HM Government

Cyber Security Regulation and Incentives Review

December 2016

1. Contents

Foreword by the Minister for Digital and Culture

As part of building a country in which people have confidence to use and build digital technology, we are committed to making the UK the safest place in the world to go online. The recently published National Cyber Security Strategy and the launch of the National Cyber Security Centre show how important this issue is.

As the threat continues to evolve so Government must keep up. We are doing this on a number of fronts - by attacking the problem at source as well as improving our protections so that we can stop and fight back against those who wish us harm.

The responsibility for keeping the UK, its economy and its citizens safe is shared. Every business, charity and institution up and down the country must realise that cyber security is their job as much as it is Government's. Only when the effort is concerted and persistent can we fully tackle this challenge.

Businesses have a responsibility to their customers to keep their data safe, as well as to shareholders and investors to remain competitive in a global marketplace. This Review has considered whether there is more that Government can do to require or incentivise good cyber risk management in such organisations.

The Review notes that the upcoming General Data Protection Regulation (GDPR) will be key to ensuring strong organisational data protection regimes supported by strong cyber security. But regulation alone is not enough. So we propose a range of new activities building on our existing approach to business engagement to ensure that organisations across the country know how to protect themselves and their digital assets.

I would like to thank all of those who contributed to this Review and I look forward to working with partners across the economy to make the vision of a safe and secure cyberspace for everyone a reality.

The Rt Hon Matt Hancock MP, Minister of State for Digital and Culture

Executive Summary

This Review was conducted in 2016 to consider whether there is a need for additional regulation or incentives to boost cyber risk management across the wider economy, i.e. beyond those delivering essential services such as Critical National Infrastructure. The Review came about from a concern that the pace of change has thus far been insufficient to deal with the growing threat from cyber attacks with potential implications for consumer confidence, public protection and economic growth. The Review process included significant stakeholder engagement and evidence gathering from a broad range of sources.

Effective cyber security risk management is vital to the success of the UK economy and to ensuring the safety of citizens. However, Government is clear that any interventions need to be proportionate. It does not want to overburden businesses and organisations with unnecessary regulatory requirements.

The Review shows that there is a strong justification for regulation to secure personal data, as there is a clear public interest in protecting citizens from crime and other harm, where it may not otherwise be in organisations' commercial interests to do so. Government will therefore seek to improve cyber risk management in the wider economy through its implementation of the forthcoming General Data Protection Regulation (GDPR). The breach reporting requirements and fines that can be issued under GDPR will represent a significant call to action. These will be supplemented by a number of measures to more clearly link data protection with cyber security, including through closer working of the Information Commissioner's Office and the National Cyber Security Centre.

For now, Government will not seek to pursue further general cyber security regulation for the wider economy over and above the GDPR. It should ultimately be for organisations to manage their own risk in respect of their own sensitive data (e.g. intellectual property) and online presence. The Review findings also suggest that the impact of other regulation would anyway be limited, and unlikely to be effective enough to outweigh the burden on business. Imposing specific requirements could also encourage a 'compliance' culture rather than proactive cyber risk management.

Government will however pursue a number of new non-regulatory interventions to incentivise better cyber risk management, in support of the existing business engagement strategy. These will mostly be delivered through the National Cyber Security Centre, providing advice and guidance to organisations and incentivising them to improve their cyber security risk management.

Given the continually changing landscape of cyber threat, Government will keep under regular review the need for regulation and further activity in this area, to ensure these conclusions remain valid.

2. Introduction

The cyber security context

2.1 Government is committed to making the UK the safest place in the world to live and do business online. The recently published National Cyber Security Strategy[1] sets out the Government's vision for the next five years, through three broad areas of activity: to defend our cyberspace, to deter our adversaries and to develop our capabilities. This holistic approach will enable us to both reduce the number of successful attacks and respond faster and more appropriately when attacks do occur.

2.2 Government has a clear interest in ensuring that individuals are protected from cyber attack. This Review came about from a concern that the pace of change across the wider economy has been insufficient to deal with the growing threat from such attacks with potential implications for consumer confidence, public protection and economic growth.

2.3 It is important to understand that this problem is not new. As the Cyber Security Strategy notes, Government has already undertaken a significant amount of work in tackling cyber crime and boosting cyber security. The Government is already delivering a number of programmes to improve business understanding and resilience, centred around the establishment of the National Cyber Security Centre (NCSC)[2]. This focuses on providing advice and tools (such as the Cyber Essentials Scheme)[3] to help businesses understand and act on the cyber security threat as well as certifying certain types of cyber security services and training. This work to engage businesses is supported by action to counter malicious activity in cyberspace before it reaches consumers or businesses, through the new Active Defence programme, and by law enforcement activity.

2.4 However, Government recognises that the threat is constantly changing and our approach should be dynamic in response. Alongside this, businesses must also accept responsibility for their cyber security and ensure that they have the appropriate controls and systems in place to deter and deal with breaches if they do occur.

---

[1] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[2] https://www.ncsc.gov.uk/

[3] The Government's scheme to help businesses get the basics in place to protect against common cyber attacks, and provide assurance. https://www.cyberaware.gov.uk/cyberessentials/

The Review

2.5 This Review is part of Government's commitment to ensure that the UK has the right regulatory framework in place for cyber security across the wider economy[4]. It has explored whether new regulation, incentives or other interventions could help to amplify or accelerate the impact of existing Government work.

2.6 The Review was led by the Department for Culture, Media and Sport (DCMS) with input from a range of departments and partners, and has considered businesses across the economy and other non-commercial organisations (e.g. charities and universities). It has not focused on cyber security regulation in relation to national infrastructure sectors including the Critical National Infrastructure (CNI) which are being considered separately, in the context of implementation of the forthcoming European Directive on Security of Network and Information Systems (the NIS Directive) and wider Government considerations of critical infrastructure.

2.7 Providing the right regulatory environment for cyber security - which incentivises better security but avoids unnecessary business burdens - should be a competitive advantage for the UK as we seek to harness the opportunities presented by leaving the EU. Ensuring confidence in the resilience of the UK's digital economy will be important for successful delivery of the Government's forthcoming industrial strategy as well as being essential for protecting ordinary citizens.

2.8 The Review therefore considered options with an understanding that any burdens placed on businesses were fair and proportionate, and that we seek where possible to build a positive and engaged approach to cyber security across the economy - rather than a 'compliance culture' - from the smallest start-up to the largest FTSE 100 company.

Approach to gathering evidence

2.9 Evidence gathering has been central to this process. The Review sought to understand the existing literature on cyber security and business behaviour change, and commissioned TNS BMRB to conduct new qualitative market research[5] to help understand the business implications of a number of the options considered. The findings have been published in full alongside this report and we have taken these into account when coming to the conclusions set out.

2.10 The Review team also met with a wide range of stakeholders representing a variety of views - including businesses and charities, regulators, sector organisations, consumer groups, academics, cyber security experts and departments across Whitehall. A senior expert advisory group including representatives from these interest groups was

[4] The Review findings are applicable to the whole of the UK, as cyber security is not a devolved issue. Therefore, any reference in the paper to 'Government' is a reference to the UK Government.

[5] Cyber Security – testing mechanisms for change, TNS BMRB, 2016

convened to advise the Review team, test potential approaches and generate new ideas. The group met three times during the course of the Review, and was chaired by Professor Chris Hankin, a leading academic in the cyber security field.

2.11 International comparisons were also sought from key countries within and outside the EU. This was both to determine whether other countries had lessons which could be learnt for the UK context on cyber security but also to ensure international harmonisation where possible, and avoid overburdening UK businesses compared with their international counterparts. More detail on the international comparisons work is at Annex B. This work was complemented by GCHQ analysis of the security impact of the proposed options.

2.12 This comprehensive approach enabled the Review to gather a wide range of evidence. However, there are inevitably limitations to the evidence base due to the immaturity of cyber risk management and difficulty collecting accurate information on the problem and solutions. Few comparable countries have regulated outside the CNI, and where they have there is little evidence on impact. Whilst Government is therefore confident that the conclusions of this Review are appropriate at the current time, this is an area of policy which will remain under review as the evidence base grows and the threat from cyber attacks develops.

2.13 The rest of this report sets out our understanding of the problem and rationale for intervention, as well as key findings of the Review in relation to both regulation and incentives.

3. Understanding the problem and the need for Government intervention

Cyber risk in the UK economy

3.1 As the digital economy is growing so too is the opportunity for cyber criminals to exploit vulnerabilities in IT systems and access, damage, and destroy data and hardware. Businesses continue to experience cyber security breaches with one in four businesses detecting a breach in the last year.[6] The nature of the attacks mean many businesses may not know their IT systems have been breached.

3.2 Cyber security breaches have a direct impact on the organisations affected, including lost staff time dealing with the breach and disruption to other work. As a result businesses incur financial losses with the average direct costs of a breach estimated at £36,000 for large businesses and £3,100 for micro/small businesses. The most costly single breach identified in the Cyber Security Breaches Survey was £3,000,000 for a large firm.[7] There can also be reputational costs with a number of firms experiencing a loss of customers following a breach. Breaches can also result in consumers and other businesses incurring costs, for example through fraud. A US survey found that the majority of consumers affected by a breach reported they incurred costs with an estimated average of $500, while less than a third said they incurred no costs.[8]

3.3 Despite the potentially significant financial costs, evidence shows businesses are not doing to enough to protect themselves, both in terms of technical controls but also risk management and incident response. Whilst 69% of businesses say their senior management consider cyber security is a very or fairly high priority for their organisation just over half (51%) of all businesses have actually taken recommended actions to identify cyber risks, and only 10% have a formal incident management plan. Only 17% of businesses say their staff attended some form of training on cyber security in the last 12 months.[9]

---

[6] Cyber Security Breaches Survey, HM Government, 2016

[7] Ibid

[8] Consumer attitudes towards data breach notification and loss of personal information, RAND corporation, accessed at http://www.rand.org/pubs/research_reports/RR1187.html

[9] Cyber Security Breaches Survey, HM Government, 2016

Rationale for Government intervention

3.4 The evidence gathered during the Review identified a number of barriers to organisations across the wider economy improving their cyber security. Some of these barriers stem from market failures (factors which prevent the market from working well and allocating resources to maximise the value for society) which have acted against widespread adoption of effective cyber risk management by organisations. The evidence and theory suggest the presence of the market failures set out below.

Information failures

3.5 The nature of the cyber threat means there is **hidden information** such that businesses do not know enough about the threat and which measures will offer the most effective protection.

3.6 This is supported by research that indicates that not all organisations have the knowledge, understanding and confidence around cyber security in order to implement appropriate measures.[10] Risks are downplayed, for example smaller firms do not think they will be the target for attack[11] and perceive themselves as too small to be the target of cyber criminals,[12] which means they may not fully understand the potential negative consequences of cyber attacks.[13] It also showed that businesses often only took action to protect themselves following a breach or attack. Users often continue to use existing security protocols that they are comfortable with but which may be out of date with the threat. There is also a perception of high cognitive effort to understand and implement changes.

3.7 The research also indicated that organisations may not fully understand who is responsible for cyber security. Some small businesses thought their bank was dealing with the cyber threat, while medium and large businesses could defer responsibility to their IT teams or outsourced providers without necessarily checking that the risk was being managed.

3.8 Another information failure is that organisations do not know which cyber security organisations they can trust. The cyber security suppliers hold more information about the effectiveness of their services and products than the buyer, who does not know whether these will be appropriate for the vulnerabilities in their IT systems, a problem known as **asymmetric information**. While a problem common to many markets, it is particularly acute for cyber security due to its technical and constantly changing nature and the barriers mentioned above. This also means it is challenging for

[10] Using behavioural insights to improve the public's use of cyber security best practices, Summary report, Government Office for Science, 2014.

[11] UK businesses don't believe they are at risk of cyber crime, Aviva http://www.aviva.com/media/news/item/uk-businesses-dont-believe-they-are-at-risk-of-cyber-crime-says-aviva-17582/

[12] Cyber Essentials Scheme – process evaluation and communications testing, TNS BMRB, 2016

[13] Cyber Security – testing mechanisms for change, TNS BMRB, 2016

consumers to determine the security of firms and therefore distinguish which have the better cyber security when making a purchase, hindering the market function.

3.9 Additionally, while not a market failure for cyber risk management, the research finds the high financial costs of security software upgrades and external consultancy also act as a barrier, especially in small businesses and charities where resources are limited.

External costs

3.10 Cyber security can protect three key areas of business interest from attack: (1) personal information, (2) other sensitive data (e.g. intellectual property, financial and commercial information), and (3) an organisation's online presence (e.g. website).

3.11 While it is expected that organisations face the right incentives to protect their own sensitive data and online presence, it may not be in their commercial interests to mitigate against the wider external costs that could occur from a successful attack that affects personal information (i.e. of customers or employees), or other businesses' commercial information.

Government intervention

3.12 The combination of the above lack of information and external costs is likely to lead to organisations under-investing in a sufficient level of cyber protection. This can have consequences for the economy as consumers and other businesses are also harmed when security is breached. Government therefore has a clear role to play in addressing the information barriers, for example through its business engagement strategy, and in ensuring the market incentives work to maximise cyber security.

3.13 In this regard, there is a strong justification for regulation to secure personal data because it may not be in organisations' commercial interests to implement protection to a level that is in the public interest. Personal data is the primary sensitive information held by many organisations and has been at the centre of many major breaches (e.g. TalkTalk and Yahoo).

4. Regulation: the role of data protection in cyber security

4.1 Given the clear justification for intervention in relation to personal data, Government already has in place a regime for data protection in the UK, set out under the Data Protection Act 1998 (DPA). This controls how personal information is used by organisations, businesses and the government. Under the DPA, those responsible for using data have to follow strict data protection principles to ensure that the data is used lawfully and limited to specifically stated purposes whilst being kept safe and secure.

4.2 The Government intends to apply the forthcoming General Data Protection Regulation (GDPR) from May 2018. The approach the UK takes to implementing the GDPR presents an opportunity to incentivise significant improvements in cyber risk management.

4.3 The GDPR gives a legislative underpinning to many data protection practices that the Information Commissioner's Office (ICO) considers to be best practice. The DPA already requires organisations to put in place appropriate organisational and technical measures to protect personal data, and this requirement will also apply under the GDPR. However, it will be significantly bolstered by a number of new requirements relevant to security, including:

- Mandatory breach reporting to the ICO and customers
- Data protection impact assessments and provisions around data protection by design
- Requirement for data protection officers in certain organisations
- Much more stringent sanctions with significantly higher fines than those currently available and the potential for further penalties via class-action lawsuits

4.4 Evidence from our research and stakeholder engagement suggests that breach reporting and the proposed sanctions in particular, will be a significant call to action on cyber security.[14] Government intends to make the most of this incentive, and will ensure that cyber security is at the centre of the way we promote and implement the GDPR, including the ongoing work required to develop the detail of GDPR-related guidance and schemes.

[14] Cyber Security – testing mechanisms for change, TNS BMRB, 2016

4.5 The ICO is responsible for enforcing data protection regulation and already has an excellent reputation for its work. The ICO will continue to increase its capacity and capability on cyber security and will work in close partnership with the new NCSC at both a strategic and operational level to ensure effective operation of the GDPR. As part of this, Government will be supporting the ICO and NCSC to agree clear information security principles to underpin guidance for organisations and enforcement. These principles are also likely to be appropriate to protect other sensitive information.

4.6 Given that our evidence showed that the fines available under GDPR represent a significant call for action, Government believes that the aggravating and mitigating factors affecting the size of fines imposed for cyber security-related breaches should incentivise organisations to adopt good cyber security practices. Government will work with the ICO and other member states to develop the detail of GDPR fining structures with this in mind. There may also be value in extending the ICO's public sector compulsory audit power to all organisations processing personal data, which would enable early intervention if the ICO has concerns. DCMS plans to consider this as part of its imminent review of ICO powers, enabling any changes to be introduced in time for GDPR implementation.

Regulation beyond data protection?

4.7 The Review has considered whether there is a need for regulation beyond data protection. Following detailed consideration of evidence from stakeholders and available literature, it concluded that additional cyber security regulation on organisations across the wider economy 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 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.

4.8 The Review explored regulatory approaches that could be adopted in the event that the Government had concluded that new regulation was necessary and in the public interest (e.g. mandating specific controls, assurance schemes, annual reporting and director liability). However, the Review concluded that their impact would be limited, and unlikely to outweigh the burden on business. Particular concerns were raised about the potential for various approaches to incentivise a 'compliance' culture rather than proactive cyber risk management. More information on the options considered, and the evidence relating to them, is included at Annex A.

4.9 The Review concluded that the new data protection regulation will be sufficient to catalyse significant change in cyber risk management by organisations. This will particularly be true when coupled with further business engagement and wider Government action, as will be discussed in the next chapter. It has also been noted that whilst enforcement will be focused on data protection, the same principles that

organisations will need to adopt to protect personal data will also help to protect other sensitive data, with an associated general uplift in security awareness and action as a result of GDPR. This was in keeping with the common view of stakeholders where there was limited appetite for regulation beyond GDPR.

4.10 It should be noted that this Review looked at cyber security risks in the wider economy and not at risks specific to those sectors delivering essential services including the Critical National Infrastructure (CNI). Government is separately considering whether additional regulation might be necessary for critical sectors, including in the context of the NIS Directive due to be implemented in 2018 as well as wider national infrastructure considerations. Under the NIS Directive operators of key essential services and key digital service providers operating in the EU, e.g. cloud computing services, will be subject to additional risk management and reporting requirements. The detailed scope and security requirements for NIS implementation will be set out by Government in 2017, informed by the work of the NCSC and lead Government departments with relevant sectors alongside broader Government consideration of critical infrastructure.

4.11 A regulatory focus on data protection for the wider economy and a more comprehensive regime for essential services in critical sectors is consistent with the vast majority of countries comparable with the UK. Consistency is important for companies trading internationally - a point raised frequently in our stakeholder engagement. The UK already has a good reputation for both its cyber security and balanced regulators, including the ICO. The combination of a proportionate regulatory framework, increased support through the business engagement strategy and NCSC and wider measures to protect UK interests, e.g. the Active Cyber Defence Programme, will create a competitive advantage for the UK.

5. Incentives and other non-regulatory interventions

5.1 A common theme in stakeholder engagement was that any regulatory requirements need to be matched by a **wider uplift in support and information**. Stakeholders had high expectations for the National Cyber Security Centre (NCSC) and welcomed the focus of the Government's business engagement strategy on improving guidance, developing high quality tools and working through important influencers and amplifiers to reach target businesses and other organisations.

5.2 Based on evidence collected, the Review therefore recommends a number of additional new non-regulatory measures which would address key market and organisational barriers identified. It should be noted that a number of GDPR-related guidance documents, schemes and stakeholder relationships are currently at an early stage of development and will be considered in light of this Review's findings.

5.3 In relation to addressing information failures, DCMS, the NCSC, and the ICO will seek to **maximise the impact of awareness-raising activity on cyber security by using GDPR implementation as a key focus and call to action**. Our research showed that some stakeholders are already aware of GDPR and its implications but this awareness is not universal. Linking cyber security to data protection from the start will help to increase this understanding - both of the issue and the potential protections that organisations can put in place. To help with this, the NCSC will **involve the business community in designing and testing the guidance it develops** for the wider economy. It is important to develop guidance which is written in language that businesses understand as it is more likely to be accessible and ultimately followed.

5.4 Addressing the information barrier is also important in relation to breach data. It is extremely helpful for businesses to understand what the latest cyber criminal activity is - and therefore where they can best focus their security efforts. The NCSC and ICO will **use breach reporting data** (which will become more readily available due to GDPR), building on the data available in the Cyber Security Breaches Survey, to increase their understanding of the threat and share this as appropriate with businesses, regulators and insurers. The NCSC will also establish a **regulators' forum**, convening influential regulators with an interest in cyber security to share good practice and threat information, and ensure consistent messaging around cyber security.

5.5 A significant area of interest for the Review was how good cyber risk management could be better embedded into corporate governance processes. Whilst there were a

number of suggestions for regulation in this space (e.g. around inclusion of a requirement to report on cyber security in annual reports or inclusion in statutory audit), the Review has concluded that this work is best pursued from a positive business engagement stance, rather than instituting a culture of compliance which ultimately does not lead to transformative behaviour change.

5.6 The Review therefore proposes that the **NCSC work with a range of partners, such as the Financial Reporting Council, to send messages to Boards** about the importance of understanding cyber risk and what they can do to improve their risk management in this area. The NCSC will also work with the Investment Association and key investors to **educate the investment community about cyber risk and give them tools to challenge Boards**, building on partnerships with the legal, accountancy and audit professions. This was seen to be a particularly useful step as investors and shareholders can have significant influence over company policies and play a key role in influencing behaviour change.

5.7 An option which attracted support during research was introduction of a 'cyber health check' for organisations - basically an independent check which would consider whether security practices in place were appropriate and sufficient to deter attacks and provide advice on how an organisation could manage its cyber risk more effectively. Whilst the Review does not recommend mandating such checks, it is clear that organisations would benefit from having access to trusted and reliable organisations to deliver health checks. The NCSC will therefore explore options for **certifying trusted organisations to deliver cyber risk management health checks** - providing businesses (particularly SMEs) with impartial advice on how to improve their cyber risk management, complementing the Cyber Essentials technical certification.

5.8 The Review also looked at ways to further incentivise the adoption of basic technical controls, including more widespread uptake of the Cyber Essentials scheme. This can partly be done through promotion of Cyber Essentials when providing advice and guidance. For example, the **GDPR information security principles** will seek to include reference to Cyber Essentials, and Government will look to **build formal links between the Cyber Essentials scheme and any new GDPR privacy seal.**[15] Government will also seek to build a requirement for Cyber Essentials certification into **Government grant schemes for innovation and research**, complementing work to embed Cyber Essentials in Government procurement and business supply chains.

5.9 The Review considered a number of other interventions in relation to promoting cyber security in the wider economy. These included new financial incentives such as enhanced tax relief and vouchers for cyber security investment. Whilst popular with some businesses, evidence suggests they would be disproportionately costly to

[15] A privacy seal is a 'stamp of approval' which demonstrates good privacy practice and high data protection compliance standards.

implement, and that a significant proportion of take up would be by organisations already planning security improvements. Basic tax relief is already available for business expenditure on cyber security, and companies should ensure they benefit from this. More detail showing consideration of financial incentives is at Annex A.

5.10 A number of stakeholders suggested that there was more that could be done by those developing internet-connected products and services to ensure that they are **secure by default**. Whilst this went beyond the remit of this particular Review, it is an issue in which Government has a clear interest. Government will therefore consider further the need for the right incentives to be in place to build security into internet-connected products and services. This is a growing priority given the challenges posed by the Internet of Things for businesses and consumers, where getting the balance right between innovation and security is critical.

6. Review conclusions

6.1 The Review has concluded that significant improvements in cyber risk management can be achieved through implementation of the forthcoming GDPR, including new requirements to report significant breaches to the ICO and individuals affected. Evidence indicates that the significant financial sanctions available for breaches, and the application of aggravating and mitigating factors, will drive the security behaviours we want to see. Government will seek to ensure that the ICO, NCSC and other agencies clearly understand their role in using the GDPR as a hook to incentivise better cyber security behaviours.

6.2 For many organisations lack of information can be a major barrier to action. Government therefore recognises the importance of matching new requirements under the GDPR with a general uplift in support and information. Government's wide-ranging National Cyber Security Strategy, centred around the establishment of the NCSC, will be vital in delivering this holistic approach to the wider economy.

6.3 International evidence indicates that following the implementation of this Review's recommendations, the UK would be in step with the regulatory requirements for cyber security on organisations in other countries, but in many cases ahead of the curve in terms of the advice and support provided by Government.

6.4 The cyber threat and the response to it from across the UK economy will continue to evolve, and our evidence base will continue to grow. It is important that businesses recognise their responsibility in this space to understand the risk, protect themselves from cyber attack and have suitable systems and processes in place.

6.5 Given the changing nature of the threat, this Review's findings on the UK's position on regulation for the wider economy will be subject to regular review. This will take account of a range of factors including data from the Cyber Security Breaches Survey, evidence gathered from the application of the GDPR and the NCSC's assessment of the security threat.

Example of how the Review recommendations will affect organisations in practice

Company A is a large organisation processing significant amounts of personal data, both in relation to its staff and its customers. Under the new requirements set out in this Review, it would be under the auspices of the new GDPR rules and requirements as well as able to access Government advice.

In the first instance, Company A would have access to the 'wider economy' support of the new NCSC. This could include access to online guidance and advice. It would be able to request a health check from a company which had been certified to carry out such services by the NCSC, and could also apply for Cyber Essentials certification which would act as a signal to industry and the public that it had undertaken basic 'cyber hygiene'. If Company A belongs to a professional body or organisation, it may also be able to access additional information through them.

Under GDPR requirements, Company A would be required to take appropriate measures to ensure that the personal data it holds is safe and secure. It would be required to carry out a Data Protection Impact Assessment in high-risk situations, for example where a new technology was being deployed or where a profiling operation was likely to significantly affect individuals. Given that the company regularly and systematically monitors data subjects on a large scale, it would also be required to appoint a Data Protection Officer, with responsibility for data protection compliance and the knowledge, support and authority to do so effectively. Cyber security would be an important aspect of this.

In the event that a data breach did take place, the company would be required to report this to (i) the Information Commissioner, and (ii) those whose data has been compromised (where this is likely to result in a high risk to individuals). Company A would be liable to a very sizeable fine (significantly higher than that currently applicable), with the final amount determined by the ICO and dependent on a number of factors. An important factor to be taken into account is whether the company had put in place appropriate technical and organisational measures (including those relating to cyber security). The security principles set out by GCHQ and the ICO would be used in part to determine whether this was the case.

Appendix A: Options analysis summary

A number of regulatory and incentive options were considered as part of this Review. They were wide-ranging and represented ideas from a range of stakeholders, as well as Government's understanding of the cyber risk threat to the broader economy. The options were considered against a range of parameters, including anticipated effectiveness, ease of implementation and cost to businesses and the taxpayer.

Measure	**Conclusions**
Forthcoming regulation	
General Data Protection Regulation (GDPR)	There are a number of important provisions within the GDPR which will be beneficial for information security: • Organisations must have in place 'appropriate technical and organisational measures to protect personal data' - this builds on existing data protection requirements (under DPA) but, combined with fines and other requirements under the GDPR, the impetus to comply with this principle will be strengthened. • Breach reporting to ICO and customers - the GDPR introduces mandatory reporting of personal data breaches to the ICO and customers (in certain instances), which places additional accountability on data controllers and should provide additional impetus to ensure good data protection practices. • Sanctions - sizeable fines, with the potential for further penalties via class-action lawsuits. • Privacy Impact Assessments and Privacy by Design. Research indicated that businesses would take action to protect themselves in response to the significantly higher fines. They also say the mandatory reporting potentially results in reputational damage and that this is also a strong call to action.[16] DCMS is working with ICO and NCSC to ensure that organisations implement good cyber security practices as they seek to meet the requirements in the GDPR, and that the ICO has the necessary capacity and capability to enforce information security obligations, including: • Set out principles of good cyber risk management - providing

[16] Cyber Security – testing mechanisms for change, TNS BMRB, 2016

	authoritative guidance on the effective technical protection of personal data will help to ensure better cyber security outcomes in businesses looking for guidance on how to meet the requirements of GDPR. DCMS is working with NCSC and ICO to ensure that NCSC-developed principles are fully incorporated into approved codes of conduct or guidance provided by the ICO, as well as encouraging adoption by other states implementing GDPR. • Reviewing the need to extend the ICO's public sector compulsory audit power to all organisations processing personal data, to ensure the ICO can intervene early where it has concerns rather than waiting for a breach to occur. • Evidence indicates that the significant financial sanctions available for breaches, and the application of aggravating and mitigating factors to the scale of fines will present a strong call for action and drive the security behaviours we want to see. • DCMS is working with ICO and NCSC on how to formalise the link between following NCSC-developed principles and reductions in fines.
Network and Information Systems (NIS) Directive	Subject to Government consideration on scale and scope, under the NIS Directive, organisations that face the highest risk (i.e. essential services in a significant proportion of the Critical National Infrastructure) and key digital service providers would be subject to more comprehensive risk management and reporting requirements. The digital service provider requirements should help to secure the digital services on which many UK businesses are dependent.
Specific controls / risk management requirements	
Require specific cyber controls, risk management practices or systems testing	Mandating specific controls or approaches could help raise businesses up to a certain minimum standard of technical controls. However, it is an extremely heavy intervention for organisations outside of CNI, which could be seen as directly interfering with the affairs of individual businesses and go against a general principle that businesses should be responsible for dealing with their own business risks. Also due to each IT system being unique, technical controls need to be appropriate for each organisation. This approach is also likely to lead to a compliance culture, rather than a more preferable proactive response with greater Board awareness and better understanding of the underlying issues. This kind of culture would not help to address the complexity of a constantly changing cyber risk landscape, which requires greater understanding and engagement, not just compliance. Specific controls could become out of date very quickly - and Government could be accused of failing to protect businesses if the information was not constantly updated. We will not pursue this option.
Require inclusion of cyber risk in statutory audit	Statutory audit is a heavily regulated and defined process. It stems directly from accountancy principles and was not designed or intended to take on significant issues outside of these. The Review concluded that statutory audit

process	is therefore not the appropriate vehicle to effect cyber security change - and that any changes to the statutory audit process would be very difficult to effect. However, a number of stakeholders were keen to point out that auditors are held in high regard by the companies they work for and can be an important source of information and advice for those companies. Government has previously produced advice on cyber security risk jointly with the ICAEW for accountants and auditors. Government will continue to work with the ICAEW to explore ways of building on this training and making the most of the opportunity given the position and influence of auditors when talking to clients. Government is also exploring whether there is further work we can undertake with the internal audit community and Audit and Risk Committees to encourage better cyber risk management.
Require businesses to undergo a cyber health check	Requiring a mandatory health check of organisations would be a very heavy intervention from Government. A requirement on all businesses would also impose significant cost on business, a number of whom may not be in need of a health check. This option also contradicts the view that business risk is in general an issue for businesses themselves, not Government (beyond protection of personal data). We will not implement this option. However, research uncovered enthusiasm from a number of businesses for an 'independent' health check process, or a way in which they could gain trusted advice from organisations which were not going to subsequently hard-sell them into further products or services, and which would advise them on how their approach compares with that of their peers with accompanying advice on next steps. Whilst it is not appropriate for Government to provide a health check service, this finding suggests a market failure in that firms do not have sufficient information to determine which services can be trusted. Government can seek to address this through non-statutory means. GCHQ already recognises certifying bodies for Cyber Essentials and offers an accreditation process for Cyber Security Consultancy Services. The NCSC will investigate whether either of these could be used or expanded to include lighter-touch consultancy services for non-CNI / smaller organisations. The Expert Advisory Group were supportive of this proposal.
Accountability and transparency	
Require cyber risk reporting, e.g. in annual reports	Including information on cyber risk in annual reports is unlikely to be an effective or popular way of encouraging large-scale change in cyber risk management. Our qualitative research found that businesses did not think this would change their behaviour. Advice from both BEIS and the FRC is clear that annual reports are not intended to work in this way. They are mainly for providing accounts information and associated narrative. Recent changes mean that reports do now include a 'viability statement' on the business but the fruitfulness of these has not yet been tested. It has also

	been noted that two-thirds of FTSE companies do already include information on cyber security risk in their annual reports.[17] The bigger question is therefore on whether the information provided is of high quality and indeed whether or not it is useful for its intended audience - shareholders and investors. In relation to investors, following detailed discussion with the investment community, it is clear that they are also against the idea of mandating inclusion of cyber risks in annual reports as they did not think it would effect change. They noted that it would be more difficult to differentiate between the cyber security maturity of organisations if they were all automatically required to include risk statements. However, stakeholders are keen to develop and promote guidance for investors on questions to ask companies about cyber risk. With the NCSC we will work with them to develop guidance for investors. In the long term they will also look to include cyber security in the guidance they provide to businesses on the kind of information they want to see in an annual report, and in the reports that they provide to investors each year on every listed company.
Introduce director liability, e.g. for breaches	Individual Director liability has been introduced in limited instances in the UK (e.g. fraud) and has seen very limited prosecutions in the cases where it does exist. Many stakeholders were against the proposal and argued that it would create a culture of penalisation rather than proactive responsibility-taking, and that it would discourage good candidates from becoming Board members. Given the complexity of cyber risk, it is argued that a holistic organisational view is instead required, rather than giving responsibility to a single individual - with Boards encouraged to face cyber risk through more positive interventions. Further, there is a relatively high likelihood of a breach happening even if measures are in place, and it would not necessarily help to penalise Directors in those instances where the burden of proof that they had 'appropriate measures' in place is high. We will not pursue this option.
Mandate identified board member and/or staff member with responsibility for cyber security reporting directly to the board	This option on its own does not clearly address either the basic cyber information failure or externalities. However, there is an argument that appointing responsibility within an organisation can focus some minds on the issue. In this way, many organisations already have a named Data Protection Officer (DPO) for example as part of their compliance with the Data Protection Act. The evidence suggests that creating responsibility alone will not have the desired impact. Named persons would need to be suitably empowered, both organisationally and in terms of the skills they need to discharge their duties. There is concern that organisations may not have sufficiently 'cyber literate'

[17] Cyber Governance Health Check, HM Government, 2015/16
https://www.gov.uk/government/publications/cyber-governance-health-check-201516

	staff with sufficient cyber expertise, mirroring concerns around identifying suitable numbers of appropriately qualified DPOs as a similar problem. Cyber security is better seen as part of wider security responsibilities within the organisation, with joint responsibility across a number of roles and not just one. We will not pursue this option. However, given the upcoming GDPR requirement for certain 'higher risk' organisations to have a DPO Government will consider whether there are synergies between that role and cyber security more broadly.
Insurance	
Require cyber insurance	Holding a cyber insurance policy can provide an organisation with cover against a range of cyber risks and government supports the uptake of cyber insurance by industry. However, the market is in nascent form and insurers lack the data required to price policies effectively. Norms are not sufficiently established to determine in all cases whether companies have been unlucky or negligent. If cyber insurance was mandated, it is not clear that the market could provide policies appropriate to the needs of the organisations required to purchase them or that those organisations could effectively judge whether a policy they are required to hold is appropriate to their needs. The insurers spoken to are not in favour of this measure. We will not pursue this option further.
Basic 'cyber hygiene' (e.g. Cyber Essentials certification or other measure) as pre-condition for access to other benefits	
Enhanced tax relief	Businesses already get basic tax relief for all expenditure incurred on maintaining their cyber security. The Review explored several options for providing additional tax relief, including an enhanced rate of relief on all cyber security investment and a capped one-off relief that could reduce the cost of obtaining Cyber Essentials or another approved programme for 1.25m employers. All tax options would have significant costs (~£1bn for an enhanced rate of relief, or ~£0.5bn for a capped relief). Costs for an enhanced rate of relief are likely to increase in future years. It is not clear whether tax reliefs would have more impact on cyber security than cheaper options. The 2013 capped annual employment allowance claimed by 89% of businesses incentivised only 6% of claimants to spend more on employing personnel. There could also be significant deadweight, where support is provided to those who would have implemented cyber security measures anyway, meaning the additional benefits are lower. We will not pursue this option.
Voucher scheme	Vouchers could be provided for Cyber Essentials certification helping to address financial constraints in small businesses but would not cover the full

	costs. For example 3,000 vouchers could be offered in a year valued at £350. The costs to the taxpayer would be over £1,050,000. This could be popular with small businesses, but would not have a significant impact on uptake of the scheme and therefore would not be good value for money. An evaluation of the 2014 BIS Growth Voucher scheme found that excluding the voucher groups' use of their voucher, there was no statistically significant differences in the actual use of advice between the voucher group and the control group. With a small scale voucher scheme, there will be a higher proportion of businesses already planning to be certified that benefit from the voucher, with no additional impact on outcomes. We will not pursue this option.
Access to Government funding streams	Mandating Cyber Essentials for those in receipt of certain government grants would increase up-take of the scheme and ensure these businesses have basic levels of security controls, particularly important where the grant is for the development of important intellectual property for the UK. It is less certain as to whether this would change security behaviour in the long term, although it is unlikely to have a negative impact. On the whole - given the limited cost to Government - we will continue to pursue this option.
Other incentives	
Benchmark cyber behaviours with targets for improvement	A compulsory benchmarking scheme would be disproportionate to establish and then assess companies against standards for cyber security risk management, given the complexities and resource in arriving at a clear position on it, particularly for complex organisations. It could also create security risks for businesses if their strengths and weaknesses were publicly exposed. Furthermore, businesses have shown opposition to any schemes that appear overly bureaucratic or carry a heavy administrative burden, as such an approach might do. We will not pursue this option. However, research has shown businesses to favour schemes which enable them to compare their performance against their peers, while reputational risk has been identified as a strong motivating factor for action. Government will therefore explore other approaches to benchmarking with NCSC, such as identifying organisations that have made use of recognised health checks (as described above) and/or making use of the results of those health checks.

Appendix B: Key lessons from international evidence

It is clear that no single country has a conclusive answer on how best to incentivise businesses to manage cyber risk effectively, and the UK's business engagement strategy is among the more developed. Overseas regulations focus on CNI, and those which are outside of CNI cover the security of personal data. A number of countries are now beginning to develop cyber security strategies which include non-regulatory measures beyond CNI and data protection. National governments are also providing support and guidance to organisations, similar to the UK. No countries have implemented wider incentives such as tax breaks.

We sought international evidence on the measures in Annex A. Responses from governments and our research indicate that most of these measures are not in place in other countries. The exceptions are set out below. It should also be noted that all EU countries will be required to implement both GDPR and the NIS Directive. GDPR will further apply to organisations outside the EU that offer goods or services to EU citizens.

1. *Statements in annual reports*: No country mandates inclusion of statements on cyber risk management but the US Securities and Exchange Commission does provide guidance that these should be disclosed if they pose a risk to investors.
2. *Breach reporting*: Laws requiring reporting of breaches related to personal data exist in Canada, Australia, Netherlands, Sweden and 48 out of 50 US states.
3. *Insurance*: Insurance is not mandated in any country and is still a nascent industry, but is more developed in the US where the focus is on third party data breaches.
4. *Voluntary measures such as guidelines and standards*: Several countries provide guidelines and advice, such as Sweden, Singapore and Israel, that cover security standards, training for board members, and more technical aspects such as vulnerability assessments and penetration testing.

For all these measures there is no evidence on whether they have changed security behaviour in organisations.

Department
for Culture
Media & Sport

4th Floor, 100 Parliament Street
London SW1A 2BQ
www.gov.uk/dcms