UKSA Response to Cyber Security Incentives and Regulation Review 2020:
Call for Evidence, 4 November 2019

This is a response from UKSA, the UK Shareholders' Association (www.uks.org.uk), representing the interests of private shareholders. In addition to our own members, there are 5 million people who own shares and have investment accounts with platforms in the UK. The Office for National Statistics estimates that individual investors own 12% of the UK stock market by value. In addition to this there are many more who have money invested in shares via funds, pensions and savings products such as employee share ownership schemes.

KEY POINTS

Information Technology (IT), including cyber, is changing constantly so that no one person can understand it all. Every nut and bolt, every line of software, the speed of innovation makes even small IT systems part of an inter-dependent infrastructure of industrial scale proportions.

This has led to many services being provided by 3rd parties throughout the supply chain, making the supply chain more complex. We describe it as the 'services and supply chain'.

Shareholders expect the boards of the companies to be cognisant of their business. Today, businesses have at least two 'business lines', their core business and the IT that underpins everything the organisation does.

Business leaders are expected to make sound judgements relevant to all business lines yet appear unwilling to gain sufficient IT understanding commensurate with their business competences (see https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is). Until our business leaders gain appropriate IT proficiency, the likelihood of their making wise cyber-security investments will remain low.

There is significant knowledge asymmetry between business leaders who know the business and the experts who know IT. The larger the knowledge gap, the greater the risk of poor decision-making, implementation and crisis resolution.

This manifests itself, from a board perspective, into overlooking the need for a robust commercial cyber security rationale. We need a different approach, such as instilling 'social responsibility' in business leaders towards their customers, clients, shareholders and beneficiaries, aligned to Section 172 requirements in the 2006 Companies Act.

We believe the starting point should be an expectation that Boards obtain relevant training to help them understand the causes and effects their technology has on the supply chain, why the likelihood of a cyber breach is considered 'when', not 'if' (see https://a-lign.com/responding-to-and-preparing-for-a-data-breach/ and https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin), and that they, like the NHS experiencing the WannaCry malware attack, may be the victims of collateral damage (see https://www.telegraph.co.uk/men/the-filter/one-year-wannacry-attack-vulnerable-ever/).

That requires boards to adopt a wider strategic outlook, placing cyber security, cyber breach recovery and business continuity at the heart of their strategy for managing the services and supply chain.

And key to maintaining a technically literate board is to have additional board roles and positions with the same status as a Chief Financial Officer. We believe that all significant companies should have a Chief Information Technology Officer capable of covering the location, usability, security and management of the hardware, software and information.

TECHNICAL RESPONSES

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 nor disagree, slightly disagree, strongly disagree)	Strongly 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)	Yes.
3. [If Yes at Q2] Please provide any evidence or examples you have of other key barriers to effective cyber risk management. Open response	Another key barrier is the industrial scale nature of technology. To get anywhere close to providing a commercial rationale, Business needs to grasp that technology is a vast array of different components and software existing within and beyond the organisation. Organisations must recognise that they have a minimum of two lines of business, their 'product and services' arm and their 'technology arm' that integrates strategic objectives with operational delivery. This requires change to how business and operational strategies are defined, resourced and managed. It means thinking beyond traditional corporate boundaries to include 3rd party technical services providers as part of an interconnected services and supply chain. It means recognising that IT's industrial scale gives people plenty of places to hide. Social media is a great example of how the 'trolls' can bully victims via the internet without revealing their identity. This is exacerbated by the combination of big data, artificial intelligence, machine learning and the internet of things that allow computers to run autonomously.

	Business must recognise their judgements are made based on advice from not only their own IT staff but by 3rd party vendors specialising in operational tools to aid and secure business. In most cases, boards are disadvantaged, having to take decisions from a position of ignorance. There is clear knowledge asymmetry between business leaders who know the business and the experts, who know IT. The larger the gap between the two sides, the greater the risk of poor decision-making, implementation and crisis resolution. Boards are, in effect, delegating operational responsibility to IT, not business, professionals. 3rd parties have their 3rd parties, too, so there is the extra complexity of sub-outsourcing to consider, too, when reviewing cyber security. The combination of technology's industrial scale, poor understanding by business leaders, computer automation and the ability to work anonymously enables hackers to work at an industrial scale too. Finding just one weakness to exploit will give them an excellent return for their efforts. Industrial scale size enables hackers of all persuasions to participate: scrip kiddies honing their skills; disgruntled staff or social and political activists to make their point; criminal gangs of global proportions; and nation states for IP and political espionage. Boards require a mindset of 'zero trust' as hackers can be anyone or any computer, from anywhere at any time. There are 9 billion potential hackers, based on our estimates: 7 billion people (2019 stats, see https://www.worldometers.info/world-population/), plus 2 billion independent, inter-connected computers (2014 stats, see https://www.reference.com/technology/many-computers-world-e2e980daa5e128d0).
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 Open response b. Barrier 2 - Complexity and insecurity of the digital environment Open response	In our interaction with many companies we note that cyber security is not mentioned. There is neither sufficient interest nor understanding between business leaders and shareholders. In conversation with experienced independent Non-Executive Directors, we have the following suggestions that would help both boards and investors. Overcoming Barrier 1: • Have a business and tech-savvy person on the board to enable a proper board discussion that goes beyond responding to an IT outage. • Sector/industry-related IT/Cyber security requirements. • A new way of looking at business continuity. It is now the start point, not the afterthought for continuing successfully after an incident.

	Overcoming Barrier 2: • A common risk language to reduce confusion over what is meant by a risk, a vulnerability and a threat. • Requiring an IT/Cyber security audit as part of mandatory reporting. It is time for Boards to provide executive and non-executive board positions to IT professionals expert in business-orientated technology and control. For executive positions, it could be the Chief Technology Officer (CTO) covering hardware and software, and the Chief Information Security Officer (CISO) focusing on data security. These two roles, co-existing in many companies, have to be represented or combined, for board purposes, into a Chief Information Technology Officer. This position is as necessary as the Chief Financial Officer is to financial matters, to ensure the depth of complexity is brought to the Board's attention. For non-executive positions, it should be someone with a broad range of understanding on IT and business governance, risk, security and control to ensure the breadth of discussion.
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))	Severe in all cases
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	We have answered 'severe' to Q5 because just one security weakness across the supply and service chain can cause damage and disruption. In our view, questions 5 and 6 are understandable but somewhat pointless questions. Business size is not the key issue. Its management quality, purpose, sector and industry are, as is technology's industrial scale referred to in Q3. Some organisations are highly regulated, driving to a great extent what is included within a 'commercial rationale'. And the disruption is not always caused by a cyber breach.

	Operational disruption can be just equally devasting, as in the case of TSB. Slaughter and May's report demonstrates that the business leaders did not understanding the significance of what they were signing-off on. See https://www.tsb.co.uk/news-releases/slaughter-and-may/. The key issue is understanding who is hurt by an attack? With the cyber and technical issues experienced by BA, Talk Talk and TSB, it was the customers/clients and shareholders/owners, who bore the brunt of the disruption and the financial cost of recovery. The BA woes (see https://threatpost.com/british-airways-e-ticketing-flaw-exposes-passenger-flight-personal-data/147260/) of stolen payment details (Sept 2018) and e-ticketing flaws exposing customer data (Aug 2019) has not stopped the company surviving in spite of, of perhaps because of, a key part to the recovery being down to customers changing payment methods and being alert to misuses of their data. We suggest that business leaders ask themselves, as part of their strategic and risk discussions, how long they expect their organisation to survive in the world of cyber, and how they will execute their duty under Section 172 of the Companies Act 2006 to ensure the fulfilment of their obligations to the company's members and wider stakeholders (see https://www.ardeainternational.com/the-new-section-172-what-do-directors-need-to-know/. However severe, Business survives cyber breaches surprisingly well. Maybe this is because it has become a daily occurrence (see https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-october-2019) so the incentive to secure and control cyber well diminishes. Or maybe there are too many vested interests to protect market share and personal reputations so that neither the severity nor the financial costs are fully publicised. Actual costs of cyber-crime are hard to find, again making a commercial rationale harder to define. There are plenty of estimates. In 2011, the UK put it at £27billion[i]. More recently, TechUK has carried out a more granular cost estimate across different type of cyber-crime (see https://www.techuk.org/images/understanding-costs-of-cyber-crime-horr96.pdf, showing that the criminal market is a diverse market place and that there is also a huge 'soft cost' borne by the victims of crime. Our analysis suggests that, from a board perspective, a commercial cyber security rationale is less important than it might seem, suggesting a different approach is needed. One is to is to instil a 'social responsibility' in business leaders towards

	its customers, clients, shareholders and beneficiaries. Another is ensuring there is a viable 'after the breach' response plan covering moral and legal liability, insurance, damage limitation and recovery, and personal liability.
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	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	We believe it is the impact or harm of cyber incidents, and mitigation activities and associated costs.
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 ● Mitigation activities and associated costs Open response	Questions 8 and 9 are difficult to address because the 4 categories are inter-related. It also depends on whom in the organisation we are talking about. Our answer to Q8 is based on our knowledge of what a non-cyber savvy board would focus on. They are related to crisis management responses, typically a key role for the board. Concentrating on them first: • *Impact or harm of cyber incidents:* a good risk and control investment should be commensurate with the level of damage that can be inflicted on assets, key processes and stakeholders. This is normal and has nothing to do with cyber per se. Whether assets and processes are physical, mechanical, automated or cyber, they need protection. With cyber security, we are talking about a 'social responsibility' mentioned towards the end of our response to Q6, succinctly articulated in a Carnegie blog (see https://www.carnegieuktrust.org.uk/blog/reducing-harm-social-media-duty-care/). The key point is that "by making companies invest in safety the market works better as the company bears the full costs of its actions, rather than

	getting an implicit subsidy when society bears the costs." The difficulty comes in knowing – in fact it is probably going to be guessing – when, whatever it is, will cause the impact or harm. Noticing the impacts might come days, if not months, after a successful breach, and the impacts experienced may be only part of the actual harm intended. Swift, and recoverable action, the stalwart of business continuity and crisis management responses, is not applicable in the same way. The paradox is the need for an immediate response to something that occurred unknowingly in the past, based on currently available information, but needing to also predict additional harms. A complex dance of ex ante/ex post information, action and reaction. • *Mitigation activities and associated costs:* this is where traditional experience of business continuity and crisis management play out to reduce corporate and personal reputational damage. This is not wrong and is a necessary component for business survival. But too often it seems if the plan is to 'cover up' with a desire to sweep it all under the carpet. The traditional approach needs to be refashioned into a 'social responsibility' approach to provide transparent, comprehensive and coordinated mitigations thereby reducing the desire for a 'cover up'. This not only helps the victims but also supports all stakeholders within the service and supply chain. But developing a viable response needs something tangible which comes from understanding the type of vulnerabilities (weakness) that exist and how these can be exploited by hackers (threats).
10. How much of a barrier do you think each of the below issues are to organisations managing their cyber risk effectively? Single code per option (Not a barrier, Somewhat of a barrier, Moderate barrier, Severe barrier)	Severe in all cases.
11. What information would allow organisations to better make investment decisions in cyber security? Please provide evidence to support your answer. Open response	Boards, senior partners and other decision-makers need a better understanding of the computing basics of IT before focusing on cyber threats. Our approach to using computing as a utility leads to us falsely believing that we do not need to understand anything. This approach works well when something is either 'on' or 'off', such as electricity, but cyber and technology can be, to all intents and purposes, running normally yet working inappropriately, Hackers are very competent at what they do, so they can

	choose to explicitly disrupt or to disrupt out of sight. They can choose easy pickings or rich pickings. Hackers with the knowledge, expertise and patience can break even the most sophisticated situations and systems, given how few people understand technology to the same degree. India recently experienced a cyber-attack on its newest nuclear site (see https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6 Defining the basics can be encapsulated in four stages. • The first is to understand how our relaxed approach to technology blinds us to its complexity. Cause and effect are, therefore, underestimated. • The second is to have an overview of the stages a message from one computer to another goes through. To know the OSI (Open Systems Interconnections) model at its most technical is unnecessary but an overview will show the 14 stages required to dismantle a message from the sending computer into binary and reassemble that message at the receiving one. Each stage is a point of failure or attack, requiring specialist management and support. Multiply that with all the devices within the organisation, then across the supply chain and then over the entire internet, gives a feel of how vulnerable and reliant we are on each other. • The third is to have to have an acceptable board approach to meaningful boardroom conversations on cyber. This covers understanding: the role of the IT department; the value of IT audit; whom on the board is accountable for risk management; where the key responsibilities for risk control lie within the organisation; and what the common forms of cyber-attack are. • The fourth is to have a set of practical plans, both proactive and responsive. The framework for proactive plans are set out in the cyber-essential programme (see https://www.cyberessentials.ncsc.gov.uk/) covering access management, change management, defence-in-depth, and testing, to hinder cyber-breaches. Response plans deal with common forms of cyber-attack, such as managing data theft, dealing with a ransomware demand, and collecting digital forensics.
12. What are the barriers preventing organisations from creating, collecting or accessing this information currently? Please provide evidence to support your answer. Open response	There are many standards and many private sector solutions, but are neither mandatory nor consistent, so applied and adhered to on a voluntary, ad hoc basis. The IT industry has legislation covering the use of data[ii], the best-known being GDPR, and several voluntary standards in existence, in draft and being proposed[iii]. But there is little UK legislation covering the minimum requirements of the manufacture, use, safety and security of computer design, infrastructure and code. There is the "The Network and

	Information Systems Regulations 2018" (see https://www.legislation.gov.uk/uksi/2018/506/contents/made), which UK national critical infrastructure providers must comply with but there is no equivalent for the many providers who are 'out-of-scope'. IT professionals are, arguably, the most powerful individuals in the world. Hence the concerns about the giant tech companies, a result of innovation without restriction. There are plenty of suppliers of cyber security solutions. See https://www.cyberdb.co/database/uk/ but how does a board know from which to choose?
13. Is there evidence of anything in the market currently effectively addressing these information transparency barriers? Single response (Yes/No/Don't know)	Yes.
14. [If yes] Please provide evidence of how the market is currently addressing these information transparency barriers? Open response	The number of players in the market shows that there are plenty of solutions are available. They are transparent, in that they are easy to find, but their products and services are meaningless unless there is true understanding between what is on offer from the vendor and what needs addressing by the client organisation. Transparency is not the issue. Meaningful disclosure is, on how cyber threats occur, how to mitigate them, how to reduce likelihood and impact, how to discover them and then correct them.
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	GDPR is the main for organisations, followed by industry/sector regulatory requirements. See response to Q12.
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)	Yes.
17. [If yes] What types of	A – C. For 'other', please refer to our response to Q11.

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)	
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	There is already a lot in place in the UK, or under discussion. It is a question of applying them. Government/regulators/ industries could request all organisations/boards to: • Apply and refresh the Board Toolkit as part of the mandatory audit (see https://www.ncsc.gov.uk/collection/board-toolkit/introduction-cyber security-board-members)**.** • Ensure organisations focus on key sound practices, access management, data management, change management and testing to support cyber-resilience (see https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda). • Be certified in cyber essentials (see https://www.cyberessentials.ncsc.gov.uk/advice and https://www.cyberessentials.ncsc.gov.uk/about). • Provide evidence of board cyber training and refreshing at least once annually. Government could consider: • A requirement for 'security by design', an equivalent to 'data protection by design' (see https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes). This is especially important for future innovations related to Quantum Computing, where physics takes over from maths, drastically changing the approach to cybersecurity. The University of Texas states "that it is common knowledge in the field of quantum computing that quantum computers, once built, will dissolve all modern methods currently used to keep the internet secure" (see https://www.cs.utexas.edu/news/2019/implications-quantum-computing-internet-security-random-bits-and-more). • A broader application of the Bank of England's approach for the financial sector, called CQUEST, a cyber-resilience questionnaire, and CBEST, a way of testing cyber-resilience framework (see https://www.bankofengland.co.uk/financial-

	stability/financial-sector-continuity). • Aspects of the King IV Code of Corporate Governance for South Africa This 2016 codes takes note of technology and information (see https://ecgi.global/code/king-report-corporate-governance-south-africa-2016-king-iv-report), stating that in the Forward that "Technology is now part of the corporate DNA". • Addressing issues raised in the PRA's CP3019[iv] covering outsourcing and third party risk management. The points made, especially in sections 7 – 10 on audit, data security, sub-outsourcing and business continuity, apply across all businesses. • USA's requirements under Sarbanes-Oxley. A UK equivalent approach has been raised in BEIS' consultation of the Future Audit Regulator, under recommendation 51.
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	See responses to Q11, 14 and 18.
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	We believe that voluntary code for IT and Cyber security is a possible way forward. For companies that do not sign up to the code, questions will be asked by investors. A code will also ensure that much more attention is paid to cyber security by Audit and Risk Committees.
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	Insurance companies now cover cyber risk. Maybe there should be a 'health and safety' requirement for all firms to have cybersecurity cover. The premiums could be less for those complying with cyber essentials, having IT audit reports available, and information on number and type of breaches detected.

RESPONDER INFORMATION

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

a. Individual

b. Organisation

Organisation

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

f. Interested in a career in cyber security

g. Interested member of the general public

h. Other Free text

N/A

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

UKSA is a membership organisation supporting the rights, education and welfare of private investors.

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

p. Other services

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

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

UK Shareholders' Association (www.uksa.org.uk)

28. Are you happy to be contacted to discuss your response and supporting evidence?

Yes.

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

Sue Milton, sue.milton@uksa.org.uk

[i] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[ii] See https://www.jisc.ac.uk/guides/networking-computers-and-the-law/laws and https://www.bristol.ac.uk/media-library/sites/infosec/documents/guide.pdf

[iii] See https://standardsdevelopment.bsigroup.com/categories/010 covering many of IT's core components from fibre optics to network design.

[iv] See https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf?la=en&hash=4766BFA4EA8C278BFBE77CADB37C8F34308C97D5.