ICAEW
REPRESENTATION 131/19

CYBER SECURITY INCENTIVES AND REGULATION REVIEW 2020: CALL FOR EVIDENCE

Issued 19 December 2019

ICAEW welcomes the opportunity to comment on the Cyber Security Incentives and Regulation Review 2020: Call for Evidence published by Department for Digital, Culture, Media and Sport on 4 November 2019, a copy of which is available from this link.

Discussions with ICAEW members and stakeholders show that decisions about cyber security are largely driven by fear, regulatory or compliance requirements, client or customer demands or direct experience of having being breached.

Organisational standards remain central to improving approaches to cyber risk management. Having a clearer and more integrated and graduated approach to standards, especially where that is underpinned by the authority of the NCSC, would help businesses to push standards down supply chains.

However, in our view, the government should also focus on the simplest way to achieve its objectives. Most security breaches are still caused by failures to have basic security measures in place and if the government's priority is to stop these kinds of breaches, relying on an approach of risk management may overcomplicate the issue. Therefore, the government needs to be clear about exactly what it is trying to achieve and prioritise action accordingly.

Assurance can play an important role in building confidence around the information provided by companies and focus attention on good practices in cyber security. We recommend that DCMS works closely with the Brydon and Kingman review teams in BEIS to consider how cyber security fits with their recommendations on the wider future of audit.

This response of 19 December 2019 has been prepared by the ICAEW Tech Faculty. Recognised internationally for its thought leadership, the Faculty is responsible for ICAEW policy on issues relating to technology and the digital economy. The Faculty draws on expertise from the accountancy profession, the technology industry and other interested parties to respond to consultations from governments and international bodies.

ICAEW Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK
T +44 (0)20 7920 8100 **icaew.com**

ICAEW is a world-leading professional body established under a Royal Charter to serve the public interest. In pursuit of its vision of a world of strong economies, ICAEW works with governments, regulators and businesses and it leads, connects, supports and regulates more than 150,000 chartered accountant members in over 160 countries. ICAEW members work in all types of private and public organisations, including public practice firms, and are trained to provide clarity and rigour and apply the highest professional, technical and ethical standards.

KEY POINTS

1. Discussions with ICAEW members and stakeholders show that decisions about cyber security are largely driven by fear, regulatory or compliance requirements, client or customer demands or direct experience of having being breached. While larger organisations may have more sophisticated and mature approaches built around risk management, commercial drivers for investment in cyber are broadly acknowledged to be weak for most businesses, especially smaller ones.
2. The experience of the implementation of GDPR demonstrate that where significant penalties are put in place around cyber security, businesses are more likely to take action. Furthermore, highly regulated sectors such as Financial Services and Pharmaceutical tend to be better at cyber security. We believe that a full review of the impact of GDPR, as well as regulatory approaches in sectors such as Financial Services, should form the starting point for understanding where regulation has changed behaviour and where further intervention may be helpful, bearing in mind that any further regulatory actions should adhere to the principle of proportionality.
3. Organisational standards remain central to improving approaches to cyber risk management. There are many standards available, which creates a complex environment for organisations to navigate. When doing due diligence over suppliers, businesses may also create their own set of questions and requirements, where they feel existing standards are inadequate.
4. Having a clearer and more integrated and graduated approach to standards, underpinned by the authority of the NCSC, would help businesses to push standards down supply chains. This approach would identify appropriate standards based on features such as organisational size and sector. Currently, there is confusion and a lack of confidence about the appropriateness of different standards, which does not easily support effective market incentives. Therefore, this should be a high priority area for further government action.
5. However, in our view, the government should also focus on the simplest way to achieve its objectives. Most security breaches are still caused by failures to have basic security measures in place and if the government's priority is to stop these kinds of breaches, relying on an approach framed around risk management may overcomplicate the issue. Effective risk management has an important role to play in prioritising and focusing resources, but meaningful information in many of these areas is likely to remain difficult for the vast majority of organisations to access, ingest and use. Therefore, the government needs to be clear about exactly what it is trying to achieve and focus actions on the simplest ways to achieve that.
6. Assurance can play an important role in building confidence around the information provided by companies and focus attention on good practices in cyber security. In the UK context, it is important to position any new assurance services or requirements in the wider discussion about the future of statutory audit. Audit around cyber security is a clear example of the kind of non-financial audit that would be strengthened under proposed changes to the sector.
7. As a result, we recommend that DCMS works closely with the Brydon and Kingman review teams in BEIS to consider how cyber security fits with their recommendations on the wider future of audit. This should include consideration of the possibility of a requirement around internal controls, similar in objectives to Sarbanes-Oxley, although designed for the UK market-place. This would incorporate some elements of cyber security and IT controls and care needs to be taken so that businesses do not end up with a patchwork of requirements from different contexts that are not easily integrated.

ANSWERS TO SPECIFIC QUESTIONS

Question 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? (Strongly agree, slightly agree, neither agree or disagree, slightly disagree, strongly disagree)

8. Strongly agree

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

9. No

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

10. No comment

Question 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? a. Barrier 1 – Inability; b. Barrier 2 - Complexity and insecurity of the digital environment.

11. In terms of **inability**, many organisations still find it very difficult to shift cyber security from being an IT issue into being a wider business risk which is the responsibility of all in the organisation. This was one of the key issues identified in ICAEW's Audit Insights: Cyber Security series ('Businesses should consider cyber in everything that they do') and links to the difficulties in making good risk management decisions.
12. Skills gaps, role profiles and reporting lines are some of the key issues in this area. While many organisations have recruited Chief Information Security Officers (CISOs), they are often insufficiently senior, have too much of a technical focus and continue to report into IT functions rather than risk functions or the board directly. This latter point is important because there are often tensions between IT functions (who are motivated to deliver high quality user experience and business innovations) and security. Having separate reporting lines is a key part of managing that tension and ensuring that the business can make appropriate decisions which balance risk with functionality and innovation.
13. However, many businesses do not have enough knowledge about cyber to define the right role for their organisation and focus on the specific skills that they need. Clearer guidance or advice in this area could help businesses define an appropriate role, recruit a person with the right skills and set up robust reporting lines and governance. In addition, smaller businesses in particular, who do not have any cyber security skills inhouse, would benefit from clearer certifications or accreditations around cyber security capabilities.
14. There are also opportunities to 'mainstream' cyber security guidance and training into other areas of government support and interaction with business. This could range from including cyber security information in communications to businesses about Making Tax Digital, to working with incubators and accelerators across provide relevant training and support to start-ups and scale-ups.
15. In terms of **complexity**, cloud security continues to be a significant concern and we receive many questions from ICAEW members about how they make good decisions about the risks of cloud suppliers. Further government focus and support in this area would be very welcome.

16. Furthermore, supply chain management, and managing the risks of third-party suppliers throughout business operations, is a major pain point for many larger businesses. Cyber security is frequently considered in the procurement process, and a lot of time can be spent on bespoke requirements and questionnaires for clients and customers. Further work on standards, especially at the more advanced level, could help to streamline this process.

Question 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. (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))

17. Micro, small and medium organisations – severe; large organisations – moderate barrier. We note that defining a large organisation as 250 or more employees covers a wide range of organisations.

Question 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? Please provide evidence to support your answer.

18. Discussions with ICAEW members and stakeholders show that decisions about cyber security are largely driven by:
    - Fear
    - Experience of having a cyber-attack or breach
    - Regulatory oversight or compliance requirements
    - Demands of clients or customers
19. While larger organisations may have more sophisticated and mature approaches built around risk management, commercial drivers for investment in cyber are broadly acknowledged to be weak for most businesses, especially smaller ones.
20. Lack of direct consequence for many security breaches, or insufficient information about the devasting impact that cyber breaches can have, is a significant barrier in many case and where significant penalties are put in place around cyber security, businesses are more likely to take action.
21. The implementation of GDPR, for example, has significantly increased board focus on cyber and data protection. We are still in the early days of implementation, with the impact of fines, for example, still to be fully understood. However the evidence to date suggests a broad increase in basic standards, based on the findings of the 2019 Cyber Breach survey, comments from the ICO and anecdotal evidence. Furthermore, highly regulated sectors such as Financial Services and Pharmaceuticals tend to be better at cyber security. We believe that a full review of the impact of GDPR, as well as regulator approaches in sectors such as Financial Services, should form the starting point for understanding where regulation has changed behaviour and where further intervention may be helpful, bearing in mind that any further regulatory actions should adhere to the principle of proportionality.
22. We also note the requirement from many parts of government that bidders for contracts comply with Cyber Essentials. This has been an effective driver to change and we believe that there is more scope for all publicly funded agencies to be consistently requiring cyber security accreditations in their procurement processes.

Question 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? Please provide evidence to support your answer.

23. No comment

Question 8. In your experience, which of the following information is used by organisations to inform cyber security investment decisions? Please select all that apply. a. Threat level; b. Vulnerabilities; c. Impact or harm of cyber incidents; d. Mitigation activities and associated costs

24. All to some degree

Question 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. a Threat level; b. Vulnerabilities; c. Impact or harm of cyber incidents; d. Mitigation activities and associated costs

25. A sophisticated risk management approach would consider all of these types of information. However, in practice, this is limited to the most mature organisations.

Question 10. How much of a barrier do you think each of the below issues are to organisations in managing their cyber risk effectively? a. Businesses do not have access to 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 (Not a barrier, Somewhat of a barrier, Moderate barrier, Severe barrier)

26. All are severe barriers

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

27. All of the types of information listed would help business make better cyber risk decisions by improving understanding the likelihood and impact of breaches. This would enable organisations to make rational choices about where to invest resources, and to prioritise their spending on cyber based on their specific risk appetite. There are also potential opportunities to make comparisons of their position with regard to industry peers.
28. However, in our view, the government should focus on the simplest way to achieve its objectives. Effective risk management has an important role to play in prioritising and focusing resources, but meaningful information in many of these areas is likely to remain difficult for the vast majority of organisations to access, ingest and use. While large organisations with sophisticated capabilities may be able to improve their risk modelling through better data, focusing entirely on risk management may not be able to deliver the government's objectives.
29. Most security breaches are still caused by failures to have basic security measures in place and if the government's priority is to stop these kinds of breaches, relying purely on an approach framed around risk management may overcomplicate the issue. Alternative approaches which focus on getting all businesses to implement basic cyber hygiene measures, to the point of mandating some type of compliance with them, is likely to be a simpler way of achieving that objective, albeit one that would require significant resources across all businesses.
30. Risk management can also have an effect of complicating discussions and relying on models which only experts can understand. Experience of ICAEW members shows that often the best way of persuading boards to invest in security is to provide relatable stories that show the impact of failures and make it real and relevant to them. Relying on data and complex models is unlikely to help in this regard.

31. Finally, the government needs to be careful not to assume that better risk management will inevitably result in better security. A business could make a rational choice, based on a high risk appetite, not to invest in particular security measures. Therefore, the government needs to be clear exactly what it is trying to achieve and prioritise action accordingly. Underpinning this is should be a clear articulation of why government action is needed and why cyber security is so important that it cannot be left to individual businesses to suffer the consequences of poor security practices

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

32. Threat intelligence information is available from various sources, including commercial providers and the NCSC. However, to be useful, such information needs to be timely, relevant and actionable. In many cases, any information sharing happens too late to be used to prevent incidents, or the information is not specific enough to enable actions by organisations. Furthermore, organisations need to have the capability to ingest and interpret such intelligence, limiting practical usefulness to the largest companies.
33. Information about the impact of breaches is likely to be commercially sensitive and organisations are generally unwilling to share such information. The annual Cyber Breaches Survey endeavours to provide data on this, but with a relatively small sample, and a wide range of experience, this part of the survey is problematic. Furthermore, many organisations may not realise that they have been breached, or recognise its full impact, limiting the usefulness of relying on self-reporting in this context.
34. The breach notification process under GDPR should provide more data on breaches. However, this continues to represent only a subset of breaches (regarding personal data) and we are still in the early stages of its operation. We suggest that the government works closely with the ICO to maximise the potential usefulness of breach data to wider cyber security decision-making, for example ensuring as much consistency as possible.

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

35. Yes

Question 14. [If Yes] Please provide evidence of how the market is currently addressing these information transparency barriers.

36. There are industry-driven forums which focus on information sharing, especially in financial services.
37. We also note the growth of cyber rating agencies, which use publicly available information to rate companies in their cyber security practices. They are generally US-focused, perhaps reflecting a longer history of breach reporting for example. They do show, though, that there is potential market demand for such ratings information, albeit they currently rely on limited information.

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

38. There are many standards and certifications available around cyber security and cyber risk management which are used by organisations. The appropriate solution depends on the size and scope of the business. These include:
    - Cyber Essentials

- IASME Audited Governance Standard
- ISO 27001
- PCI DSS

39. Some elements of cyber security are included in the statutory audit in the UK, and therefore build on IT audit methodologies such as COBIT. However, this is limited to the controls around financial reporting and does not cover wider aspects of cyber security and cyber risk management.
40. For larger companies in particular, US standards can be relevant, in particular the NIST framework and the assurance standards ISAE 3402 or SSAE 18, which are used when looking for assurance over the cyber security of service providers (known as a SOC 2 audit).

Question 16. Do you think that additional solutions for assuring and standardising the information used in cyber risk management is required? (Yes/No/Don't know)

41. Yes

Question 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)

42. Any of these could be assured, depending on the needs of the users

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

43. Assurance can play an important role in building confidence around the information provided by companies and focus attention on good practices in cyber security. Further information about the role and operation of non-financial assurance can be found here
44. In the UK context, it is important to position any new assurance services or requirements in the wider discussion about the future of financial statement audit. Audit around cyber security is a clear example of the kind of non-financial audit that would be strengthened under proposed changes to the sector. Creating new separate audit products of this kind, distinct from the statutory financial statement audit, may enable new providers to grow and increase capacity in the UK market for cyber-related audit and assurance. ICAEW would look to work with regulators, member firms and other stakeholders to develop an appropriate approach and standard for such engagements.
45. Whether such assurance should be mandated in some way is a separate question. The government should consult widely with stakeholders such as investors to gauge the appetite for commissioning such assurance, as well as consider the proportionality of requiring businesses to gain assurance over cyber risk management. Furthermore, the implementation period would need to take account of the current skills and capabilities available in the UK marketplace in this area.
46. As a result, we recommend that DCMS works closely with the Brydon and Kingman review teams in BEIS to consider how cyber security fits with their recommendations on the wider future of audit. This should include consideration of the possibility of a requirement around internal controls, similar in objectives to Sarbanes-Oxley, although designed for the UK market-place. This would incorporate some elements of cyber security and IT controls and care needs to be taken so that businesses do not end up with a patchwork of requirements from different contexts that are not easily integrated.

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

47. Organisational standards remain central to improving approaches to cyber risk management. There are many standards available, which creates a complex environment for organisations to navigate. When doing due diligence over suppliers, businesses may also create their own set of questions and requirements, where they feel existing standards are inadequate.
48. Having a clearer and more integrated approach to standards, especially where that is underpinned by the authority of the NCSC, would help businesses to push standards down supply chains. Currently, there is confusion and a lack of confidence about the appropriateness of different standards, which does not easily support effective market incentives. Therefore, this should be a high priority area for further government action.
49. This approach would reflect a graduated scheme of standards, which starts at a basic level of security, such as Cyber Essentials, and moves into more sophisticated risk management practices. It would identify appropriate standards based on features such as organisational size and sector. While a perfectly integrated solution in this area is unlikely to exist, a further review of how standards sit together would be valuable and would identify whether any further standards, especially at the high end, are needed.
50. The operation of the PCI DSS standard also shows how positive, publicly available assurance models can work effectively. This approach sets clear expectations for controls, delineates between organisations based on size and activity (risk), has clear financial and operational implications in the event of breaches, requires external assurance and publishes the achievement of compliance.
51. Another useful support would be suggested metrics for boards around cyber security. The work done by the NCSC on the board toolkit has been recognised as valuable and further work to provide a list of potential business-orientated metrics would be helpful. Board reporting is often cited as an area of poor practice, typically exacerbated by the technical focus of CISOs, and better reporting would improve the ability of boards to understand the business risks.

Question 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.

52. Lack of board engagement and accountability for cyber security is a well-known challenge for businesses of all sizes, as repeatedly highlighted in our Audit insights research. Some boards have improved their knowledge, but this remains a weakness in many businesses.
53. As highlighted earlier, recommendations of good practice in reporting lines for security could help, along with role descriptions for CISO. The definition of the Data Protection Officer in GDPR could provide useful lessons in this regard.
54. The government could consider specifying cyber security responsibility for directors, and this would undoubtably drive greater board focus on the issue. However, the government would need to be clear as to why cyber security merited such treatment, given all the other responsibilities that boards have.
55. Furthermore, while regulation is likely to drive behaviour change, businesses that are leading in their cyber security practices recognise the value in being good at cyber security and build a culture on that basis. Turning cyber security into a compliance activity runs the

risk of making it a tickbox exercise that consumes significant resources but does not necessarily improve security in practice.

Question 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.

56. Cyber insurance is a further option that is consistently discussed but has yet to achieve its potential in this regard. Cyber insurance, which is backed up by clear standards that policy holders need to abide by, should help to drive up good practices, and we note that this was an original intention of Cyber Essentials.
57. To date, cyber insurance has had limited appeal and insurance companies appear to have continuing difficulties with data, which makes pricing premiums difficult. Furthermore, most policies do not specify good practices to be followed and generally focus on the recovery activities around cyber breaches, rather than wider business disruption, for example. As a result, there is scepticism about how useful policies may be in practice and significant further work is required to deliver an effective market in this area.
58. The success of the CBest approach is also noted in driving improvements in cyber security and improving the practical resilience of organisations in financial services. This approach has the advantage of providing hard evidence to an organisation of how they have been breached, and specific actions that they can take to improve their defences and resilience. The role of regulator has focused board attention on the tests, and while they involve significant work, the approach has been copied in other sectors, especially across the public sector. A review of the lessons from this kind of approach, based on intelligence-based penetration testing, may have wider applicability for larger companies.
59. Finally, we suggest that government itself takes more of a lead in this area, visibly raising standards across all areas of government. While there are pockets of good practices, more can be done to show leadership. For example, we highlighted earlier the opportunity to push cyber security standards further into all areas of public procurement, and there are other opportunities to demonstrate good practices and develop benchmarking of cyber practices across government departments.