horizon
DIGITAL ECONOMY RESEARCH

Response to DCMS Call for Evidence:

Cyber Security Incentives and Regulation

Submitted by Prof. Derek McAuley and Dr. Jiahong Chen of
Horizon Digital Economy Research Institute, University of Nottingham

20 December 2019

1. Horizon[1] is a Research Institute centred at The University of Nottingham and a Research Hub within the UKRI Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and principal investigator of the EPSRC-funded DADA (Defence Against Dark Artefacts) project,[3] addressing smart home IoT network security, and its acceptability and usability issues, and Co-Investigator of the UKRI-funded PETRAS National Centre of Excellence for IoT Systems Cybersecurity.[4] Dr. Chen is a Research Fellow of Horizon, currently working on the DADA project.

Consultation Questions:

1. To what extent do you agree that the barriers outlined ((1) inability; (2) complexity and insecurity of the digital environment; and (3) lack of a strong commercial rationale) are the main barriers to organisations undertaking effective cyber risk management? ***Single response (Strongly agree, slightly agree, neither agree or disagree, slightly disagree, strongly disagree)***

2. Slightly agree.

2. Are you aware of any other key barriers to effective cyber risk management that are not captured in the 3 barriers highlighted? ***Single response (Yes/No)***

3. No.

3. [If Yes at Q2] Please provide any evidence or examples you have of other key barriers to effective cyber risk management. ***Open response***

4. N/A.

4. What evidence do you have for how Government and/or industry could help address the following two barriers, in addition to the existing interventions outlined?

[1] http://www.horizon.ac.uk
[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[3] https://www.horizon.ac.uk/project/defence-against-dark-artefacts/
[4] https://www.petrashub.org/

a. Barrier 1 - Inability *Open response*

5. As elaborated below, the Government may mitigate the inability barrier by identifying the key actors in the ecosystem (paras 6, 7, 26), ensuring security by design and by default (para 9), and providing standardised information for stakeholders (para 15).

b. Barrier 2 - Complexity and insecurity of the digital environment *Open response*

6. We share the same observation that the interconnectivity and interdependency of organisations and their information systems have posed serious challenges to cyber risk management. While it is important to involve all stakeholders to enhance the general level of cybersecurity, the Government should also identify the key players in the ecosystem, who are better positioned and resourced – in both technical and financial terms – to put appropriate cybersecurity safeguards in place. Incentive and regulatory strategies should take these organisations into primary account.

7. An important consideration is the involved parties' position in the supply chain. Many of the connected devices used by individual consumers or SMEs, for example, are manufactured overseas and then branded and sold by vendors who have little control over the design of such products. Our research has also found many start-ups developing digital products or services rely on advice and support from innovation agencies, who may play an important role given their influence in the industry. Identifying the key players in specific sectors can help policymakers prioritise resources in addressing security issues in a complex economy.

5. How much of a barrier is a lack of commercial rationale to organisations managing their cyber risk effectively? Please answer for each of the organisation sizes below.

Single code/matrix (Not a barrier, Somewhat of a barrier, Moderate barrier, Severe barrier) / (Micro organisations (Less than 10 employees); small organisations (10-49 employees; medium organisations (50-249 employees); large organisations (250 or more employees))

8. Micro organisations (Less than 10 employees): Severe barrier

Small organisations (10-49 employees): Severe barrier

Medium organisations (50-249 employees): Moderate barrier

Large organisations (250 or more employees): Moderate barrier

6. [If moderate barrier/severe barrier for any organisation size] What are the reasons for a lack of strong commercial rationale for the following organisations to invest in cyber security? [organisation sizes selected at Q2] Please provide evidence to support your answer. *Open response*

9. Through our interviews with industry experts, we found that the main reason for a lack of incentive in investing in cybersecurity is the insufficient alignment between this objective and other priorities of SMEs. For many start-ups, it is their top priority to survive in the competitive market with lower costs or novel features of their products or services. Cybersecurity, whether as a reputational appeal or a compliance requirement, comes only as a secondary consideration. In the absence of a

specialised team of cybersecurity, micro and small organisations often need to count on the security of the products or services they use, as well as the default configurations of these assets. In this regard, SMEs are sometimes in a position as vulnerable as individual consumers. The Government's consultation on regulatory proposals on consumer IoT security[5] has already highlighted such aspects and they are equally applicable to smaller organisations.

10. However, it should be noted that the size of an organisation is not the only decisive factor when it comes to the degree of commercial rationale in taking cybersecurity initiatives. Apart from the organisation's position in the supply chain and the market structure of a particular sector as mentioned above, another important aspect is their business model. Some businesses handle sensitive information from their clients/customers and will have a much stronger reputational motivation to maintain a high level of cybersecurity. Others may provide regular products or services to customers, which may create sufficient incentives for them to ensure the product/service is secure but not necessarily their own operation of business (which remains an important part of the wider cybersecurity landscape). Moreover, some traders simply offer low-cost, one-off products or services to the market, which provides little incentive for implementing cybersecurity measures. An effective cybersecurity strategy will need to acknowledge the heterogeneity within and across sectors on those dimensions.

7. [If not a barrier/ somewhat of a barrier] What evidence do you have that there is a strong commercial rationale for the following organisations to invest in cyber security? [organisation sizes selected at Q2] Please provide evidence to support your answer. *Open response*

11. N/A.

8. In your experience, which of the following information is used by organisations to inform cyber security investment decisions? *Please select all that apply*

- **Threat level**
- **Vulnerabilities**
- **Impact or harm of cyber incidents**
- **Mitigation activities and associated costs**

12. No response.

9. [For those selected at Q8] In your experience, how is this information used by organisations to inform cyber security investment decisions? Please provide any evidence you have for how this information is used.

- **Threat level**
- **Vulnerabilities**
- **Impact or harm of cyber incidents**

[5] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

- **Mitigation activities and associated costs**

Open response

13. No response.

10. How much of a barrier do you think each of the below issues are to organisations managing their cyber risk effectively?

a. Businesses do not have or draw on the right information about the cyber threat or their own cyber risk posture

b. The direct and indirect impacts of a cyber attack are not fully recognised by the organisation

c. There is no agreed definition of effective risk management

Single code per option (Not a barrier, Somewhat of a barrier, Moderate barrier, Severe barrier)

14. Businesses do not have or draw on the right information about the cyber threat or their own cyber risk posture: Moderate barrier

The direct and indirect impacts of a cyber attack are not fully recognised by the organisation: Moderate barrier

There is no agreed definition of effective risk management: Severe barrier

11. What information would allow organisations to better make investment decisions in cyber security? Please provide evidence to support your answer. *Open response*

15. Currently, there is a lack of clear, easy-to-follow, free-to-access[6] and sector-specific guidelines on practical actions that smaller organisations can take to achieve a baseline level of cybersecurity. Providing such information will enable organisations to make informed decisions on how they better invest in cybersecurity.

12. What are the barriers preventing organisations from creating, collecting or accessing this information currently? Please provide evidence to support your answer. *Open response*

16. No response.

13. Is there evidence of anything in the market currently effectively addressing these information transparency barriers? *Single response (Yes/No/Don’t know)*

17. No response.

[6] ISO/IEC 27032:2012 (Information technology — Security techniques — Guidelines for cybersecurity), for example, is not a free standard.

14. [If yes] Please provide evidence of how the market is currently addressing these information transparency barriers? *Open response*

18. N/A.

15. What solutions do organisations currently have for assuring and standardising the information used in cyber risk management? Please include evidence or examples. *Open response*

19. It is not yet common among organisations, in particular for SMEs, to adopt guidelines, best practices, standards, or emergency plans to identify and address cybersecurity threats. In terms of technical solutions, a number of experts mentioned Darktrace,[7] a service claiming to use AI to detect and respond to cyber-threats.

16. Do you think that a solution for assuring and standardising the information used in cyber risk management is required? *Single response (Yes/No/Don't know)*

20. Yes.

17. [If yes] What types of information should be assured or standardised? *Please select all that apply*

a. What 'good' looks like and how effective businesses are at managing their cyber risk

b. The impact (costs) of a cyber incident

c. Threat identification

d. Other (please specify)

21. What 'good' looks like and how effective businesses are at managing their cyber risk; The impact (costs) of a cyber incident; Threat identification.

18. How can Government or industry create a solution(s) that provides this assured or standardised approach to defining and assessing the key information underpinning cyber risk management? Please include evidence or examples from other areas. *Open response*

22. No response.

19. What approaches could Government or industry take to make this information for cyber risk management more transparent, accessible and trusted? Please include evidence or examples. *Open response*

23. No response.

[7] https://www.darktrace.com/en/

20. What is required to ensure that, at a senior level, organisations take responsibility and accountability for effective cyber risk management? Please describe how this responsibility and accountability will stimulate action to manage cyber risk within an organisation. *Open response*

24. No response.

21. What more do you think Government and/or industry could do to help stimulate investment in effective cyber risk management? Please include any examples or evidence of how industry in other countries have helped to stimulate investment in effective cyber risk management. *Open response*

25. The lack of motivation to adopt best practices to maintain a high level of security applies to smaller organisations and individual consumers alike – both consuming connected products and digital services as end users. They should be encouraged, for instance, to purchase only safe products that meet minimum security standards, to update and patch software in time, and to stop using products and services that are no longer supported. This would require a feasible financial structure to support longitudinal maintenance of product security in both B2B and B2C contexts. The 'right to repair' legislation in the EU[8] may represent a sustainable model to create and strengthen such incentives.

26. The current NIS regulatory framework[9] targets only operators of essential services in regulated sectors and major digital service providers, many of whom are subject to incentive barriers less serious than SMEs. To increase the overall cybersecurity level, policymakers may consider introducing incentives or regulation, as well as providing standardised information, to entities not currently covered by the NIS framework. As a matter of priority, this may include identifying the key players in other critical sectors such as IoT hub providers.

22. Are you responding as an individual or on behalf of an organisation?

- **a. Individual**
- **b. Organisation**

27. Individual.

23. [if individual] Which one of the following statements best describes you?

- **a. Cyber Security professional**
- **b. Employer of cyber security professionals or consumer of services provided by a cyber security professional**
- **c. Professional in another sector**
- **d. Academic**
- **e. Student**

[8] https://www.bbc.co.uk/news/business-49884827

[9] Including the NIS Directive and the NIS Regulations 2018.

f. Interested in a career in cyber security

g. Interested member of the general public

h. Other Free text

28. Academic.

24. [if organisation] Which one of the following statements best describes your organisation?

a. Organisation that employs, contracts or uses cyber security professionals

b. Cyber security training provider and or certification/qualification provider

c. A cyber security professional body

d. Other form of cyber security professional organisation

e. An academic or educational institution

f. Organisation with an interest in cyber security

g. Non-cyber security specific professional body or trade organisation with an interest in cyber security

h. Other Free text

29. N/A.

25. [if organisation] Which one of the following best describes the sector of your organisation?

a. Agriculture, forestry & fishing

b. Production

c. Construction

d. Wholesale and retail; repair of motor vehicles

e. Transport & Storage (inc. postal)

f. Accommodation & food services

g. Information & communication

h. Finance & insurance

i. Property

j. Professional, scientific & technical

k. Business administration & support services

l. Public administration & defence

m. Education

n. Health

o. Arts, entertainment, recreation

p. Other services

30. N/A.

26. [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.

a. Under 10

b. 10–49

c. 50–249

d. 250–999

e. 1,000 or more

31. N/A.

27. [if organisation] What is the name of the organisation you are responding on behalf of? Free text

32. N/A.

28. Are you happy to be contacted to discuss your response and supporting evidence? [YES/NO]

33. Yes.

29. [if yes] Please provide a contact name and email address below.

34. Prof. Derek McAuley (derek.mcauley@nottingham.ac.uk) and Dr. Jiahong Chen (jiahong.chen@nottingham.ac.uk).