ICAEW
REPRESENTATION 30/19

NATIONAL CYBER SECURITY SKILLS STRATEGY

Issued 1 March 2019

ICAEW welcomes the opportunity to comment on the National Cyber Security Skills Strategy published by Department for Digital, Culture, Media and Sport on 21 December 2018, a copy of which is available from this link.

1. ICAEW has worked closely with the National Cyber Security Centre to improve the skills and capabilities of chartered accountants with regard to cyber security, and welcomes the continuing focus on improving cyber skills. In particular, we strongly agree that cyber security needs to be seen as a responsibility of all, not just the technical experts, and therefore raising awareness and improving skills across all levels of the workforce is a critical task.
2. Businesses of all sizes have access to lots of excellent guidance and good practice resources which can help them increase their understanding, skills and capabilities in cyber security. However, meaningful change continues to be slow in many cases. While there are many reasons for that, we believe that further review of the economic and regulatory incentives around cyber security is needed if a step change in broad capabilities is to be achieved.
3. Achieving good cyber security is a core part of being a chartered accountant. For ICAEW, cyber is reflected in the ACA qualification, member support, the code of ethics, and the review of regulated firms. We would be pleased to work with government and other professional bodies to share experience and work to further improve cyber capabilities in the profession.

This response of 1 March 2019 has been prepared by the ICAEW IT 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 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

4. ICAEW has worked closely with the National Cyber Security Centre to improve the skills and capabilities of chartered accountants with regard to cyber security, and welcomes the continuing focus on improving cyber skills. In particular, we strongly agree that cyber security needs to be seen as a responsibility of all, not just the technical experts, and therefore raising awareness and improving skills across all levels of the workforce is a critical task.
5. Businesses of all sizes have access to lots of excellent guidance and good practice resources which can help them increase their understanding, skills and capabilities in cyber security. However, meaningful change continues to be slow in many cases. While there are many reasons for that, we believe that further review of the economic and regulatory incentives around cyber security is needed if a step change in broad capabilities is to be achieved.
6. Achieving good cyber security is a core part of being a chartered accountant. For ICAEW, cyber is reflected in the ACA qualification, member support, the code of ethics, and the review of regulated firms. We would be pleased to work with government and other professional bodies to share experience and work to further improve cyber capabilities in the profession.

ANSWERS TO SPECIFIC QUESTIONS

Questions 1 - 10

7. No comment

Question 11 – are there any specific initiatives that you think government and industry should focus on in order to increase the cyber security capability across the general workforce?

8. The National Cyber Security Centre has published lots of good material which can help to improve businesses awareness, understanding and capabilities around cyber security. However, our perception is that awareness of these resources continues to be low. The government needs to engage in far higher levels of publicity and awareness raising on an ongoing basis, especially amongst small businesses, if these initiative are to have any real impact and significantly increase capabilities. This could include;
    a. Mass media campaigns on a regular basis: while there are occasional campaigns, such as through Cyber Aware, far more is needed to keep cyber front of mind for smaller businesses.
    b. More joined up approaches across government, including reference to cyber security resources or issues in communications to small businesses from HMRC, or other government agencies. Making Tax Digital, for example, is a good opportunity to embed cyber security advice in broader government messaging and advice.
9. The ICAEW series **Audit Insights: Cyber security** has tracked the engagement of boards in cyber security issues and notes general improvements in awareness and board capabilities in this area. However, we agree with the government that there are still significant gaps, especially between boards and senior cyber security leaders. Many boards have undertaken cyber training, increased their briefings on the topic and found ways to increase access to expert knowledge, such as through Cyber Expert Advisory Groups, use of external

consultants or recruiting specialists onto the board. These mechanisms can continue to improve board knowledge, and success stories/learnings should be shared where possible.

10. However, the communication gap continues to exist in most cases, and our work highlighted a particular lack of strategic and business focused security specialists who can operate at senior levels. This hinders meaningful discussion and decision-making at board level and finding ways to bridge this gap should be a high priority. This could be through encouraging mentoring or fast-tracking of talented individuals, for example, or helping to bring across experienced professionals from other fields and equipping them to take a CISO role.
11. Embedding consideration of cyber risk into all business decision making is also a critical point, and our Audit Insights reports have highlighted many different steps that businesses can take to support this shift – for example adopting a cyber-by-design approach, closely reviewing the cyber security practices of companies being acquired or invested in, linking cyber risks to strategic change or initiatives and embedding responsibility for cyber security alongside day-to-day operational responsibility.
12. However, change has been slow in practice and we see significant differences in maturity levels across the business landscape, as well as continuing failures to get basic security right.
13. It is notable that the greatest increase in awareness and accessing resources about cyber over the last few years has been driven by GDPR. This suggests two things:
    a. The NCSC should continue to work closely with the ICO, and other relevant bodies, to embed help, awareness and training about cyber security into GDPR-related activities.
    b. Current market-driven approaches alone are unlikely to drive the kind of step-change in skills and capabilities that government appears to want. We recognise that the government has undertaken a number of reviews around the incentives for good cyber security, and there is a careful balance to be struck. However, current approaches do not appear to be driving significant changes in behaviour and the Government should consider whether some form of tax break, mandation (for example around Cyber Essentials), or other incentive should be applied to drive further and quicker change.

Question 12 – We propose working with other professions and disciplines to embed cyber security in codes of conduct and codes of ethics and to ensure cyber security is adequately reflected in the implementation of new technologies. Which of the following sectors should the government prioritise?

14. Good cyber security is a core part of being a chartered accountant. ICAEW includes cyber security in a number of key areas:
    a. The ACA qualification has been updated in recent years to include more content on technology in general and cyber security specifically. This is built into existing accountancy modules, rather than creating separate qualifications, which supports the idea of embedding awareness of cyber risks in everything that chartered accountants do, rather than treating it as a distinct, technical topic.
    b. The accountancy Code of Ethics has ‘confidentiality’ as a core ethical principle. When we speak about cyber security, therefore we can place it in the context of confidentiality and the ethical obligations of accountants to maintain client confidentiality.
    c. Quality reviews of accountancy firms undertaken by ICAEW include reviews of cyber security practices.
15. ICAEW would be pleased to work with the government and other professional bodies to share experience in these areas and work to improve further cyber security across the profession.