

Although the GDPR has applied directly in EU member states since May 2018, its principles were also incorporated into UK law via the Data Protection Act 2018 (DPA 2018). As such, the DPA 2018 ensures that EU and UK data protection laws will remain aligned post-Brexit, at least

[1] This part draws on practice notes maintained by Practical Law and Lexis PSL.

[2] A *controller* decides on the manner in which data is processed. A *processor* is a separate legal entity from a controller that acts entirely under instruction from the controller with respect to data processing activities.

until such a time as EU or UK laws are amended. The DPA 2018 also goes beyond the GDPR in some areas, for example concerning the processing of personal data by law enforcement and intelligence organisations, and it sets out specific UK exemptions. Following Brexit, the GDPR has become part of the body of retained EU law and is referred to as the UK GDPR. The GDPR itself is therefore now referred to as the EU GDPR in the UK. The UK GDPR and DPA 2018 represent the principal pieces of data protection legislation in the UK.

The obligations of controllers are summarised in six data protection principles contained in the UK GDPR. Controllers are responsible for ensuring compliance with each of them (the accountability principle). Of these data protection principles, the sixth relates directly to cybersecurity. It states that data should be

> "processed in a manner that ensures *appropriate security of the personal data*, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
>
> Article 5(1)(f), UK GDPR, emphasis added

The balancing of risks against rewards in determining the appropriate level of cybersecurity is made explicit in Article 32:

> "Taking into account the state of the art, *the costs of implementation* and the nature, scope, context and purposes of processing as well as *the risk of varying likelihood and severity* for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure *a level of security appropriate to the risk*."
>
> Article 32(1), UK GDPR, emphasis added

As this Article also states, the measures businesses are required to take in order to comply with the security principle include those of a technical nature (e.g. firewalls and threat-detection software) and an organisational nature (e.g. training, policies and procedures).

Other provisions of the UK GDPR can be seen as imposing additional cybersecurity requirements on firms. In particular:

1. data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (Article 5(1)(e), UK GDPR),[3] and

[3] Another security-related context that builds on this principle is the Payment Card Industry Data Security Standard (PCI DSS), applicable to merchants and payment processors, which prohibits storing payment card verification codes once a transaction has been authorised (Rule 3.2.2, PCI DSS v3).

2. the processing of personal data undertaken by controllers should build on the data protection by design and default principle (Article 25, UK GDPR).

These security principles are enforced by the Information Commissioner's Office (ICO). Any incident leading to a breach of personal data must be notified to the ICO within 72 hours of the controller becoming aware of it, where feasible (Article 32(1), UK GDPR). Similarly, processors must inform their controller without undue delay following a cyber-breach (Article 33(2), UK GDPR).

Enforcement powers held by the ICO include information notices (requests for information), assessment notices (inspections to determine compliance with legislation), enforcement notices (requiring a controller or processor to take a particular action) and penalty notices. In the case of the latter, failure to ensure appropriate security measures can result in fines of up to the greater of £17.5 million or 4% of annual global turnover (Article 83(5), UK GDPR). The ICO may take enforcement action, even without a data breach having occurred. In practice, reputational costs and private actions for damages are likely to represent further incentives to ensure appropriate levels of cybersecurity.

2.2 Network and Information Systems Regulations 2018

The Network and Information Systems Regulations 2018 (SI 2018/506) (NIS Regulations) are the UK enactment of the Network and Information Security Directive ((EU) 2016/1148) (Cybersecurity Directive). These regulations impose a number of cybersecurity-related obligations on two classes of firms:

1. Operators of essential services (OESs): firms that operate in important sectors such as energy, transport, health and digital, and which rely on network and information systems to perform their economic role.

2. Relevant digital service providers (RDSPs): firms that provide certain types of digital services in the UK, including online marketplaces, search engines and cloud computing services.

In contrast to the Cybersecurity Directive, banking and financial market infrastructures are not covered by the NIS Regulations. These areas are instead monitored by the Financial Conduct Authority (FCA) (see Cybersecurity in the Financial Services Sector below).

In each case, threshold requirements in terms of firm size must be met in order for an OES or RDSP to fall within the scope of the NIS Regulations. For OESs, and depending on the sector

in which they operate, these requirements are set out in Schedule 2 to the NIS Regulations. For RDSPs, small and micro businesses are generally exempted. OESs and RDSPs are required to self-identify to their designated competent authority. The designated competent authority varies for OESs according to the sector of their operations as reflected in Schedule 1 to the NIS Regulations. All RDSPs are subject to the oversight of the ICO.

Unlike the GDPR and DPA 2018, the focus of the NIS Regulations is not the security of the data being processed, but rather the security of the information technology (IT) infrastructure on which the essential services provided by OESs and RDSPs rely. OESs and RDSPs satisfying the threshold requirements fall under the NIS Regulations precisely because outages of the networks and systems they control could lead to substantial damage to consumers and the wider economy.

The main security obligations of OESs under the NIS Regulations are to:

> (1) "take *appropriate and proportionate technical and organisational measures to manage risks* posed to the security of the network and information systems on which their essential service relies.
>
> (2) take *appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems* used for the provision of an essential service, with a view to ensuring the continuity of those services."
>
> Regulation 10, NIS Regulations, emphasis added

The measures adopted under (1) must "ensure a level of security of network and information systems appropriate to the risk posed" (Regulation 10(3)). An important difference to the UK GDPR lies in the fact that OESs (and RDSPs) may not take the cost of implementing cybersecurity measures into account when deciding on their appropriateness. Rather appropriateness in the context of the NIS Regulations is based on the "state of the art", that is the measures currently available to them.

With regard to RDSPs, the security requirements are somewhat lighter than for OESs. Services provided by RDSPs are typically less critical to the continued normal operation of the wider economy. An "RDSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide" (Regulation 12(1)). These measures must "(having regard to the state of the art) ensure a level of security of network and information systems appropriate to the risk posed" (Regulation 12(2)).

The reporting obligations under the NIS Regulations are similar to those under the UK GDPR. An OES or RDSP must notify its designated competent authority without delay and no later than 72 hours after becoming aware of a security breach that has a significant impact on the continuity of the service which the OES or RDSP provides (Regulations 11, 12). It is important to note, in contrast to the UK GDPR, the absence of the phrase "where feasible" in this notification provision.

Enforcement of the NIS Regulations with respect to OESs falls to distinct and sector-specific designated competent authorities, such as Ofcom in the case of digital infrastructure. The ICO is the competent authority for all RDSPs. Fines under the NIS Regulations are not linked to global annual turnover, but instead follow tiered, static, upper limits depending on the infringement up to a maximum of £17 million. The possibility of double jeopardy, whereby an organisation is fined under both the UK GDPR and the NIS Regulations for the same event, is not ruled out. Other enforcement powers of designated competent authorities include information notices, inspections and enforcement notices.

NIS Regulations & Supply Chains

The NIS Regulations push cybersecurity through the supply chain. In particular, the OES or RDSP is held responsible for security, even if the delivery of its services is delegated to third parties. This implies contractual arrangements will typically be in place between OESs, RDSPs and third parties, covering, for example, auditing rights and a duty to report security incidents promptly. The National Cyber Security Centre (NCSC) has published supply chain security guidance comprising 12 principles to help firms manage the security of their supply chains.[4] Since the UK GDPR and DPA 2018 already require controllers to put in place minimum contractual obligations on processors,[5] these aspects of the UK GDPR, DPA 2018 and NIS Regulations relating to supply chains should be seen as mutually reinforcing.

2.3 Other Legislation

Communications Act 2003

Section 105 of the Communications Act 2013 (CA 2013) concerns the security of public electronic communications networks and services. These terms describe, respectively, "an elec-

[4]This guidance is accessible at *https://www.ncsc.gov.uk/collection/supply-chain-security*.

[5]See further *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/*.

tronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public" and "any electronic communications service that is provided so as to be available for use by members of the public" (Section 151). Providers of public electronic communications networks and services "must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services" (Section 105A). They must also inform Ofcom of any security breaches having a significant impact on the operation and availability of those networks and services (Section 105A).

Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)[6] implement the European e-Privacy Directive (2002/58/EC) into UK law. The PECR imposes obligations on providers of public electronic communications services that mirror those under Article 4 of the e-Privacy Directive. In particular, providers must "take appropriate technical and organisational measures to safeguard the security of that service" (Regulation 5(1)). The appropriateness criterion is satisfied in this context "if, having regard to (a) the state of technological developments, and (b) the cost of implementing it, [a measure] is proportionate to the risks against which it would safeguard" (Regulation 5(4)).

Enforcement of the PECR lies in the hands of the ICO. Security breaches must be notified "without undue delay" (Regulation 5A(1)), although this notification requirement disappears if data has been adequately encrypted (Regulation 5A(6)(a)). Enforcement powers of the ICO include audits and enforcement notices, as well as fines of up to £500,000.

Computer Misuse Act 1990

The Computer Misuse Act 1990 differs from the above legislation in that it defines a number of cyber-crimes that hackers may commit, rather than imposing security obligations on data processing firms or operators of critical networks and services. Crimes covered by the Computer Misuse Act 1990 include unauthorised access or interference with a computer, distributed denial of service attacks and the creation of hacking tools. The Computer Misuse Act 1990 has subsequently been amended by the Serious Crime Act 2015, which created the new offence of impairing a computer such as to cause serious damage.

[6] As amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208).

Cybersecurity in the Financial Services Sector

Providers of financial services including banks, insurance companies and financial advisers are subject to sector-specific cybersecurity regulations that are enforced by the FCA. These cyber-regulations stem from two sources: the Principles for Business and the Senior Management Arrangements, Systems and Controls (SYSC), both of which are contained in the FCA Handbook.

The SYSC are responsibility standards for company directors and senior management in financial firms. They contain rules that were previously part of the Capital Markets Directive (2006/49/EC) and the Markets in Financial Instruments Directive (2004/39/EC). Some of these rules directly or indirectly impose cybersecurity requirements on financial firms, in particular insofar as they relate to securing systems, managing risks, reducing the risk of financial crime and ensuring customer confidentiality. For instance, SYSC 3.2.21 states that "a firm should have appropriate systems and controls in place to fulfil the firm's regulatory and statutory obligations with respect to adequacy, access, periods of retention and security of records." These requirements also relate explicitly to the security of data that is transmitted: "a common platform firm[7] must have sound security mechanisms in place [...] to guarantee the security and authentication of the means of transfer of information" (SYSC 4.1.1). Other relevant SYSC rules include SYSC 6.1 (Compliance), SYSC 7 (Risk control) and SYSC 8 (Outsourcing).

Similarly, the third Principle for Business (PRIN 2.1.1, FCA Handbook) requires a firm to "take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems." Under Principle 11, regulated firms have a duty to report cyber-attacks to the FCA. A similar requirement also exists under Rule 7 of the Prudential Regulation Authority Rulebook.

European Regulation with Extraterritorial Effect in the UK

Post-Brexit, the EU GDPR will continue to affect UK businesses that are controllers or processors and that have an establishment in the EU, that offer goods or services to EU data subjects, or that monitor the behaviour of EU data subjects (Article 3, EU GDPR). UK firms may also be subject to member state enforcement of the Cybersecurity Directive (EU) 2016/1148. This may involve UK digital service providers having to comply with additional registration, security and notification requirements in those EU markets in which they operate.

[7] This term describes firms, such as banks, building societies and designated investment firms, which were simultaneously subject to the Capital Markets Directive and the Markets in Financial Instruments Directive.

2.4 *Open Questions*

The preceding review allows us to draw preliminary conclusions about the extent to which UK regulations incorporate relevant interactions between cybersecurity, data privacy and competition. First and foremost, the security principle contained in the UK GDPR and the DPA 2018 applies to all data processing activities, including data transfers. It requires processors to put in place security measures that are appropriate, given the risks associated with the processing activity. This should make the level of cybersecurity that firms implement responsive to the cyber-risks associated with data sharing. The Information Commissioner's Office Data Sharing Code of Practice makes this dependence explicit by providing specific guidance on how to manage and mitigate risks when sharing data. From an international perspective, Chapter V of the UK GDPR restricts the lawful bases for data to be transferred outside the UK. These data transfers are restricted precisely because of concerns over the level of cyber-protection in third countries (Article 45(2)(a), UK GDPR).

Other aspects of the UK regulatory framework discussed above link data privacy and cybersecurity by addressing the security of the networks via which data is transmitted. The NIS Regulations impose security obligations on OESs in the digital infrastructure and other sectors, and on RDSPs such as online marketplaces and cloud computing services. The PECR imposes similar duties on providers of public electronic communication services, who must ensure the security of data that is stored or transmitted (Regulation 5(1A)(b)). Both regulations stipulate security measures that are appropriate to the level of risk.

The principal question that emerges here is whether these provisions are sufficient to achieve socially desirable cybersecurity and data privacy outcomes. This is a question that we address from a variety of perspectives in the remainder of the report, starting with an analysis of primary data drawn from interviews and workshops in Part 3.

From a competition perspective, it is apparent that none of the regulations discussed above explicitly account for the competitive effects that adherence to these rules entails. The main source of concern that emerges in this context is that data sharing is often imposed as a means of promoting competition, for example under Open Banking. It is important to consider the extent to which the pro-competitive effects of such policies need to be balanced against security and privacy goals. Greater co-ordination between cybersecurity, data privacy and competition may be achieved, either by incorporating competition concerns into the above system of digital security regulations, or by incorporating a data protection objective into competition policy. This is an issue that we return to in detail in Part 5.2.

Part 3

Primary Data Analysis

We begin our evaluation of cybersecurity regulations in the UK and, in particular, their effectiveness in addressing interactions between security, privacy and competition by reviewing the primary data that was collected as part of this project via stakeholder interviews and workshops. Part 3.1 describes the nature of this primary data. A SWOT analysis of the existing regime of digital security regulation in the UK is presented in Part 3.2, before Part 3.3 discusses a range of policy recommendations that emerged from our interviews and workshops. We reflect on the open questions remaining after this qualitative analysis in Part 3.4.

3.1 Primary Data Collection

Primary data was collected via interviews and online workshops. We conducted ten structured interviews of c.1 hour duration with interview subjects representing a range of professional backgrounds, as summarised in Table 1 below.

Interviewee Area of Work	Number
Regulator & Government-linked	1
Law Enforcement	2
Legal & Security Advisers	5
Private Enterprise	2
Total Interviews	*10*

Table 1: Interview Data Collection

In each interview, we asked interviewees to assess the strengths and weaknesses of the existing regulatory framework, and to identify the most significant challenges and opportu-

nities connected with the promotion of digital security in the UK. We also invited interview participants to address directly the importance that should be attached to interactions between cybersecurity, data privacy and competition in designing more effective regulations.

Three online workshops were held on the topics of "Regulatory Interactions and the Design of Optimal Cybersecurity Policies" (April 2021), "Considerations in the Design of Cybersecurity Policies" (June 2021) and "Competition and Digital Security Regulation" (July 2021). The typical format for these events consisted of a panel of speakers, whose opening remarks were followed by discussion and Q&A with audience members. Our workshops were attended by a total of 36 participants representing academia and private sector research, regulation, law enforcement, financial services, SMEs and start-ups, legal, IT and information security consultancy.

3.2 Strengths, Weaknesses, Opportunities, Threats

The strengths, weaknesses, opportunities and threats highlighted by our interviewees in connection with the UK framework of digital security regulation are summarised as follows.

Strengths	Weaknesses
• NCSC and Government offer good advice • GDPR requirements for risk management and data protection are useful	• The human factor: consumers lack awareness and knowledge & employees are vulnerable to psychological manipulation • Lack of budget, planning and awareness, especially for SMEs • Risk-based approach lacks transparency
Opportunities	**Threats**
• International co-operation • Better defining liabilities and securing the supply chain • Auditing and enforcement • Ensuring trust, privacy and security in autonomous systems and AI	• Compliance costs and compatibility • Reliance on lay advice • System complexity, uncertainties and zero day threats • Enforcement issues around cost, consistency and transparency

Figure 1: Summary of SWOT Analysis

Strengths

The *NCSC* was highlighted as a strength, particularly in connection with the clarity of the advice it provides to market participants. More broadly, the *risk-based approach of the UK GDPR*,

as reflected in the appropriateness criterion, was viewed favourably by interview participants.

Weaknesses

The *human factor* was highlighted as a major weakness. Many issues around cybersecurity cannot be resolved technologically. Individuals may lack knowledge and awareness of cyber-risks and may not be savvy enough to follow best-practice.[1] For instance, they may be reluctant to change habits and may struggle to form accurate perceptions about their exposure to risk. Individuals can also be targets of *psychological manipulation*.

Particularly for SMEs, a *lack of planning* and *limited budgets* can prevent higher standards of security being implemented. Investments in cybersecurity are often neglected in a company's business plan on the basis that they offer little perceived return, resulting in cybersecurity becoming a priority only after a breach has occurred. Meeting standards such as ISO 27001 can involve hiring an additional staff member for many SMEs, with significant cost implications. Nonetheless, offering self-certification schemes free of charge has led to little increase in uptake in the past, suggesting a *lack of awareness* remains a significant issue for small firms.

While larger corporations are likely to have a dedicated legal function, *expertise in the area of data protection* specifically may nonetheless be lacking.

The risk-based approach to cybersecurity also has drawbacks in terms of *transparency*. For example, it may not be clear what precise measures have been implemented under self-assessment schemes such as Cyber Essentials. Moreover, the risk-based approach can be confusing for people, and the accurate assessment of risks is challenging.

Opportunities

Several means of improving outcomes within the current regulatory regime were suggested. Firstly, increased *international co-operation* was seen as a means of speeding up investigations into cyber-attacks. Secondly, a *clearer definition of liabilities* would allow firms to factor cyber-risks into their decision making more easily. Cases of invoice hijacking illustrate the difficult questions courts face in assigning liability in complex cases.

There are also significant opportunities for *pushing cybersecurity through the supply chain*. For example, this may happen by increasing awareness of required contractual terms under

[1] This also supports the Data & Marketing Association (DMA), according to whom "[t]he proportion of UK society who show little or no concern with the issue of digital privacy or data exchange has increased from 16% of the population in 2012 to 25% [in 2017]" (DMA, 2018). Deloitte (2020) found that the proportion of UK consumers who were "very concerned" about the use of their data halved from 47% in 2018 to 24% in 2020.

the GDPR, or by ensuring that unregulated entities operate in close enough proximity to regulated entities, as in Open Banking.

There is potential for regulators to *strengthen the auditing and enforcement process.* In addition, making government-approved security resources and guidance about best-practice more readily available could improve digital security outcomes.

Finally, there are significant opportunities around *automation and the use of Artificial Intelligence (AI) technologies*, which can improve security by recognising behavioural traits of users. This requires privacy and security concerns to be addressed, in particular the fact that the same technology can also be used to malign ends, for example by impersonating individual users.

Threats

The most significant threat to the more widespread adoption of hardware and software security is *cost.* Security features remain optional add-ins rather than default settings in many contexts such as cloud computing services. *Uncertainty* about the benefits of cybersecurity often leads to such options not being implemented on cost grounds. This is reflected in relatively low shares of cybersecurity in total business costs: these were estimated by interviewees at c.0.75% for manufacturing and retail, rising to c.1-2.5% for financial services and c.5% for dedicated security advisory firms.[2] Costs of updating old systems and compatibility between legacy systems and new technology are further threats.

On the enforcement side, *consistency* on the part of regulators as to which data breaches are investigated has been lacking. *Transparency* of investigation outcomes is also problematic, since any detected gaps in security protection cannot be too widely disclosed. This applies in connection with the FCA's CBEST testing, for example. Delays in introducing legislation to address new cyber-risks as well as the slow pace of co-operation across international jurisdictions represent additional threats.

Finally, despite the availability of detailed guidance from the NCSC and other sources, *lay advice* and worst-practice is often shared among firms via social networks. The *complexity* of systems and *zero day vulnerabilities* represent another serious threat.

[2]For large firms, these figures are likely to be reduced by a factor of up to 4 according to the response of another interviewee.

3.3 Policy Recommendations

Building on this SWOT analysis, we present a summary of the policy recommendations that were made in the course of our interviews and workshops. These recommendations fall into two broad areas. Firstly, they relate to the effectiveness of a centralised as opposed to a decentralised approach to regulating cybersecurity, including assessments as to the most appropriate regulatory instrument falling within each category. Table 2, below, provides a summary of policy measures associated with each approach.

Centralised Approach	Decentralised Approach
Standards	Penetration Testing
Awareness & Education	Data Anonymisation
Information Disclosure	
Liability Rules	
Consumer Control and Consent	

Table 2: Overview of Regulatory Instruments

Secondly, they address the importance of regulatory interactions and the appropriate degree of policy co-ordination between cybersecurity, data privacy and competition.

Interviews

All interviewees believed that more regulation and policy initiatives around cybersecurity and data privacy are needed, and that current regulation needs to be updated. They differed in terms of their precise ideas about which approaches to regulation would work best, however.

Concerning the desirability of a centralised vs. decentralised approach:

I_1 *Most* stated that a centralised approach is more effective than a decentralised approach. *A small number* mentioned that a decentralised approach may nonetheless be effective in raising awareness about security issues. *One* interviewee saw advantages and disadvantages with both approaches, depending on the precise way in which they are implemented.

I_2 *Some* interviewees argued in favour of minimum security standards, for example self-certification schemes (e.g. Cyber Essentials, Cyber Essentials Plus), the NIS Regulations in relation to OESs and RDSPs, standards for digital payments infrastructure, the duty

of care for financial firms, and safety regulations for the Internet of Things and motor vehicles.

I_3 *Most* advocated for measures to increase consumer awareness, such as education about security risks and training in the use of protective measures. *One* interviewee mentioned that cyber-awareness training, such as the NCSC's Cyber Aware campaign, is a useful way of promoting a wider understanding of the value of security.

I_4 *Some* interviewees emphasised the importance of information disclosure. This relates to the mandatory reporting of data breaches and vulnerabilities to regulators, but also to information sharing regarding cybersecurity between different departments within an organisation.

I_5 *Some* highlighted the importance of consumer control and consent. The UK GDPR gives consumers greater control of their data, but *one* interviewee mentioned that there is excessive reliance on consumer consent as the legal basis for data processing.

I_6 *A small number* mentioned liability rules and the difficulties involved in clearly allocating liability for cyber-damages when they arise.

I_7 *A small number of* interviewees emphasised consumer protection policies, for instance ensuring that adequate mechanisms for redress are available to end users.

I_8 In terms of data sharing, *none* of our interviewees remarked on any difficulties among small firms in accessing data from large, gatekeeper firms.

I_9 To reduce the cognitive burden of regulations, *one* interviewee highlighted the potential for regulation to become automated, though implementing this in practice would be challenging. Relatedly, *a small number of* interviewees also mentioned that government guidance needs to be easy to understand and simple to follow.

I_{10} In terms of the decentralised approach, *most* interviewees said that penetration testing and 'white hats' are important because they help to identify vulnerabilities, induce responsible disclosure, and lead to better reporting incentives since private companies, subject to reputational pressure, may have incentives to hide vulnerabilities. In general, the effectiveness of penetration tests depends on company size and budget. *Some* viewed anonymisation of data as useful, but only if it is done correctly. *A small number* regarded full anonymisation as difficult and costly to achieve.

Concerning regulatory interactions and policy co-ordination:

I_{11} *All* interviewees viewed cybersecurity and data privacy as interdependent but stated that, in practice, they are often treated in isolation of one another. For example, cybersecurity is often delegated to IT departments, while HR manages data retention and disclosure. *A small number of* interviewees mentioned that this could be due to a lack of awareness and understanding about security, and the fact that links between security and privacy are not adequately reflected in current regulations.

I_{12} *Most* interviewees thought that regulations need to be co-ordinated because (i) co-ordination can help to close regulatory gaps and pool regulatory competencies, especially when, in the digital age, the finance, health, water, and energy sectors all confront digital problems, (ii) a one-stop-shop would be especially useful for SMEs, which have limited resources, although this can take a long time to set up, and (iii) unintended side-effects caused by regulations targeted exclusively in one area can be costly.

I_{13} *A small number of* interviewees identified overlaps between regulations targeting cybersecurity/data privacy and competition. *One* interviewee mentioned that access by privileged firms to large volumes of data can create competition concerns but, on the other hand, that competition may not work effectively if data is very fragmented.

I_{14} *Most* agreed that a firm's cybersecurity and data privacy practices can give it a competitive advantage over market rivals. A cyber-breach affects reputation negatively, while having a cybersecurity badge or certificate and sound data protection policies generates trust and positive reputational effects. *Some* stated that firms will adjust their security and data privacy strategies in response to an increase in competition.

Workshops

In general, regulation was felt to be lacking, although the appropriate design of regulations needs further investigation.

Concerning the desirability of alternative regulations:

W_1 In broad terms, regulation can be effective in achieving greater security. To do so it needs to alter *firm incentives* (as the GDPR did by increasing fine levels, for instance). Changes to firm incentives brought about by regulation can explain important security improvements, for example with respect to sim cards (preventing toll fraud), banking

(preventing liability claims from depositors) and wi-fi connectivity (authentication enabled to prevent signal stealing).

W_2 Digital security by design should not ignore the importance of the *human factor*. The human factor is not only present in the form of the end-user, but integral to every level of the security ecosystem. The human factor represents one reason why increasing security is not always in firms' private interests, since consumers may not be aware of such improvements. Raising *awareness* among consumers is an important objective, but security communications, informal security training and formal security education must be effectively designed to meet that objective. For example, they should avoid a one-size-fits-all approach and focus on the specific threats and vulnerabilities in each specific context.

W_3 *Employee training* and *workplace culture* are also important. Staff need to be trained and work in a culture in which mistakes can be reported. SMEs in particular need to be given *support* to understand and comply with regulations. Given appropriate training and staff culture, the human factor can also become a strength in the security context. *Automation* can be helpful in mitigating risks associated with the human factor. One example of this is including the payee's name in bank transfers.

W_4 *Certification schemes* are an increasingly important driver of cybersecurity incentives. These are a recognised means under the GDPR for firms to demonstrate compliance with data protection regulations but, in general terms, their quality and independence remains unclear. Certification is particularly important for smaller companies that are not under close regulatory scrutiny. In that connection, SMEs account for the majority of firms achieving Cyber Essentials certification. Only 13% of certified companies are large.

W_5 *Disclosure* matters, although it can be difficult to convey to customers that a firm is actually regulated, since regulators (for example the FCA in the context of its CBEST reviews) cannot disclose the outcome of its security reviews, because this would highlight vulnerabilities.

W_6 *Independent oversight*, as is required in connection with cyber-insurance for example, can be an important tool to prevent security incidents being suppressed. In relation to cyber-insurance, characterising cybersecurity risk is a major obstacle to wider adoption, especially given the lack of historical data concerning risks in this area.

W_7 *Liability rules* can also be an important tool to alter firm incentives.

Concerning regulatory interactions and policy co-ordination:

W_8 *Competition* has an important role to play. While most firms do not compete on the strength of their cybersecurity, there are important exceptions (e.g. vendors of security products, Apple, and banks).

W_9 Competition also matters in connection with regulatory issues around cybersecurity and data privacy because access to personal data is often concentrated in the hands of a few 'gatekeeper' firms, who derive their dominant market position from the access they have to consumer data. The EU Data Governance Act is a proposal to limit this market power by preventing gatekeepers from storing or moving European data subjects' data, instead obliging them to access it via data trusts.

W_{10} *Open Banking* is another example of an attempt to limit the power of incumbent firms by promoting data sharing. This aims to reduce switching costs, although there is limited evidence that Open Banking has succeeded in this objective. On the other hand, security has been robust under Open Banking thanks to the "whitelist" model operated by the OB Implementation Entity, which owns and maintains the directory of OB participants.

W_{11} More broadly in the financial services context, the usual *know your client checks* extend beyond financial concerns (counterparty risk, money laundering, etc.) to encompass security checks. It is important to go beyond verifying that certification is current to determine the actual security measures that are in place.

W_{12} New means of organising and sharing data present new challenges for cybersecurity and data privacy regulation. From an individual data subject's perspective, these means include personal information management systems, personal online data stores and privacy-enhancing technologies. From a collective perspective, they include data trusts and data co-operatives.

W_{13} Given the importance of the human factor, there is significant overlap between cybersecurity regulation and consumer protection. The ICO and CMA are working together to develop a new norm of 'fair by design'.

W_{14} Regulations and their enforcement need to be co-ordinated *within firms*, to take into account disparities between new and legacy systems that might have been acquired via

mergers & acquisitions and *nationally*, to prevent a situation in which different regulators provide conflicting messages. Regulation also needs to keep pace with innovation and not stick to a technologically outdated status quo.

3.4 *Open Questions*

In summary, our primary data analysis demonstrates that regulatory interactions, especially those between cybersecurity and data privacy, matter in the eyes of market participants. Despite this, current regulations can lead to shortcomings in this respect, as security and privacy decisions are often separated within firms. While the current regime of digital security regulation in the UK has several strengths, there are also important weaknesses, opportunities and threats, in light of which it is important to consider what measures might be taken to improve the regulatory framework.

A wide range of policy recommendations emerges from our primary data analysis. While broadly in favour of a centralised approach, they are varied in terms of the importance they attach to specific regulatory instruments falling within this approach. In order to determine the most effective way of aligning firms' incentives with society's interests, we therefore require an objective basis on which to evaluate these competing proposals.

Theoretical modelling work allows the welfare consequences of alternative regulations to be studied in isolation of conflating factors. We therefore move on to a review of the academic literature and technical reports to summarise the existing state of knowledge in this area. Thereafter, we present the results of two original pieces of research that directly address the question of regulatory interactions in relation to cybersecurity.

Part 4

Literature Review

In this part, we review a number of technical reports on the question of cybersecurity incentives and regulation (Part 4.1) before reviewing the academic literature in the area of cybersecurity and data privacy (Part 4.2).

4.1 Technical Reports

The reports we discuss below serve to highlight the importance that policy makers attach to the question of economic incentives in the cybersecurity context, thereby underlining the importance of this research agenda. They also give important insights into the approaches to regulation currently favoured by policy makers.

UK

The 2020 Review of Cyber Security Incentives and Regulation (hereafter, 'the Review') invited responses from industry participants in order to identify the major obstacles to greater digital security adoption in the UK (see DCMS, 2020b).[1] In contrast to the previous Cyber Security Regulation and Incentives Review (see DCMS, 2016), the latest Review was characterised by a far greater focus on economic incentives in addition to technological capabilities. Lacking incentives were identified both by the Government in advance of the Review and by respondents to the Review as one of the most significant barriers to adoption.[2]

[1] The issue of incentives is also mentioned in connection with the question of trust in data ecosystems in Open Data Institute (2021).

[2] By comparison, the 2016 Review concluded that "additional cyber security regulation [...] is not currently justified. It should ultimately be for organisations to manage their own risk in respect of their own sensitive data and online presence, and it should be in their commercial interests to invest in their protection. Government

> "While we believe that Government initiatives to date have had a positive impact on cyber security, these efforts have tended to focus on improving organisational *capability* [...]. Less explicit focus has been placed on exploring and addressing *commercial rationales for investment in cyber security.* [...] The findings highlight that a lack of commercial rationale is a *significant barrier for organisations*, and was identified to be an even more severe barrier for micro and small organisations."
>
> DCMS (2020b), emphasis added

Over 70% of respondents to the Review agreed that the lack of a commercial rationale represented a moderate or severe barrier to firms managing cyber-risks. Moreover, the additional barriers that were mentioned by respondents both relate precisely to the question of incentives and regulation. The first of these was "a lack of incentives to support organisations to protect their organisation online". The second, was "insufficient regulation to compel organisations to better manage cyber risks."

A major obstacle to security incentives identified in the Review concerned information about the harm of cyber-attacks, which 89% of respondents viewed as integral to decisions about cyber-investments. Without clear information about the benefits of cyber-investments, their costs typically cannot be justified (this ties in with the threats identified in our qualitative analysis). 10% of respondents stated that a lack of regulation was one factor preventing greater access to information. Moreover, 45% thought that more regulation was needed to increase senior management accountability for cyber risk management, which ties in with our preceding discussion of liability rules.

In terms of Government responses, the Call for Evidence coincided with the launch of the Cyber Aware campaign and the introduction by the NCSC of new guidance for firms. These measures tie in with the issue of awareness discussed in Part 3.2 (see weaknesses). Moreover, the Government has also recently launched a new cybersecurity funding scheme for healthcare suppliers, see HM Government (2020). Of course, to the extent that inadequate incentives are due to a lack of information rather than budget constraints, the effectiveness of such funding may be limited. This relates back to the weaknesses discussed in Part 3.2, where it was stated that offering self-certification schemes free of charge led to limited increases in uptake among firms, which might be explained by a lack of awareness on their part.

Finally, the Review contains limited discussion of most of the regulations summarised in Table 2 of this report. These will be analysed in more detail in Part 5, where we also argue that

is clear that all businesses have a responsibility to consider their own cyber security and act in their business interests to protect themselves from cyber attack." (DCMS, 2016, p11).

a more prescriptive approach to regulation than is currently envisaged by the Government may well be needed.

Internationally

In the US, the Department of Homeland Security has published a research strategy that highlights the principle objectives for economic research in the area of cybersecurity (see Department of Homeland Security, 2018). Most of these tie in closely with the focus of this report, not least Theme 2 ("Role of Government, Law, and Insurance"), Theme 3 ("Third Party Risk"), Theme 4 ("Organizational Behavior and Incentives") and Theme 5 ("Data Collection and Sharing").

Finally, the Organisation for Economic Co-operation and Development (OECD) provides an overview of digital security threats and mitigation approaches in OECD (2021). As well as describing the nature of various cyber-threats, the report also highlights the importance of economic incentives:

> "Many challenges to effective vulnerability treatment are economic in nature. They include a lack of co-operation amongst stakeholders, *limited market incentives*, legal barriers, and lack of resources and skills."
>
> (OECD, 2021, p.6), emphasis added

Incentives are particularly emphasised in connection with achieving the ideal 'vulnerability lifecycle' (discovery, handling, management, disclosure), which ties in with several points from our qualitative analysis (e.g. I_4, W_5).

4.2 Academic Literature

Cybersecurity

This section reviews the economics and management literatures on cybersecurity, which mainly focus on the incentives to invest and the efficiency of markets in providing such incentives. The security features of a given product can be seen as one factor determining that product's quality. We can therefore apply classic economic theories on quality competition, such as Spence (1975) and Mussa and Rosen (1978), to analyse incentives and distortions from the efficient market outcome caused by market power in the context of cybersecurity. However, rather than providing an exhaustive review of the vast literature on market power and

regulation, the primary focus of this review is to survey the more recent literature relating to specific issues of cybersecurity.

To start with, it is common for firms to invest in multiple alternatives to protect their IT systems before and after a product launch. Lam (2016) studies multi-dimensional security investments in preventing and mitigating the effects of cyber-attacks. She shows that when IT users can undertake security measures to reduce the expected damage of cyber-attacks, firms may underinvest in attack prevention early on but overinvest in damage control after sales. Government interventions in the form of a security standard and a partial liability rule, which does not hold the firm fully liable for cyber-damages, can be used to improve efficiency in cybersecurity investments, as these legal requirements offer incentives for firms to rely less on bug fixing investments after sales and to release a safer product in the first place.

Much of the prior work on cybersecurity focuses on a single dimension of security investment, for example, on damage control or bug fixing. If a vulnerability is discovered after product launches, an important question is whether firms should disclose such information. Some papers have debated the pros and cons of voluntary versus mandatory vulnerability disclosure. In Choi *et al.* (2010), vulnerability disclosure along with the release of patches or updates can help protect users who apply these updates. However, applying updates is costly because of downtime that interferes with the current activities of users, the effort required to download and install updates, and potential risks of system crashes brought about by the updates. Therefore not all users are prepared to incur these costs and apply updates in a timely manner. For these users, vulnerability disclosure may enable hackers to exploit the vulnerability and harm them. When users' costs of installing the updates are sufficiently high, a mandatory disclosure regulatory policy may be desirable.

When vulnerability disclosure does not coincide with the patch release time, Arora *et al.* (2008) show that patch releases are excessively delayed because firms do not fully internalise user damage when attackers exploit a known vulnerability. In these cases, it would be useful for the regulator to consider shortening the notification period when it is legal for a firm to keep a vulnerability secret.

As mentioned in the Introduction, the damages associated with a security breach are varied and include the costs of preventing, detecting, and mitigating such breaches, revenue losses, reputational damage, and legal liabilities. To quantify these costs, some research studies have examined the impact of security information disclosures on stock market returns, albeit with mixed results. Cavusoglu *et al.* (2004) find that disclosure of a security breach has a significant negative effect on a firm's stock price. However, Campbell *et al.* (2003) show that this effect depends on the nature of the data that is compromised. Stock prices are likely to fall whenever

a breach leaks confidential information, but when confidential information is not involved a breach has no significant effect on stock price. Using a different categorisation of breaches, Gordon *et al.* (2011) show that different types of security breaches have different impacts on stock market returns, with breaches related to denying authorised users access to services having the most negative impact. Gordon *et al.* (2010) further consider voluntary disclosures of proactive security measures and show that this has a positive effect on a firm's market value.

In an event study, Gordon *et al.* (2011) show that security breaches have become less costly over time by comparing the costs of security breaches in the periods preceding and following the September 11, 2001, attacks. A plausible explanation is that investors' attitudes towards security breaches have changed. As security breaches become more common, people tend to become less concerned and view security breaches as a small nuisance rather than a serious risk management issue. When investors and firms grow overly optimistic about what might go wrong, it might be desirable for regulators to step in. In summary, whether information disclosure increases or decreases firm value depends on what type of security information is disclosed. Firms may also strategically disclose information to attract customers and investors, leading to an increase in firm value. For a recent review of event studies, see Spanos and Angelis (2016).

Firms may also decide to share security information among themselves. Gal-Or and Ghose (2005) show that an increase in security investments or information sharing by one firm will induce other firms to increase their security investments and information sharing. Information-sharing alliances that promote disclosure and sharing of security vulnerabilities, security best-practices, and technological solutions (such as the Information Sharing and Analysis Centres in the US) are more valuable in more competitive industries, where firms strategically share information and increase security investments to reduce the intensity of price competition with rivals.

On the issue of user incentives, Varian (2004) considers security investments as a public good, since the security of the whole system depends on the investments of individuals in the team. He shows that system reliability depends on whether protection levels are determined by the efforts of the most careless defender, the best defender or all defenders. Accordingly, a firm could improve protection levels by strategically adjusting its IT hiring decisions (e.g. hiring fewer but better staff, hiring only the best, or prioritising quantity of staff over quality). August and Tunay (2006) consider the incentives of users to patch security vulnerabilities in the presence of patching costs and negative security externalities. The unpatched users exert negative externalities on patched users since, if a user fails to install patches, they will harm

other users by increasing the level of risk they are exposed to. Their results indicate that when security risk and patching costs are high, a subsidy on patching (e.g. a reward to encourage timely patching) is better than mandatory patching.

Furthermore, network structure can strongly influence investment incentives. Acemoglu *et al.* (2016) examine a model of security investments in a network where attacks are contagious. In the case of strategic attacks, that is when an attacker can target a particular firm, overinvestment may emerge because larger security investments shift attacks to other firms. Closely related is a large literature on network games (see Jackson and Zenou, 2015, for a thorough review). These models can be applied to various settings, such as a network of players/firms undertaking investments against a cyber-attack, a financial risk or an infectious disease.

Data Privacy

The literature on data privacy is very rich, dating back to the 1970s (see seminal writings of researchers such as Richard Posner and George Stigler), but an exhaustive review is beyond the scope of this report. The main focus of the more recent literature is on the sharing of customer information between firms and information disclosure by consumers. For example, Calzolari and Pavan (2006) show that the exchange of information between two firms that are interested in discovering consumers' willingness to pay may, in some cases, induce more efficient information use and benefit both firms and consumers.

In Taylor (2004), a firm selling a product in early periods can sell customer data to a firm that sells a related product in a later period, which allows the second firm to infer consumers' preferences and engage in price discrimination. For example, if a consumer purchased from the first firm, then the second firm can infer that the valuation of that customer is higher than if the consumer did not make the purchase. If consumers are savvy, in the sense that they are able to anticipate that disclosing information will reduce their future surplus and therefore strategically withhold such information, then it is in firms' best interest to implement their own privacy protection policies, even without any government regulation that prohibits information sharing.

In a related set-up, Argenziano and Bonatti (2021) study the impact of different forms of privacy regulations, such as transparency, consent, and limits to discrimination. They show that voluntary consent is beneficial to consumers but that a ban on discriminatory offers is harmful. This is because, under voluntary consent, consumers can veto data sharing between firms, and firms can adjust their terms of trade (quality level and price) based on consumers'

consent decisions. Thus, data sharing happens whenever it is mutually beneficial for both consumers and firms. However, under the right to equal service, firms cannot adjust their terms of trade in response to consumers' strategic information disclosure. As a consequence, limits to discrimination may result in consumers consenting to harmful data sharing practices, even if they would have refused to share their data when discriminatory offers are possible.

With recent advancements in consumer tracking technologies, firms can build a precise profile and offer personalised products, prices or ads to consumers, but the collection and usage of consumer information may raise privacy concerns. This has led to a flurry of research on the interplay between privacy considerations and enhanced personalisation. For instance, Gal-Or *et al.* (2018) examine the effect of privacy concerns on competition between online advertising platforms, such as Facebook and Google, who collect consumer information for the purpose of making ads more relevant. In their model, consumers' and advertisers' preferences for targeting are heterogeneous: some consumers are more sensitive to data collection and are therefore more averse to targeted advertising, while other consumers prefer to view more relevant ads. Firms that focus on a niche market can benefit more from high levels of targeting than firms that sell products that have a broad appeal. The presence of such heterogeneity in preferences for targeting on the demand side leads platforms to differentiate the targeting levels they offer to advertisers, which in turn influences the offers received by the consumers. The platform that offers the higher targeting level ends up with larger market shares in both the ad and the product markets, which allows it to charge higher prices and earn higher profits. On the other hand, smaller platforms offer more privacy to consumers in order to differentiate themselves from their competitors.

Further up the supply chain, we observe data brokers (e.g., Acxiom, Datalogix, and Nielsen) aggregating data from different sources, and selling information to firms for price discrimination purposes. They can influence downstream competition by controlling access to information. When data brokers can only sell either all available information on consumers or no information at all (i.e., they cannot sell a subset of information), Montes *et al.* (2019) show that a data broker has incentives to sell information exclusively to one firm. With only one of the competing firms able to set personalised prices, price competition is less intense in the product market.

However, when data brokers can sell a subset of information to downstream firms (e.g., large versus smaller datasets, and more precise versus less precise profiles), Belleflamme *et al.* (2020) show that a data broker has incentives to sell datasets of different qualities to downstream firms in a non-exclusive manner, as firms ending up with different abilities to profile consumers can soften price competition in the product market and, hence, increase the firms'

willingness to pay for the data brokers' services.

Data brokers may also transact and exchange information with each other (see Federal Trade Commission, 2014). Gu *et al.* (2020) show that data brokers have incentives to share information with each other when datasets contain overlapping information or data points are correlated, as information sharing avoids fierce price competition between data brokers.

Ichihashi (2020) studies a monopolist who uses information about consumers for both product matching and pricing purposes. He shows that, in some cases, the firm prefers not to use information for pricing in order to incentivise information disclosure by consumers, but such a strategy hurts consumers due to potential product mismatch.

Empirical studies investigating the need for data privacy regulations provide mixed results. In a field study, Goldfarb and Tucker (2011a) provide empirical evidence that overly precise profiling can trigger a negative response from consumers due to privacy concerns. However, other empirical studies caution that privacy regulations, despite their positive intentions, may reduce ad effectiveness. For example, Goldfarb and Tucker (2011b) find that, after the implementation of the EU e-Privacy Directive, advertising effectiveness of internet banner ads in Europe decreased significantly on average. However, not all advertising was affected equally. The loss in effectiveness is more pronounced for ads on general-interest websites (such as news and games) compared to ads on niche websites (such as health and automotive). The consequence might be a higher price charged to the consumers for access to content or a change in the mix of content. First, as advertisers become less willing to pay for less effective ads and content providers earn less from the advertisers, platforms may charge a higher price to consumers in order to recoup lost revenues on the advertisers' side. Second, as niche content becomes more profitable relative to general-interest content, content may become more narrowly focused. Therefore, privacy regulation can be seen as a trade-off between the benefits of consumer privacy on the one hand, and the costs of reduced ad and content relevance and higher prices on the other.

Overall, topics related to data can be very diverse, For more general discussion, we refer interested readers to excellent surveys of the economic literature on privacy and data markets by Acquisti *et al.* (2016) and Bergemann and Bonatti (2019).

4.3 *Open Questions*

This literature review emphasises the importance that governments and international organisations attach to the question of economic incentives in the context of cybersecurity regulation. Moreover, the discussion of the academic literature highlights the insights that a

theoretical investigation of cybersecurity and data privacy can bring.

Despite the variety of approaches to studying regulation in these areas, what is notable about the academic literature is that it considers security and privacy questions in isolation of one another. One example of a paper that does touch on both security and privacy simultaneously is Jullien *et al.* (2020). However, this work does not clearly distinguish between these concepts. In particular, Jullien *et al.* (2020) analyse a monopolist platform's optimal privacy policy when it monetises information collected from consumers by charging third parties for access. The platform's privacy policy can be interpreted as a precautionary 'investment' that screens third parties and limits third party access in order to protect consumer data from attacks. Therefore this notion of investment encompasses both cybersecurity and data privacy.[3]

The principle open question emerging from this review is therefore the following: what implications does the clear logical separation of cybersecurity and data privacy have for the design of optimal cybersecurity policies once we allow for firms' incentives in these dimensions to be interrelated? In Part 5, we discuss two original contributions that investigate this question, and which further allow us to contrast the outcomes arising in monopolistic and competitive market settings. We also relate the conclusions of this research back to the primary evidence summarised in the qualitative analysis of Part 3.

[3]In this model, data collection may lower the quality of the consumer experience, for example when third parties expose consumers to data leaks, theft or extortion. Consumers have limited or no awareness about these potential cyber-risks when dealing with third parties. While a higher level of privacy/cybersecurity protects consumers from cyber-risks, it limits their opportunities to learn about their vulnerability to attacks and to enjoy beneficial matches with third parties.

Part 5

Theoretical Results & Evidence

In this part we discuss two original contributions that extend the academic literature by addressing directly the question of regulatory interactions. Part 5.1 discusses interactions between cybersecurity and data privacy. Part 5.2 discusses the role of competition.

5.1 Interactions between Cybersecurity & Data Privacy

As motivated in the Introduction, both cybersecurity and data privacy can be understood in terms of the dissemination of consumer data through the economy. This occurs intentionally when a data controlling firm decides to share data with a third party, and unintentionally when hackers succeed in overcoming the controller's cyber-defences.

Our primary data analysis in Part 3 highlights the fact that market participants consider interactions between security and privacy to be important (I_{11}, I_{12}). From Part 2 we know that, in the existing UK framework of regulations, these interactions are taken into account in a rather limited sense. In particular, the UK GDPR and DPA 2018 rely on a firm's assessment as to the appropriate level of security given its data processing (data sharing) activities.

In order to study the interactions between security and privacy in more detail and to derive regulatory implications, Lam and Seifert (2021a) develop a model that clearly distinguishes between cybersecurity and data privacy. The structure of this model is illustrated in Figure 2 below.

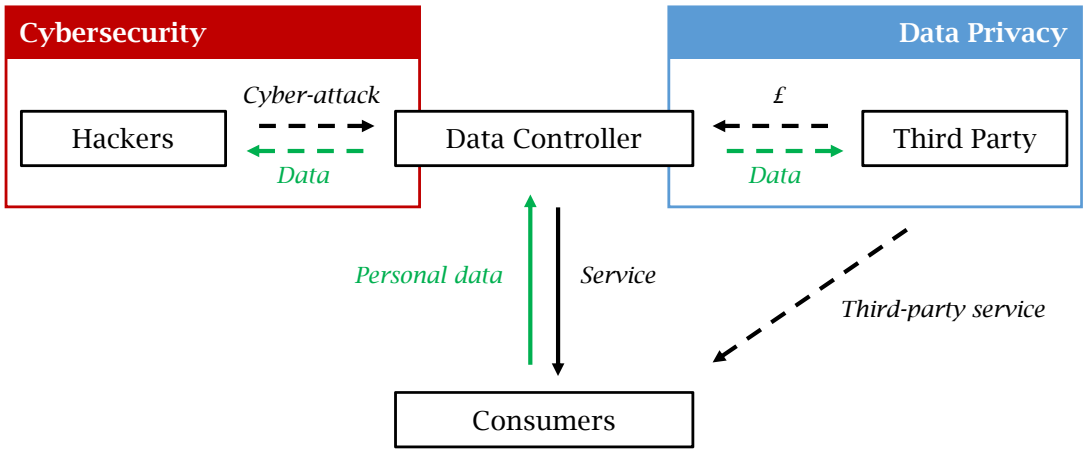


Figure 2: Model Schematic – Cybersecurity & Data Privacy

The strategic actor in this model is the data controller, which faces a threefold decision problem. Firstly, it decides on the price to charge consumers for access to its product or service, and any consumer who purchases the product simultaneously hands over a volume of personal data to the controller.[1] Secondly, the data controller then decides whether or not to share this data with a third party. This third party is willing to pay for data access because it provides its own service to consumers, the value of which is increased if it has access to the data collected by the controller.[2] Finally, the data controller also determines the level of its investment in cybersecurity, with higher levels of security investment leading to a lower probability of a harmful hack occurring.

The only consumers who will purchase the product offered by the data controller will be those attaching a sufficiently high value to it. In particular, this valuation must be high enough to offset not only the purchase price, but also any residual cyber-damages that consumers anticipate in the future. This residual liability for cyber-damages on the part of consumers arises because, when data is shared with the third party, a successful hack on the controller leads to a possible follow-on attack on the third party and, in the baseline model, consumers are liable for damages arising from such follow-on attacks.[3]

In this regard, the model further distinguishes between *savvy* and *non-savvy* consumers. This allows us to separate (savvy) consumers who are able to factor data-related risks into their decision to interact with the data controller from (non-savvy) consumers who disregard

[1] This data may capture name, address, and other details required by the data controller, or information that is collected passively via browser cookies.

[2] The reasons for which this might occur include product customisation and price targeting, for example (McKinsey & Company, 2016).

[3] This ties in with point I_{12} in Part 3.3, for example, relating to the difficulty of holding firms liable for cyber-damages. Intuitively, the more widely data is shared, the more points of attack there are for hackers to target.

cyber-risks. In this way, we capture the observed tendency of significant proportions of the consumer population to disregard data risks in their decision making.[4]

Business Implications

Since regulations exist in order to bring private incentives into line with societal goals, a first important question concerns the interactions between a firm's cybersecurity and data privacy (data sharing) choices. If these are interdependent, regulations targeting one or other of these areas must take the interrelated nature of firms' incentives into account.

In this regard, we show that a profit maximising data controller will tend to increase its security investment when sharing data with the third party. In particular, we have:

> ***Result 1:*** *Provided the damage caused by a data breach is not too large, profit maximisation implies that firms will invest more in cybersecurity when they share data with a third party.*

This relationship between security and privacy arises as the balance of several conflicting effects. Whenever the damage of any individual data breach is not too large,[5] the overall result goes in the same direction as the *demand responsiveness effect.* This describes the fact that, as soon as data is shared, the demand for the data controller's product becomes responsive to the chosen level of cybersecurity because savvy consumers anticipate that, the lower the level of security, the greater the likelihood with which they will incur damages as a result of follow-on attacks in future. This incentivises the controller to invest more in security when data is shared in order to retain a greater share of its demand originating from savvy consumers.

This also supports the GDPR's notion of appropriateness, according to which more risky data processing activities, reflected here in the controller's decision to share data with the third party, should be accompanied by higher levels of security. Nonetheless, we explain below that regulation is still needed in order to tackle market failures relating to both cybersecurity and data privacy.

Regulatory Implications

Regulation is needed in this market because, despite the broad relationship between cyber-security and data privacy described above, important market failures remain with respect to both. Firstly, we have:

[4] Recall footnote 1 in Part 3.

[5] The relevant condition is satisfied for the majority of cyber-breaches, see Mann (2015, pp. 321-322).

Result 2: *Firms under-invest in cybersecurity.*

Under-investment occurs because of a divergence between the data controller's and society's objectives. The firm's concern for its margin leads it to increase prices above the level that society would choose, since society is more concerned with ensuring that consumers have access to the product or service offered by the firm. With a higher price, and the associated lower demand, the incentive to invest in security falls.

This ties in with the evidence discussed as part of the threats in our primary data analysis, in particular the low levels of operational expenditure that is typically allocated to cybersecurity.

The second market failure relates to the firm's data sharing decisions.

Result 3: *Firms tend to over-share data.*

The reason for this result goes back to the presence of non-savvy consumers in the population. Since these consumers do not respond to the increased cyber-risks that accompany the data controller's decision to share data, the firm exploits the presence of non-savvy consumers by sharing data too frequently. Society takes all cyber-damages into account, irrespective of whether they are anticipated by consumers or not.

While direct evidence on the tendency of data controlling firms to share data is difficult to obtain, this relates to point I_8, according to which no difficulties in obtaining data from gatekeeper firms were reported by our interviewees.

In correcting these market failures, it is of course vital to select the most appropriate of a wide range of possible instruments (see Table 2). By considering, in particular, minimum security standards, disclosure and consumer education policies, liability rules, and consumer mitigation strategies, we demonstrate below that evaluating the welfare impact of alternative regulations requires the interactions between cybersecurity and data privacy to be taken into account.

(i) *Minimum standard on security.* A first potential solution to the under-investment problem lies in the imposition of a minimum security standard, which stipulates a minimum level of security that firms must implement. These have already been discussed in the context of our primary data analysis (I_2, W_4). We are able to show analytically that, holding fixed the firm's data sharing decision, implementing a minimum security standard improves social welfare when it causes the firm to increase its investments above the level they would otherwise have chosen. However, the firm's data sharing decision

typically cannot be held fixed in practice. We show that, allowing for profit maximising data sharing choices on the part of the data controller, increasing the level of the security standard can have unintended social welfare consequences when it induces the firm to share data inefficiently. Determining whether or not minimum standards are an effective solution to the under-investment problem therefore rests crucially on the impact they simultaneously exert on a firm's decision to share data.

(ii) *Disclosure and consumer education policies.* Disclosure and consumer education policies were discussed extensively in our interviews and workshops (e.g. I_3, I_4, W_2, W_5). We are able to capture the effects of disclosure and consumer education policies in the model by associating them with an increase in the fraction of savvy consumers. We again demonstrate the crucial importance of regulatory interactions. While the firm's security investments rise as the fraction of sophisticated consumers increases, total demand in the economy simultaneously falls because more consumers decide to withhold data in the face of data risks. Consumer policies may have unintended consequences on welfare, unless the increase in savvy consumers deters the firm from sharing data at all. In that case, welfare increases because the risk of follow-on attacks is eliminated entirely. Again, the welfare properties of this class of regulation rest crucially on the interactions between cybersecurity and data privacy.

(iii) *Stricter liability rules.* Liability rules were also covered during our interviews and workshops (I_6, W_7). We can study the effect of stricter liability rules by supposing that the data controller is liable for cyber-damages, irrespective of whether they arise from an attack on the controller itself or on the third party. We show that welfare is lower under such a full liability rule when the firm would share data, regardless of which liability rule is implemented. This is the case because the firm internalises follow-on cyber-attacks under the full liability rule by setting a higher price, and the associated drop in demand is not sufficiently offset by increases in security investment. On the other hand, the firm is less likely to share data under full liability, since it is now liable for the harm of follow-on attacks, and, when the full liability rule causes the firm to stop sharing data, welfare can again increase because the risk of follow-on attacks is eliminated.

(iv) *Consumer mitigation strategies.* A final regulatory approach that we study in the model encompasses consumer mitigation strategies. These capture methods, such as changing passwords, spending time to monitor user accounts, and using private browsing modes and ad blockers, by which consumers can themselves reduce the extent of the damage they suffer as a result of a cyber-attack. This ties in with the ideas of empowering

consumers in digital markets contained in I_5, I_7 and W_{12}. We find that giving consumers the means to reduce the extent of the damages they suffer in case of a successful hack crowds out the security investments made by the data controller. Offering consumers more mitigation options may have unintended consequences, especially when the drop in the firm's investments is not adequately offset by consumers' mitigation efforts.

This analysis highlights the fact that many of the policy recommendations made in the course of our primary data collection exercise represent only partial solutions to market failures in the area of cybersecurity. Whenever unilateral regulations exert unintended effects on welfare, a co-ordinated approach to regulation, which simultaneously considers firm's data sharing incentives, is needed. This will likely need to go beyond the more limited co-ordination currently reflected in the UK GDPR (see Part 2.4). In particular, while there is some evidence that the GDPR has increased cybersecurity investments (see RSM UK Consulting, 2020), we show that firms nonetheless face insufficient incentives in this regard.

This suggests that a more prescriptive approach is needed. Such an approach would need to set out not only the limits within which firms may lawfully share data, but also specify more directly the required security precautions that must accompany specific types of data sharing, rather than relying on firms to make their own decisions in this regard. More broadly, any regulatory approach in this area must appropriately balance firms' interdependent decisions regarding cybersecurity and data privacy.

5.2 The Effect of Competition

Our second theoretical contribution extends the above analysis to consider the effect of competition. This is an important innovation if we wish to analyse the impact of Open Banking (see W_{10}) and related initiatives, which take a data-driven approach to increasing market competition. More broadly, interactions between cybersecurity and competition were also highlighted as important by several of our interviewees and workshop participants (see, in particular, I_{13}, I_{14}, W_9, W_{10}).

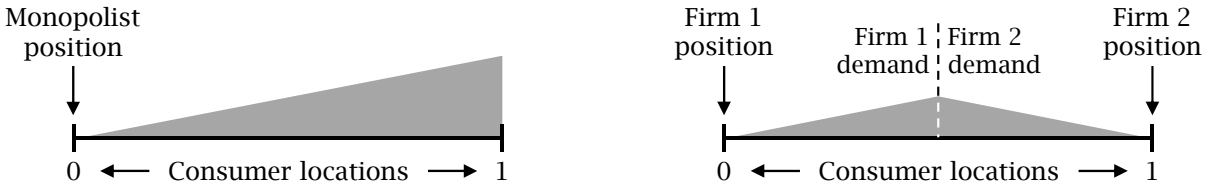
Open Banking was introduced following the CMA Retail Banking Market Investigation in 2017. Rather than breaking up the small number of banks that occupy a dominant market position in the UK, this remedy sought to promote competition by encouraging data sharing between incumbent banks and third parties, thereby reducing the costs of switching providers. Discussions are already taking place around proposals to extend Open Banking beyond transaction data from bank accounts and payment services to include mortgage, savings, pensions,

insurance and consumer credit products ("Open Finance"), and to other sectors besides financial services, particularly communications and energy ("Smart Data").[6]

Evaluating the consequences of any of these data-focused means of promoting competition must consider their effects on cybersecurity and data privacy. To that end, Lam and Seifert (2021b) develop a model to investigate whether or not increasing competition improves welfare once the interactions between firms' cybersecurity and data sharing choices are taken into account.

This model is based on the Hotelling framework of horizontal product differentiation (Belleflamme and Peitz, 2015). In this set-up, a market of a fixed size is envisaged as an interval or line comprising all possible locations at which consumers seeking to purchase a product or firms looking to sell might be located. These locations and, in particular, the distance between a given consumer and its nearest firm can be understood in terms of both geography (think, for example, of the distinction between city-centre vs. out-of-town shops) or distances in the space of product characteristics. The latter is the more general interpretation, and considers a consumer's location to indicate their preferred product type. The closer a firm is to a given consumer's location, the smaller the departure from their ideal product type that the consumer has to make when it purchases from the firm. Increasing competition by increasing the number of firms in the market is beneficial because it reduces the extent to which consumers have to depart from their ideal product characteristics when making a purchase.

Indeed, we capture the effect of enforced data sharing via Open Banking and related measures by associating them with a shift in the market structure from a single-firm monopoly to a two-firm duopoly. The distinction between these market structures in terms of total travel costs, to be understood in terms of the cumulative cost to consumers of having to purchase a product that departs from their ideal specifications, is illustrated in Figure 3 below.



(a) Monopoly (b) Duopoly

Figure 3: Total Travel Costs (shaded grey)

[6]See, respectively, the responses to the FCA's Call for Input at *https://www.fca.org.uk/news/news-stories/fca-publishes-feedback-call-input-open-finance* and the Spring 2021 Report of the Smart Data Working Group at *https://www.gov.uk/government/publications/smart-data-working-group-spring-2021-report*. Relatedly, the Centre for Data Ethics and Innovation (CDEI) has been considering the potential benefits of facilitating the more widespread sharing of anonymised public sector data, see CDEI (2020).

However, the effect of an increase in variety has to be balanced against potential costs arising from security and data sharing. Regardless of the number of firms that operate in the market, each firm faces a decision as to (i) how much to invest in order to protect consumer data from cyber-attacks, and (ii) whether or not to share data with a common third party. The precise assumptions regarding cybersecurity and data privacy parallel those in Lam and Seifert (2021a).

A first result concerns the choices a monopolist would make with respect to cybersecurity and data privacy. In this regard, we have:

> ***Result 4:*** *In the monopoly benchmark, the firm's cybersecurity and data sharing choices coincide with the social optimum.*

This differs notably from the conclusions drawn about the monopolistic data controller in Lam and Seifert (2021a), see above. The reason for this distinction is that, in the present model, the market is assumed to be saturated, in the sense that consumers view the product being sold as essential, so that every consumer will end up purchasing one unit of the product in equilibrium.[7] This differs from Lam and Seifert (2021a), where the firm's pricing decisions always lead to some consumers being excluded from the market. The reduction in demand that goes along with the firm's more aggressive pricing strategy was one important factor in explaining the market failures in Lam and Seifert (2021a), which is absent in this model.

We contrast this result with the cybersecurity and data privacy outcomes arising under competition. In that case, we have:

> ***Result 5:*** *In the competitive market setting, firms' cybersecurity investments:*
>
> *(i) coincide with the social optimum if firms' data sharing choices are symmetric (either both share or neither does), but*
>
> *(ii) diverge from the social optimum if firms' data sharing choices are asymmetric (only one firm shares).*

The reasons for which the firms' privately optimal choices depart from the socially optimal ones again relate to price and associated demand effects. In particular, when only one firm is sharing, the firms' freely chosen prices lead to an inefficiently large portion of demand being allocated to the firm that does not share. Thus, overall security investments are lower.[8]

[7] This is appropriate given the nature of the products (e.g. banking and utility services) that we consider here.
[8] In this model, we assume that firms are fully liable for cyber-damages.

It follows that a move to competition can introduce new cybersecurity and data privacy market failures that do not arise under monopoly. They do so when an asymmetric data sharing outcome is socially optimal, which occurs when neither firm sharing would excessively limit the benefits of data sharing, while both firms sharing would lead to an excessively high risk of cyber-attacks.

It is consequently vital that Open Banking and related initiatives are co-ordinated with suitable measures on the cybersecurity side. While advice about ensuring appropriate security under Open Banking has been provided,[9] and in keeping with the advice put forward in Part 5.1, a more prescriptive approach that more closely defines the security precautions that must accompany involvement in the Open Banking ecosystem may therefore be needed. Cybersecurity needs to be placed at the centre of data-driven initiatives to promote competition.

Finally, while Lam and Seifert (2021b) develop initial results concerning the interactions between cybersecurity, data privacy and competition, it also remains to study the extent to which these results can be applied to other sectors that face a distinct yet closely related set of regulations to Open Banking, such as energy and telecommunications in light of the Smart Data initiative.

5.3 *Open Questions*

This part has demonstrated the importance that regulatory interactions play in designing optimal cybersecurity policies. In Part 5.1, we show that market failures relating to security investment cannot be resolved in isolation of a firm's data sharing choices. In Part 5.2, we demonstrate that promoting a more competitive market structure in digital markets can introduce new market failures in relation to cybersecurity. Consequently, cybersecurity needs to be integral to any regulatory initiatives that seek to promote competition by enforced data sharing. These theoretical results support the feedback received from interviewees and workshop participants concerning the importance of regulatory interactions (I_{11}–I_{14}, W_8–W_{14}). They also go some way towards improving our understanding of the welfare-desirability of some of the regulatory instruments discussed in Part 3.

In combination with the open questions raised in Parts 2.4, 3.4 and 4.3, a number of important questions remain unanswered, however. We present an overview of several important open questions for economic research in Part 6 that follows.

[9] See *https://www.openbanking.org.uk/wp-content/uploads/2021/04/Participant-Guide-Information-Security-Operations.pdf*.

Part 6

Future Research Directions

This part ties together the open questions identified in the overview of existing UK legislation, our primary data analysis, the literature review and our theoretical analysis in order to identify several important directions for future research. The first set of open questions, discussed in Part 2.4, concerned the extent to which regulatory interactions are already accounted for in the UK framework of cybersecurity regulation. In this regard, our qualitative analysis in Part 3.3 confirms the importance of regulatory interactions in practice, while our theoretical results in Parts 5.1 and 5.2 suggest that (i) a more prescriptive approach to cybersecurity than that currently reflected in the UK GDPR may be needed in order to ensure that cybersecurity and data privacy are sufficiently co-ordinated, and (ii) any data-centred initiatives to promote competition similarly need to incorporate appropriate cybersecurity measures.

In terms of the open questions raised by our primary data analysis, see Part 3.4, our theoretical results provide some guidance as to the properties of alternative regulatory instruments that fall under the centralised approach. These results also address the principal open question emerging from our literature review, see Part 4.3, insofar as they consider analytically for the first time the question of regulatory interactions in evaluating the welfare-desirability of alternative cybersecurity policies. Important questions that remain to be explored include the following.

6.1 Welfare Properties of the Decentralised Approach

The majority of research into incentives and regulation in the area of cybersecurity has focused on measures falling under the centralised approach, see Table 2. It is equally important to consider the potential for penetration testing and data anonymisation to promote socially desirable cybersecurity outcomes.

One particular understudied issue in this regard concerns the incentives of hackers, who do not feature as strategic actors in most economic models, in which cyber-threats are instead captured in an exogenous probability of attack. While hacker motivations have been discussed elsewhere in the cybersecurity literature (e.g. Barber, 2001; Caldwell, 2011), these issues are understudied in economic research. Accurately accounting for the motivations and incentives of hackers is an important step towards a complete modelling of the cybersecurity ecosystem. The problem that ethical hackers may not receive adequate protection from legal systems is also raised in OECD (2021).

6.2 Behavioural Economics

A lack of awareness among individual consumers and employees about cyber-risks was highlighted as one of the most prominent weaknesses in the current regime of cybersecurity regulation. This issue is also integral to the theoretical modelling that we discuss in Part 5. In Lam and Seifert (2021a), for example, the tendency for the data controller to share data too frequently, thereby introducing an excessively high risk of follow-on attacks into the economy, was driven by the presence of non-savvy consumers in the market, who do not factor cyber-risks into their decision making.

While this reflects an important element of bounded rationality underlying consumer behaviour in digital markets, it would be very interesting to introduce a more explicit modelling of consumers' behavioural decision making into the analysis. This approach would more directly account for a variety of heuristics and rules of thumb that, beyond a lack of awareness, can skew consumers' decisions away from the full rationality benchmark. These issues have already been highlighted in related settings where consumers face complex decision problems,[1] but have so far not been extensively investigated from a behavioural economic perspective in the cybersecurity context. One important example of relevant work in this area is Lam and Lyons (2020), who explore the effect that GDPR-style opt-in regulation has on firm incentives to invest in both product quality and data security.

6.3 Interactions with Consumer Policy

As motivated in the Introduction, as well as posing challenges for data security and privacy, the extensive collection and usage of personal data can cause competition concerns. These

[1] For example, the first Occasional Paper published by the FCA concerned a range of behavioural biases that affect consumer decisions in financial markets. See Erta *et al.* (2013).

issues can potentially be worsened by weak consumer protection rules, under which consumers make poor choices. The recent Yale Tobin Center Report by Crawford *et al.* (2021) presents a list of features of online markets that differentiate them from offline environments, and discusses whether we need tighter consumer protection rules for online markets to function well. In particular, the report mentions the greater collection and use of personal data as a key feature, and recommends standardising ways of presenting privacy policies and options for consumer control. This relates to the discussion in Lam and Seifert (2021a) on awareness, disclosure and consumer mitigation. However, with each of these two papers having a separate focus (one on consumer policy, the other on cybersecurity), there is significant scope for future research to unite these separate strands by considering more fully the interactions between cybersecurity, data privacy and consumer policy.

6.4 International Co-operation

The issue of international co-operation was highlighted in the context of the opportunities discussed in Part 3.2 and is also mentioned in OECD (2021). While implementing appropriate cybersecurity policies is challenging in a national context, particularly in light of the important regulatory interactions we have highlighted throughout this report, the international nature of cyber-threats has not been touched on so far. This raises a number of issues in relation to the enforcement of cybersecurity laws, not least because these laws may not exert the desired deterrent effect on threats located outside of a country's jurisdiction.

Moreover, delays in pursuing cyber-criminals across national borders were highlighted as a threat by our interview participants. The difficulties in aligning data-related policies internationally have also been made clear by the legal challenges on privacy grounds to the EU-US Privacy Shield. While the harmonisation of regulations internationally has received widespread attention in connection with environmental, tax and banking regulation, among others, this question has not been studied from an economic perspective in the cybersecurity context. Doing so introduces new incentive considerations in relation to competing governments' objectives, as part of which the stringency of cybersecurity policies may be traded off against promoting the competitiveness of the economy and attracting inward investment.

6.5 Autonomous Systems & AI

The final open area of research that we highlight here relates to the opportunity for automation and AI technologies to play a greater role in cybersecurity regulation. The topic of AI has

been receiving growing interest from economists, for example in the context of algorithmic collusion (see, e.g., Calvano *et al.*, 2020). The potential for AI to play a more positive role in the context of cybersecurity regulation remains unexplored. Preliminary work around the ethical issues surrounding the introduction of AI technologies to cybersecurity regulation is contained in GCHQ (2021), which, in keeping with the feedback we received from interviewees, highlights that these solutions must take account of possible "[u]nintended negative consequences" (GCHQ, 2021, p.27) when AI is used as regulatory tool. The nature of these negative consequences and the impact of AI on relevant incentives remain to be explored.

Part 7

Conclusion

This report studies the optimal design of cybersecurity policies with a specific focus on the effect of regulatory interactions between cybersecurity, data privacy and competition. We demonstrate that the existing UK framework of digital security regulation does take interactions between cybersecurity and data privacy into account to some extent, as reflected in the "appropriateness" criterion underlying the UK GDPR and DPA 2018. This requires firms to implement security measures that are appropriate to the risk of their data sharing (data processing) activities. Competition is not directly reflected in cybersecurity regulations, highlighting the scope for closer integration between security and competition objectives.

The input gathered from interview and workshop participants supports the view that regulatory interactions matter. All interviews confirmed that cybersecurity and data privacy should be seen as interdependent, and a smaller number identified overlaps between security and competition. The policy recommendations gathered from these interviews and workshops concerned a wide range of regulatory instruments, but broadly supported a centralised approach to cybersecurity regulation.

In order to evaluate the desirability of alternative regulatory approaches, we reviewed the existing academic literature and technical reports in the area of cybersecurity regulation, and also presented the results of two original pieces of theoretical work. These results highlight the importance of regulatory interactions by demonstrating that unilateral regulations targeting cybersecurity can, in some cases, have unintended consequences if firms' data sharing decisions are left to be determined by market forces. Concerning the effect of competition, we show that data-driven measures to promote competition, such as Open Banking and Smart Data, can introduce new market failures in the area of cybersecurity.

These results suggest that the degree of policy co-ordination between cybersecurity and data privacy currently reflected in the UK system of regulations might need to be strength-

ened. Allowing firms to implement security measures that they deem appropriate in the face of market forces may not be sufficient. Instead, a more co-ordinated approach that more closely prescribes the security measures that must accompany specific types of data sharing is needed. On the competition side, our results highlight the need for cybersecurity considerations to be integral to any competition remedy that relies on enforced data sharing.

While our theoretical analysis is the first to account explicitly for the importance of regulatory interactions in the design of cybersecurity policies, many important questions remain unanswered in this area. These concern, for example, the precise way in which cybersecurity, data privacy and competition policies should be co-ordinated. Another important objective for research concerns the behavioural nature of consumers' decision-making, whose choices may be more likely to be governed by various heuristics and rules of thumb than by fully rational utility maximisation. While some aspects of this bounded rationality are reflected in our work, there are many more detailed questions to be addressed through the application of behavioural economic analysis to the study of optimal cybersecurity policies.

Bibliography

Acemoglu, D., Malekian, A. and Ozdaglar, A. (2016). Network Security and Contagion. *Journal of Economic Theory*, 166, 536–585.

Acquisti, A., Taylor, C. and Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, 54 (2), 442–492.

Argenziano, R. and Bonatti, A. (2021). Data Linkages and Privacy Regulation. *Working Paper*.

Arora, A., Telang, R. and Xu, H. (2008). Optimal Policy for Software Vulnerability Disclosure. *Management Science*, 54 (4), 642–656.

August, T. and Tunay, T. (2006). Network Software Security and User Incentives. *Management Science*, 52 (11), 1703–1720.

Barber, R. (2001). Hackers profiled — who are they and what are their motivations? *Computer Fraud & Security*, 2001, 14–17.

Belleflamme, P., Lam, W. M. W. and Vergote, W. (2020). Competitive Imperfect Price Discrimination and Market Power. *Marketing Science*, 39 (5), 849–1031.

— and Peitz, M. (2015). *Industrial Organization: Markets and Strategies*. Cambridge University Press, 2nd edn.

Bergemann, D. and Bonatti, A. (2019). Markets for Information: An Introduction. *Annual Review of Economics*, 11, 85–107.

Caldwell, T. (2011). Ethical hackers: putting on the white hat. *Network Security*, 2011 (7), 10–13.

Calvano, E., Calzolari, G., Denicolò, V. and Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. *American Economic Review*, 110 (10), 3267–97.

Calzolari, G. and Pavan, A. (2006). On the Optimality of Privacy in Sequential Contracting. *Journal of Economic Theory*, 130 (1), 168–204.

Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11 (3), 431–448.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9 (1), 70–104.

CDEI (2020). Addressing Trust in Public Sector Data Use. Independent Report. *https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing*.

Choi, J. P., Fershtman, C. and Gandal, N. (2010). Network Security: Vulnerability and Disclosure Policy. *The Journal of Industrial Economics*, 58 (4), 868–894.

Crawford, G., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P., Luca, M., Salz, T., Schnitzer, M., Scott Morton, F. M., Seim, K. and Sinkinson, M. (2021). Consumer Protection for Online Markets and Large Digital Platforms. *Yale Tobin Centre for Economic Policy, Policy Discussion Paper*, 1, *https://tobin.yale.edu/sites/default/files/pdfs/digital%20regulation%20papers/Digital%20Regulation%20Project%20-%20Consumer%20Protection%20-%20Discussion%20Paper%20No%201.pdf*.

DCMS (2016). Cyber security incentives & regulation review. *Policy paper*, *https://www.gov.uk/government/publications/cyber-security-regulation-and-incentives-review*.

DCMS (2020a). Analysis of the full costs of cyber security breaches. *Report*, *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf*.

DCMS (2020b). Cyber security incentives & regulation review: summary of responses to the call for evidence. *Policy paper*, *https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence*.

Deloitte (2020). Digital Consumer Trends 2020. Available in summary at *https://www2.deloitte.com/uk/en/pages/technology-media-and-telecommunications/articles/digital-consumer-trends-data-privacy.html*.

Department of Homeland Security (2018). Cyber Risk Economics Capability Gaps Research Strategy. *Report*, *https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf*.

DMA (2018). Data Privacy: What the Consumer Really Thinks. *https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf*.

Erta, K., Hunt, S., Iscenko, Z. and Brambley, W. (2013). Applying behavioural economics at the financial conduct authority. *FCA Occasional Paper*, 1.

Federal Bureau of Investigation (2020). Internet Crime Report 2020. *Internet Crime Complain Center*, *https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf*.

Federal Trade Commission (2014). Data Brokers: A Call for Transparency and Accountability. May, 2014.

Gal-Or, E., Gal-Or, R. and Nabita, P. (2018). The Role of User Privacy Concerns in Shaping Competition Among Platforms. *Information Systems Research*, 29 (3), 698–722.

— and Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16 (2), 186–208.

GCHQ (2021). Pioneering a New National Security: The Ethics of Artificial Intelligence. *Report*, *https://www.gchq.gov.uk/news/artificial-intelligence*.

Goldfarb, A. and Tucker, C. (2011a). Online Display Advertising: Targeting and Obtrusiveness. *Marketing Science*, 30 (3), 389–404.

— and — (2011b). Privacy Regulation and Online Advertising. *Management Science*, 57 (1), 57–71.

Gordon, L., Loeb, M. and Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, 34 (3), 567–594.

—, — and Zhou, L. (2011). The Impact of Information Security Breaches: has there been a downward shift in costs? *Journal of Computer Security*, 19, 33–56.

Gu, Y., Madio, L. and Reggiani, C. (2020). Data Brokers Co-opetition. *Working Paper*.

HM Government (2020). Funding boost to help healthcare suppliers improve cyber security. Press Release of September 10, 2020.

Ichihashi, S. (2020). Online Privacy and Information Disclosure by Consumers. *American Economic Review*, 110 (2), 569–95.

Jackson, M. and Zenou, Y. (2015). Games on Networks. In P. Young and S. Zamir (eds.), *Handbook of Game Theory with Economic Applications*, vol. 4, Elsevier, Amsterdam, pp. 91–157.

Jullien, B., Lefouili, Y. and Riordan, M. H. (2020). Privacy Protection, Security, and Consumer Retention. *Working Paper*.

Lam, W. M. W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy*, 37, 42–51.

— and Lyons, B. (2020). Does data protection legislation increase the quality of internet services? *Economics Letters*, 195, 109463.

— and Seifert, J. (2021a). Regulating Data Privacy and Cybersecurity. *Working Paper*.

— and — (2021b). Competition, Digital Security and Data Privacy. *Working Paper*.

Mann, C. L. (2015). Information Lost. In A. Goldfarb, S. M. Greenstein and C. E. Tucker (eds.), *Economic Analysis of the Digital Economy*, Chicago: NBER, pp. 309–351, *https://www.nber.org/system/files/chapters/c12990/c12990.pdf*.

McAfee (2020). The Hidden Costs of Cybercrime. *Report*, *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf*.

McKinsey & Company (2016). The Age of Analytics. Competing in a Data-Driven World. McKinsey Global Institute Report. *https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world*.

Montes, R., Sand-Zantman, W. and Valletti, T. (2019). The Value of Personal Information in Online Markets with Endogenous Privacy. *Management Science*, 65 (3), 955–1453.

Mussa, M. and Rosen, S. (1978). Monopoly and Product Quality. *Journal of Economic Theory*, 18, 301–317.

OECD (2021). Encouraging Vulnerability Treatment: Overview for Policy Makers. *OECD Digital Economy Papers*, 307, *https://www.oecd.org/sti/encouraging-vulnerability-treatment-0e2615ba-en.htm*.

Open Data Institute (2021). Economic Impact of Trust in Data Ecosystems. *Report*, *http://theodi.org/wp-content/uploads/2021/03/RPT_Trust-in-data-ecosystems-23.02.21-STC-final-report.pdf*.

RSM UK Consulting (2020). Impact of the GDPR on Cyber Security Outcomes: Final Report. *Communications Consumer Panel Research Report*, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf*.

Spanos, G. and Angelis, L. (2016). The Impact of Information Security Events to the Stock Market: A systematic literature review. *Computers & Security*, 58, 216–229.

Spence, M. (1975). Monopoly, Quality, and Regulation. *The Bell Journal of Economics*, 6 (2), 417–429.

Taylor, C. R. (2004). Consumer Privacy and the Market for Customer Information. *The RAND Journal of Economics*, 35 (4), 631–650.

Varian, H. (2004). System Reliability and Free Riding. In J. Camp and S. Lewis (eds.), *Economics of Information Security*, Dordrecht, The Netherlands: Kluwer, pp. 1–15.