Title: The Network and Information Systems Regulation 2018 **IA No:** N/A **RPC Reference No:** RPC-4066(2)-DCMS **Lead department or agency:** Department for Digital, Culture, Media and Sport **Other departments or agencies:** BEIS, DfT, DHCS, Defra, and HMT	**Impact Assessment (IA)** **Date:** 12/04/2018 **Stage:** Final **Source of intervention:** EU **Type of measure:** Secondary legislation **Contact for enquiries:** evidence@culture.gov.uk or Stuart Peters stuart.peters@culture.gov.uk
Summary: Intervention and Options	**RPC Opinion:** Green

Cost of Preferred (or more likely) Option

Total Net Present Value	Business Net Present Value	Net direct cost to business per year (EANDCB in 2014 prices)	One-In, Three-Out	Business Impact Target Status
£-402.59m	£-202.54m	£20.4m	Not in scope	Qualifying provision

What is the problem under consideration? Why is government intervention necessary?

The functions of our societies and economies are increasingly underpinned by the internet and private network and information systems. Hence it is important to ensure a high common level of network and information security (NIS). In the event of a security incident the owner of the network does not incur all of the losses to the economy and may therefore have a less than optimal incentive to invest in security. Increasingly network and information systems also contribute to cross-border movements of goods, services and people through interconnected systems such as the internet. Hence the disruption in one Member State can lead to potentially serious consequences in other countries.

What are the policy objectives and the intended effects?

The policy objective is to prevent (where possible) and improve the levels of protection against NIS incidents across the EU. Currently there is no overarching legislation or regulatory requirements covering all Member States, where some of these have developed solutions on a country by country basis. Hence the Commission considers that at the minimum an approach is required that leads to minimum capacity building and planning requirements, the exchange of information and coordination of actions as well as common security requirements for all market operators concerned to be able to respond effectively to challenges of the security of network and information systems.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

Option 1: Continue with status quo (individual Member State Activity) - 'Do Nothing' This option assumes that current arrangements on security, reporting and monitoring will continue either based on existing regulatory requirements or on a voluntary basis. This will act as a baseline for the remainder of the policy options.
Option 2: Introduce an EU wide regulatory approach 'Implementing the Directive'. The Directive will be transposed into UK law. The approach to implementing the directive is then compared to the 'Do nothing' case of making no changes to current arrangements. Alternatives to regulation have been considered by the commission at the negotiating stage. Non-compliance with the Directive would most likely lead to infraction proceedings by the EU. Hence voluntary measures were not considered in more detail as a further potential option.

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** Month/Year				
Does implementation go beyond minimum EU requirements?		No		
Are any of these organisations in scope?	**Micro** Yes	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded: N/A**	**Non-traded: N/A**	

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister: *Margot James* ***Date:*** *18 April 2018*

Summary: Analysis & Evidence

Policy Option 1

Description: Option 2: Implement the NIS Directive
FULL ECONOMIC ASSESSMENT

Price Base Year 2017	PV Base Year 2018	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: - 403.10	**High: -216.50**	**Best Estimate: -403.10**

COSTS (£m)	**Total Transition** (Constant Price)	Years	**Average Annual** (excl. Transition) (Constant Price)	**Total Cost** (Present Value)
Low	0.5	1	24.8	**216.0**
High	0.5		46.5	**402.6**
Best Estimate	0.5		46.5	**402.6**

Description and scale of key monetised costs by 'main affected groups'

Costs to businesses include familiarisation costs, competent authority costs, additional security spending, and administrative costs associated with reporting incidents and providing evidence on security risk assessments or audits to the competent authority. Costs to Government include the ongoing familiarisation costs, reporting costs, compliance costs, and miscellaneous additional cyber security spending.

Other key non-monetised costs by 'main affected groups'

Non-monetised costs include those to the NCSC in its role of single point of contact. Estimates for the initial security costs incurred by businesses are not included separately and may be included in businesses estimates of annual security costs.

BENEFITS (£m)	**Total Transition** (Constant Price)	Years	**Average Annual** (excl. Transition) (Constant Price)	**Total Benefit** (Present Value)
Low				
High				
Best Estimate				

Description and scale of key monetised benefits by 'main affected groups'

Other key non-monetised benefits by 'main affected groups'

The main benefits to the UK economy are improved protection of the network and information systems that underpin the UK's essential services; reducing the likelihood and impact of security incidents affecting those networks and information systems and the corresponding impact on economic prosperity. Businesses also may benefit from reduced breaches or attacks that are below the Directive thresholds. International cooperation and information sharing is also expected to improve advice and incident response for firms.

Key assumptions/sensitivities/risks	Discount rate (%)	
Data from the Cyber Security Breaches Survey is used to provide an indication of additional security spending, the proportion of businesses with a breach or attack, and illustrative benefits assuming a 5 percentage point reduction in the number of businesses with a breach or attack.		

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m: 79
Costs: **20.4**	Benefits:	Net: **-20.4**	

Responses to the comments from RPC issued on 11th January 2018

The RPC offered nine comments to the consultation NIS IA. Responses to some of the comments by DCMS is provided below:

i) ***Whether the directive affects the price of essential services and the number of workers employed by essential service providers.*** Responses from the consultation indicate, recruitment of additional staff and retraining of existing staff is one of the most significant addition to the operational costs of essential service providers. This is mentioned 'Estimating additional security spending', however, there is a lack of primary data collection on staff recruitment and retraining at firm-level due to which we are unable to estimate the exact impact of additional employment on prices of essential services. The Directive may have an upward impact on prices of essential services due to increases in familiarisation costs, administrative costs incurred by businesses which may be passed on to consumers. However, there is a scarcity of both primary and secondary-level data to model an accurate impact on consumer's prices as a result of implementing the NIS Directive.

ii) ***Whether the measures will have a disproportionate impact on small businesses***. There is no direct evidence that new measures under NIS regulation will have any disproportionate impact on small businesses. With one exception (in the digital infrastructure sector), no Operator of Essential Services is small or micro business, and small and micro businesses are specifically excluded from the digital service providers aspect of the Directive. According to the Breaches Survey, average spending by small businesses in cyber security is as low as £2,600.

iii) ***Whether costs will differ among essential service providers from different sectors (e.g. energy, transport and health care).*** We do not have primary data for cost comparison across sectors to estimate the extent and direction of cost variation across sectors. There will be some difference in approach between sectors, particularly in regard to cost recovery, where those sectors that are publicly owned (in particular the Health Sector) likely to face fewer demands for cost recovery by their Competent Authority. We estimate that the largest drive for cost differential, both between sectors and within sectors will be existing preparedness for cyber security, with those least prepared facing the highest cost burden.

iv) ***More details about implementation of the directive (e.g. how non-EU firms in the UK will be bound by the regulation, and why banking and financial sectors are exempt from the directive).*** The NIS directive applies equally to any non-EU firm in UK owned by overseas entities as to any EU firms. The determining factor for Operators of Essential Services is the service they provide in the UK, not their physical location, and for digital service providers, they must be established in an EU Member State in order to operate in the Single Market. As of now, there is specific guideline for non-EU firms indicating that their implementation requirements will be any different from EU firm). Banking and financial sectors are not exempt from the Directive itself, but the UK Government in its transposition planning has taken the decision to exclude these sectors as the UK already has existing legislation that meets the requirements and security measures set out in the NIS Directive.

v) ***Whether the IA has considered all the potential costs and benefits (e.g. the costly interaction between***

the NIS directive, general data protection regulation and the e-privacy directive, establishment costs for sectoral-competent authorities, and the increase in revenue of digital service providers from providing security services to essential service providers). Due to limitations in time and scoping of existing commissioned surveys by DCMS, monetisation of all potential costs and benefits has not been feasible. However, we are open to expanding the scope of our analysis in future to strengthen post-implementation evaluation. When considering the Government's transposition of the NIS Directive we have taken these factors into account. Where possible, we have aligned our approach with that of the General Data Protection Regulation (for example with incident reporting timelines) and are putting a requirement on competent authorities to take into account other legislation when considering any financial penalties, to minimise duplication.

vi) ***Whether some of the uncertainties will be resolved by the further consultation which, the RPC understands, the Government plan to conduct.*** The future (targeted) consultation was specifically aimed at digital service providers, as the EU's security and incident reporting requirements were not agreed at the time of the UK's public consultation. This targeted consultation was launched on 26 March 2018, following publication of the EU's requirements on 30 January. Given the late publication of the EU's requirements, the targeted consultation focuses on where the ICO, as Competent Authority for digital service providers, can best support industry in meeting the EU's requirements. It is our intention that responses to this targeted consultation will assist the ICO in reducing the burden on business by providing guidance and support tailored to address their concerns.

Problem under consideration

The Security of Network and Information Systems Directive (NIS Directive) was adopted by the European Parliament on 6 July 2016 (2016/1148). Member States have until 9 May 2018 to transpose the Directive into domestic legislation.

Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the UK economy.

The purpose of the NIS Directive is therefore to improve the security of network and information systems across the European Union, with a particular focus on essential services (energy, health, transport, water and digital infrastructure and finance) which if disrupted, could potentially cause significant disruption to the UK economy, society and individuals' welfare.

Network and information systems, and primarily the internet, play an essential role in facilitating the cross- border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the EU as a whole. The Commission state that the 'resilience and stability of network and information systems is therefore, essential to the completion of the Digital Single Market and the smooth functioning of the Internal market' (EC5, 2013, p. 3). It is for this reason that the NIS Directive also covers Digital Service Providers, although in a lighter touch manner, in order to reduce the burdens on businesses.

On 23 June 2016, the EU referendum took place and the people of the United Kingdom voted to leave the European Union. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will continue to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what arrangements apply in relation to EU legislation in future once the UK has left the EU. It is the UK Government's intention that on exit from the European Union these policy provisions will continue to apply in the UK.

The NIS Directive

The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- that Member States have in place certain mechanisms to support and promote national cyber security, such as a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
- improved cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. Member States will also need to participate in a CSIRT Network, in order to promote swift and effective operational cooperation on specific cyber security incidents and sharing information about risks;
- that there is a culture of security across sectors which are vital for our economy and society and which rely heavily on information networks, such as energy, transport, water, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as "operators of essential services" will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

Rationale for Government intervention

There are two key characteristics of networks information systems with respect to security and resilience which may prevent economically efficient decisions being made from a societal point of view on the level of security and which therefore, could require Government intervention.

Externalities: The network only functions and has significant benefits to customers if it is possible to interconnect. However, this also implies that security threats or impacts can affect other participants on this network as well. Hence it is important to maintain a certain level of resilience and security. The potential costs on others through the network though is usually not taken into account when companies consider how much to invest in resilience and security measures and practices. Through the interdependent nature of these networks, negative effects associated with these externalities can potentially also spread more widely, especially in the case of those that are relied upon to provide essential services that enable the economy to function.

Hidden information: Businesses do not have full visibility of the threat against them and therefore have a level of uncertainty as to what they should be doing to protect themselves. As

many cannot calculate accurately the cost or benefits to their business, cyber security may not always be considered a priority.

Therefore, Government intervention in this case might potentially be justified.

Evidence to support rationale for intervention

There is clear evidence showing internal costs to businesses resulting from cyber security breaches or attacks. The average cost to all businesses of all the breaches in a year was £1,570, though this rises to £19,600 for large businesses.[1]

Generally there is little evidence on the external costs of cyber security breaches or attacks and no evidence has been found on the costs of breaches that caused significant disruption to essential services. There is some evidence to support the presence of external costs resulting from data breaches. A US survey of consumers on their attitudes to data breaches found that 32% of respondents reported no costs of the breach and any inconvenience it garnered, while, among those reporting some cost, the median cost was $500.[2] A survey of credit unions in response to the data security breach at Home Depot stores in September 2014 found it cost credit unions nearly $60 million to reissue cards, deal with fraud and cover other costs.[3]

There is also an indication that suppliers are a contributing factor to some breaches. Among those that identified their most disruptive breach or attack, 4 per cent thought weaknesses in others security including suppliers was a factor that contributed to the breach or attack. Though only 13 per cent require their suppliers to adhere to any cyber security standards or good practice guides.[4]

The cost benefit analysis section explores in more detail the outcomes and impacts that result from breaches or attacks, indicating that in some cases these can be significant.

Cost benefit analysis

Summary of changes following consultation

This final impact assessment updates the analysis conducted prior to consultation. Consultation responses have been reviewed and used as the basis for cyber security spending estimates. Departments have refined their estimates of the number of essential service providers in scope of the Directive. This has meant it is no longer necessary to use the business population estimates as an upper bound. Compliance costs have been reviewed with revised estimates provided. Additional case studies have been included to demonstrate the types of incident the Directive is looking to address, building a better picture of the potential benefits.

We can confirm that the UK's implementation of the Directive will not go beyond the minimum requirements of the Directive. The UK Government is limiting the scope of its implementation to

---

[1] Cyber Security Breaches Survey 2017

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

[3] News report: http://www.mcun.coop/Communications_and_PR_29.html?article_id=711

Survey conducted by CUNA

[4] Cyber Security Breaches Survey 2017

those set out in the Directive, and where there is existing legislation that provides equivalent measures (such as in the finance and banking sectors) the Government is relying on those measures and not including them in the scope of its transposition. The proposed NIS Regulation implements only the minimum measures required by the Directive to comply with its provisions and does not expand on these.

Limitations of the calculations and estimates

While this impact assessment brings together evidence from a number of sources we would like to note there are still a number of limitations to the analysis.

The 'digital' domain is characterised by dynamic phenomena with heavy-tailed statistical distributions. Past outcomes are a poor guide to future outcomes. There are thus few simple and definitive answers and, where there are, there is no guarantee that the answers will remain 'true' in the future. These challenges inhibit the ability to measure and generate comparable results over time and across research methods.

At a more practical level, these methodological issues subsequently impede the ability to determine the probabilities and impacts of digital security incidents.

Cyber security also has a unique problem when it comes to requesting information from businesses and individuals in that they can only report attacks and breaches that are detected. Technical experts know that viruses and malware can embed themselves deep into IT systems making them hard to detect. Therefore reports from businesses on the scale and impact of the problem are likely to be underestimates.

The academic research base for cyber security is growing and private sector reports are frequent but do not always employ robust methodologies. From the literature review there seems to be very limited evidence on the effectiveness of measures to improve businesses cyber security.

A further limitation lies in the definitions used in the directive as there is not always data that directly relates to these definitions. This includes definitions for the businesses covered by the Directive and the thresholds at which incidents should be reported as required by the Directive.

Despite these challenges, the estimated figures presented in this impact assessment have been based on the best available data for the UK, and the responses to the public consultation, and our best efforts to align this with the definitions used. In some cases proxies are used, such as security measures, where principles and guidelines are still in development. The revised estimates in this enactment IA includes new cost recovery estimates from competent authority which will be passed from government to businesses.

The revised figures presented in this impact assessment are best available final estimates to date for potential costs and benefits under this Directive. One of the challenges we face are that the costs will be different depending on the cyber security readiness of businesses - those who already take cyber security seriously will face lower compliance costs as they should already have many of the requirements in place, whilst those who have yet to address cyber security effectively will face higher costs to become compliant.

Option 1: Do nothing - setting the baseline

This option reviews the current situation including the estimated number of businesses to be covered by the Directive, any existing requirements on firms to assess cyber risks or implement security measures, and the current level of investment in cyber security.

It is clear that doing nothing is not an acceptable option given the 2017 ransomware attacks on multiple networks. Also if we do not implement the Directive the UK risks infraction proceedings. Non-regulatory options were considered by the EU commission at the negotiating stage but not taken forward.

Number of businesses

Essential service providers

Operators in the sectors within the scope of the Directive are identified as providing an essential service if they meet the following criteria:

- an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.

The sectors in scope are summarised in the table below with a brief description outlining what may be considered an essential service. Full details for the thresholds determining which organisations are in scope is included in the consultation response.

Table 1: Summary of the sectors within scope and essential services provided

Sector	Sub-sector	Essential service	Relevant entities
Drinking water supply and distribution		The supply of potable water to households	Entities involved in the wholesale supply of potable water
Digital infrastructure		Provision of internet infrastructure service	Internet exchange points (IXPs) Domain name service providers (DNS) Top level domain name registries (TLD)
Energy	Electricity	Electricity supply Electricity distribution Electricity transmission	Electricity supply businesses, distribution and transmission companies
	Oil	Oil transmission Oil production, refining and treatment and storage	Oil pipeline (transmission), production, refining and treatment and storage businesses
	Gas	Gas supply	Gas supply businesses, distribution and transmission companies, storage and LNG operators, and operators of refining and treatment facilities
Health	Health care	Non-primary NHS healthcare services	NHS Trusts and Foundation Trusts
Transport	Air transport	Passenger air transport Cargo air transport	Airport managing bodies Traffic management control operators Air carriers
	Maritime transport	Passenger transport Cargo transport	Managing bodies of ports Passenger water transport companies Cargo water transport companies Operators of vessel traffic services

			Operators of port facilities
	Rail transport	Heaver rail passenger services (including international rail)	Licensed train operators which provide services on the national rail network under contract to a public authority. International rail services operators Operators of mainline railway assets
		Light rail and metro passenger service (including underground)	Light rail operators subject to regulation for security under the railways act 1993
		Road transport	Roads authorities

The consultation stage impact assessment mapped the Directive sector definitions against the Standard Industrial Classifications codes with the number of companies from the Business Population Estimates to provide an upper bound estimate of the number of companies that may be in scope. Since then Departments, Regulators and the Devolved Administrations have refined their estimates of the number of organisations in scope according to the thresholds set. This therefore negates the need to use the Business population Estimates, especially as the number of expected companies is only a fraction of the total business population. The figures presented in table 2 are taken as the best estimate of the number of companies providing essential services and subject to the directive, and will be used for calculations throughout the impact assessment.

Table 2: Departments' estimates of the number of businesses subject to the Directive

	Drinking water supply and distribution	Digital infrastructure	Energy[5]	Health	Transport
Micro/Small	0	1	0	0	1
Medium	1	2	2	0	13
Large	18	15	45	268	66
Total	19	18	47	268	80

The 268 estimated number of health sector organisations consists entirely of public organisations across the UK. Therefore any costs borne by these organisations due to the directive will be counted as costs to government and not included in the business impact target. Drinking water supply companies are made up to the 15 companies in England, two in Wales and the Scottish and Northern Ireland state owned providers.

Digital service providers

For digital service providers, only one member state will be responsible for each organisation. This means there is no duplication and businesses are only required to have contact with one point in the EU. Only businesses that have their head offices in the UK will be regulated by the UK.

Since the 2013 impact assessment the definition of digital service providers covered by the Directive has changed. Broadly it now covers search engines, online marketplaces, and cloud service providers. These are explained below with the definition as it is set out in the Directive (italicised) and our estimates of the number of firms in each. For all types of digital service

[5] Estimates of the number of energy companies relates to those in GB only.

provider only those businesses with 50 or more employees and a minimum of £10 million turnover are included, with all micro and small Digital Service Providers excluded from scope.

Search engines

'Online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

There is no identifiable source of official data on the number of search engines that either operate in the UK or that are established here. Therefore an online search was conducted to identify any search engines that may be covered by the Directive. This found seven companies that are registered and have their main offices in the UK. However, none was large enough to meet the size threshold of a digital service provider. It is therefore concluded that there are currently no search engines based in the UK that would be the subject of the Directive.

Online marketplaces

'Online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (1) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.

An online marketplace is defined as a platform that acts as an intermediary between buyers and sellers, facilitating the sale of goods and service. Online marketplaces are only in scope if sales are made on the platform itself. Sites that redirect users to other services to make the final transaction (e.g. some price comparison sites) are not in scope. Sites that only sell directly to consumers are not in scope (e.g. online retailers).

An online search was taken to identify online marketplaces in the UK. Following the consultation this was extended to ticket market places however most are based in other countries, particularly the US. In total we have so far identified three marketplaces that are likely to be the subject of the Directive with headquarters in the UK, with others such as Amazon, eBay and Etsy being based in other countries.

It should be borne in mind though that it was not possible to divide the aforementioned figures for market places and search engines from the internet search by company size and therefore, it is possible that the figures presented still include micro or small enterprises despite these small firms being excluded from scope. Furthermore, some of these companies are also likely to operate not only in the UK but also in other European countries or globally.

Cloud service providers

'Cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Cloud services can be broken down into one of three categories, those that provide infrastructure, platforms, or software as a service (SaaS). For SaaS operators, only business to business service providers will be included, and entertainment providers (such as Netflix or

online games) will be excluded. While no estimates are available of the number of businesses that operate in these categories we have obtained data that provides our best estimate. This shows that there are 129 businesses providing SaaS that meet the size definition and are headquartered in the UK. A further keyword search was conducted for "cloud" to identify other businesses with this in their description of services offered which identified a further 40 unique records. This gives a total of 169 businesses headquartered in the UK, with 50 or more employees and a turnover of £10m or greater.[6] It has not been possible to refine this figure further.

As with above some of these companies may operate in other European countries and globally.

Existing investment spending on cyber security by businesses

The Cyber Security Breaches Survey provides evidence that has been designed to be representative of the business population in the UK. If finds that 67 per cent of businesses spend some money on cyber security with the average amount spent being £4,590. This varies by size and sector as can be seen in table 3 and figure 1 below.

Table 3: Average investment in cyber security in last financial year

	All businesses	Micro/small[7]	Medium	Large
Mean spend	£4,590	£2,600	£15,500	£387,000
Median spend	£200	£200	£5,000	£21,200
% spending £0	33%	34%	13%	9%
Base	1,209	829	268	112

Source: Cyber Security Breaches Survey 2017

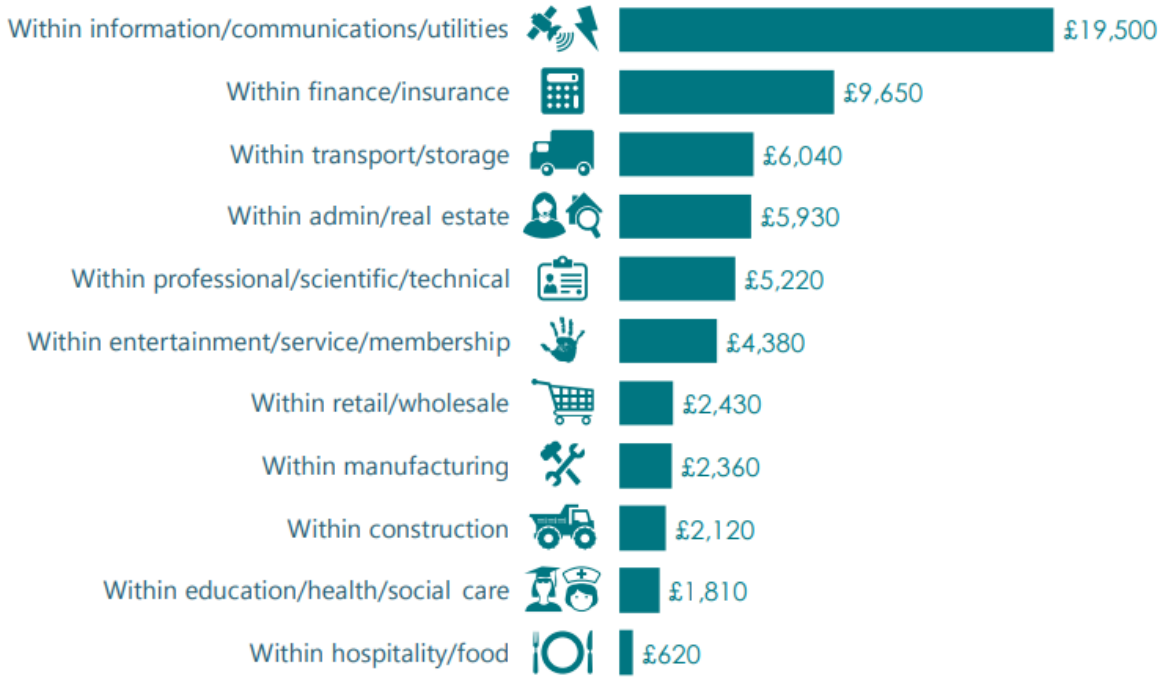
Looking at median spend figures, the typical micro or small business tends to spend a very small sum, just over what an annual subscription to antivirus or anti-malware software might cost, while the typical large firm spends at a level more akin to an individual's annual salary.

The variation in spending is much higher among large firms than others. This is likely to reflect the considerable sector differences with the largest firms having the capacity and choice to spend very large or relatively small amounts on cyber security.

[6] Sourced from Pink Book which records investment transactions by investor and company. Businesses are classified by industry sector and can also identify by industry vertical such as SaaS and cyber security.

[7] Micro and small firms have been merged to make this analysis more statistically robust.

Figure 1: Average investment in cyber security in the last financial year by grouping



Source: Cyber Security Breaches Survey 2017[8]

This is the best evidence available on cyber security spending in the UK but it does not provide a level of detail enabling a direct comparison with the sectors and sub-sectors covered by the Directive. This is due to the limitations of the sample size for each sector. It is this reason that analysis will focus on size differences rather than sectors.

The responses from the consultation about expected spending, discussed in option 2, indicate that these organisations are likely to be spending large amounts, placing them in the top end of the spending distribution, although companies did not provide details of their existing spending. Only a few consultation responses provided limited information on existing areas of spending with no information on current amounts.

Current regulations, reporting and security requirements

There are a number of existing regulations and requirements that need to be taken into account as part of the baseline and in conducting analysis under option 2. These are set out in full below.

New Data Protection Bill

A new Data Protection Bill, implementing the EU General Data Protection Regulation, will replace the existing Data Protection Act (1998) when it is implemented in May 2018. This will strengthen existing regulation and require reporting of all breaches of security that results in the loss, corruption or release of personal data to the Information Commissioner's Office (ICO). It is

[8] Bases: 96 administration or real estate firms; 83 construction firms; 131 education, health or social care firms; 87 entertainment, service or membership organisations firms; 350 finance or insurance firms; 93 food or hospitality firms; 140 information, communications or utility firms; 187 manufacturing firms; 126 professional, scientific or technical firms; 136 retail or wholesale firms; 94 transport or storage firms

expected that the new regulation will bring about an improvement to organisations security measures to protect personal data due to the significant fines that can be given for data breaches, and also because guidance will be provided on the level of security required to comply with the regulation. Consultation responses indicated businesses are already investing in security measures to comply with the new regulation. It is expected that the cyber security guidelines for Data Protection and the Directive will be similar as both are being produced by the NCSC.

It is also reasonable to assume that companies systems handling personal data will have the appropriate security requirements in place as they will be covered by Data Protection regulation. There will though be companies with both personal data systems and separate networks that don't process personal data who may have to invest in security in response to the Directive.

Data shows that approximately 61 per cent of the business hold personal data on their customers. It also indicates that of the 46 per cent of all businesses that suffered a breach or attack in the last year, only 4 percent of these resulted in the alteration, destruction or theft of personal data.[9]

While currently only a small proportion of businesses report their breaches or attack to anyone other than their IT or outsourced security provider (26%),[10] this is expected to increase with the new Data Protection regulation. Businesses will be required to report breaches that affect the rights and freedoms of individuals to the ICO with the following information provided after 72 hours from detection of the breach:

- Organisation details
- Description of incident
- Details of personal data at risk
- Containment and recovery, actions taken to minimise and mitigate the effect on data subjects affected
- Any training and guidance provided to staff on data protection
- Previous breaches reported to the ICO

Some of this information is very similar to that which would be required to be reported under a NIS incident. Therefore where breaches occur to systems with personal data that also disrupt the provision of an essential service we may consider that there is little or no additional reporting burden.

Current security requirements

As well as the new Data Protection Bill which requires personal data to be protected, there are a number of sector specific regulations and requirements that address the continued provision of services. While none address cyber security directly they cover risks to the essentials services provided. This can be used as an indication that any additional security spending as a result of the directive in option 2 may be lower for these sectors.

[9] Cyber Security Breaches Survey 2017

[10] Ibid.

Energy

It seems that UK energy companies could face limited extra costs, providing the Directive reporting rules are relatively flexible. However, it should be borne in mind that in terms of the regulations, licences, standards and codes of conducts that can be applicable in the energy sector, their meaning can depend on the purpose for which these have been specifically written. In some cases these could be applied to NIS incidents as well although they were not originally intended for this purpose and some examples of this are outlined below. Examples of the licences, standards and codes of conduct can be found on Ofgem's website for information (see https://www.ofgem.gov.uk/sites/default/files/favicon.ico)

For example according to the guidance for the Electricity, Safety, Quality and Continuity Regulations 2002 general duties are placed on 'generators, distributors, suppliers and meter operators to prevent danger, interference with or interruption of supply so far as is reasonably practicable' and to 'ensure their equipment is sufficient for the purposes in which it is used' (HMG, 2002, p. 6). In addition it specifies that 'generators and distributors are required to assess the risk of danger from interference, vandalism or unauthorised access associated with each substation and each overhead line circuit' (HMG, 2002, p. 6). It also requires them to assess the risk, record these and to take action to mitigate these as well (HMG, 2013, p. 6). These requirements could potentially cover NIS incidents as well although they were not originally intended or written for this purpose.

With respect to the oil and gas sector (upstream only) BEIS has a voluntary arrangement for terminal operators to report production losses of 10 million cubic metres of gas per day or more to the National Grid as well as BEIS. This applies to losses which could result from any cause including for example equipment failure and external events such as ship collisions or malicious acts but also for public interest events which may attract media attention. A crisis management plan outlines in detail the various responsibilities and reporting mechanisms in case of an energy emergency as well.

In the downstream oil sector, the Health and Safety Executive (HSE) have recently published their Operational Guidance on Cyber Security for Industrial Automation and Control Systems (IACS), which is intended to contribute towards a suitable demonstration of compliance with relevant H&S legislation in order to demonstrate cyber security risks have been reduced to as low as reasonably practicable.

Given the implied high scrutiny level already by regulation and the regulator, the current level of security spending could potentially be high already and some energy firms indicated this in the consultation. Consultation responses also indicated it was still uncertain to what extent further spending would be needed as it depends on the specific guidance provided to the sector.

Health

Organisations in the UK health sector could face limited additional costs, providing the Directive reporting rules are relatively flexible.

In England the NHS Standard Contract requires organisations commissioned by commissioners (clinical commissioning groups and NHS England) to provide clinical services other than primary care to adopt and implement the ten data security standards recommended by Dame Fiona Caldicott, the National Data Guardian for Health and Care. Further, the contract requires these

providers to comply with further guidance issued by the Department of Health, NHS England and/or NHS Digital pursuant to or in connection with those recommended standards.

Given the existence of this requirement it seems that most of the health sector is already required to have a suitable level of data security as well as a reporting and monitoring system in place. However, the actual impact of the Directive will depend on its final implementation. A more comprehensive assessment of whether companies in the health sector are likely to be already compliant with NIS will be possible once security principles and guidelines have been finalised.

Transport

Legislation is already in place to regulate the aviation, maritime and rail transport sectors to protect against security threats, specifically those associated with terrorism. These do not currently extend to cover the full range of cyber security threats and are generally limited to protection against acts of violence. Some regulatory requirements for cyber security are in place or in the process of being developed/introduced for parts of the rail and aviation sector. These regulations will be aligned with NIS and will, where possible, support organisations in meeting some aspects, but they do not cover all the organisations that are in scope of NIS, and in some cases NIS may introduce additional requirements. The Department for Transport also published guidance for other parts of the transport sector (for example, Cyber Security for Ports and Port Systems, 2016) which organisations are currently being encouraged to follow. it is not possible to fully assess the level to which organisations are currently meeting NIS requirements as this will depend on the final form of the implementation, specifically regarding the security requirements, detailed guidance and the incident reporting thresholds.

Option 2: Implement the Directive

In this section we will look to estimate the additional costs organisations may incur following implementation of the NIS Directive. It will also look at the potential benefits from increased security.

Costs

The costs of implementing and running the NIS regulation will be split between those falling on businesses and additional costs to government from enforcement activity with each of the costs below explored in detail:

- **Costs incurred by businesses** include (a) familiarisation costs, (b) competent authority costs, including compliance costs, (c) costs of incidence reporting, (d) responding to enforcement activities, and (e) additional security spending.

- **Costs to government** include (a) setting up Computer Security Incident Response Team (CSIRT), single point of contact, and a cooperation group, and, (b) delivering enforcement activities, and international cooperation.

Costs to Businesses

Familiarisation costs

Administrative costs will be incurred by businesses as they familiarise themselves with the legislation and its implications for their firm. The consultation did not specifically reveal familiarisation costs but indicated there would be increased activity in compliance. Compliance costs are discussed separately from familiarisation costs in a later section.

From consulting our own legal department, we estimate that the majority of firms in scope of the directive will require 6 hours of work from a lawyer to help the firm understand the legislation and the requirements it places on them. We estimate that a similar amount of time from lawyers and IT professionals will be required to help familiarise businesses with the guidance documents that are being provided by the government, for example the security principles and guidelines.

For each hour of time required for familiarisation from a lawyer, we estimate that half as much time (3 hours) will be required by senior managers/directors to digest the work of the lawyer, and to identify how their firm will comply with the legislation. This is similar to estimates set out in the Broadband Cost Reduction Directive impact assessment.[11]

The wages for the legal profession and Information technology and telecommunications directors are taken from the ONS's ASHE 2016. The median is used as it is believed to be the most representative wage (it's less skewed by outliers). Overhead charges of 30% are added to the wages, in accordance with the International Standard Cost Model Manual.

Table 4: Administrative costs of familiarisation

	Number of hours for familiarising with legislation	Number of hours for guidance documents	Hourly wage of advisor/ consultant (£)	Total cost per firm, including overhead charge (30%)
Legal profession	6	6	25.17	£392.65
Information technology and telecommunication directors	3	3	34.30	£267.54

The total familiarisation costs to businesses have been calculated using the business population estimates and departmental estimates for the sectors subject to NIS and for digital service providers.

[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/534185/2016-06-23_BCRD_IA_FINAL.pdf

Table 5: Total familiarisation costs by group

	Micro/small	Medium	Large	Medium/Large (DSPs)	Total
Essential service providers	£1,320	£12,544	£278,601		£292,465
Digital service providers	n/a	£660	£1,320	£111,572	£113,553

Competent Authority Costs

Under the proposed NIS Regulation costs incurred by Competent Authorities to regulate NIS in the UK will be passed on to the businesses sectors. The decision to transfer costs of operating competent authorities from governments to businesses was adopted in January 2018, after the submission of the consultation IA to the RPC.

The new amendments of regulatory costs of NIS have been made to reflect a change in the UK Government's approach. It was originally intended that all costs for regulating NIS would be met by UK or devolved Government departments. However, a number of Departments have decided to utilise the experience of existing regulators in their sectors to deliver regulatory oversight of NIS. Those regulators, such as the Health and Safety Executive and the Drinking Water Inspectorate, work on a full cost recovery basis. The move to use experienced regulators is a positive one from a policy perspective, as it ensures greater understanding of the sector by the regulator, but does mean that more of the costs of NIS will be met by industry rather than Government. Therefore, we needed to revise the Impact Assessment to take this into account.

The NIS Directive (Article 8(5)) requires that Member States ensure that Competent Authorities have adequate resources to carry out their duties. The proposed NIS Regulation provides a broad power to permit Competent Authorities to recoup reasonable recovery costs from those that they regulate. These costs can be recovered through a fees-based regime, direct charges for actual costs (e.g. the cost of appointing an auditor to investigate an incident) or a mixture of both.

A multiple competent authorities approach has been identified as the most suitable for the UK, allowing Lead Government Departments and regulators to build on their existing sector relationships and use their sector expertise to set guidelines and conduct enforcement activity. The competent authorities will be the main contact point for the operators in scope of the Directive and will be responsible for:

- identifying, with line ministries, operators that fall under the definition of NIS and who must comply with its requirements;
- publishing guidance on risk management, security guidelines and best practice;
- working with industry to assess and analyse the security standards in place, with powers to audit. (for Operators of Essential Services only)
- receiving incident reports from either NCSC or companies (to be decided);
- taking decisions on whether to make incidents public;
- enforcement of the Directive, assessing whether an operator is compliant, recommending remedial action, and as a last resort, levelling penalties.

There are expected to be between 9 and 13 competent authorities. This consists of 5 covering England and reserved sectors, the ICO who will act as CA for digital service providers, one in Northern Ireland, and one or more CAs in each of Wales and Scotland depending on whether they have a single or multiple competent authorities for the devolved sectors[12]. Each organisation is expected to require additional staff to enable it to carry out its functions as a competent authority. Lead Government Departments and the Devolved Administrations have provided their best estimate of additional resource from the information available. Some have provided an indication of the number of full time equivalent (FTE) employees they will require by level, while other such as Wales has indicated the total cost. The table below breaks down the CA costs transferred to businesses, by sector.

Table 12: Competent authority costs, transferred to businesses.

Competent authority sector	Competent Authorities (CA) - England	Expected FTE	Estimated cost of staff	Estimated total cost where staff resources have not been provided.
Transport (air, maritime, road)	Department for Transport, Civil Aviation Authority,	4.5	£954,647	
Energy (electricity, oil, gas)	BEIS and Ofgem (joined CA)	6	£415,054	
Digital infrastructure	Ofcom	4	£219,124	
Health	Department of Health	1.2	£57,956	
Drinking water supply and distribution	Defra	2.5	£646,154	
Digital service providers	ICO (UK wide)			£461,252 (plus £100,000 upfront costs)
Devolved Administrations (aggregated across sectors)				
Scotland	Scottish Government, Drinking Water Quality Regulator (Scotland)	5	£358,161	
Wales	Welsh Government			£480,000
Northern Ireland	Department of Finance (Northern Ireland)	8	£411,687	

Note: these are initial high-level estimates.

To calculate the staff costs salary bands for DCMS were used in lieu of average salary bands across the civil service which were not available, and salary bands were provided for the Scottish estimates. This includes national insurance and pension costs. Some departments only provided the total amounts they expected their CA to require which are set out in the right hand column.

[12] Both Wales and Scotland have responsibility for the water and health and transport sectors and are deciding between one competent authority or one for each sector. This also depends whether the Department for Transport acts as the CA for devolved administrations in this sector.

The estimated total cost of operating the competent authorities is therefore **£4,104,035 per year**. Only Defra and the ICO indicated its estimated one-off set up costs of £998,000 and £100,000, respectively.

The Civil Aviation Authority will act as competent authority for aviation who stated to incur costs of up to £500,000 for 4.5 FTEs which will be passed onto businesses through their charging regime. These costs have therefore been included in the total cost to business.

Other Competent Authorities are still exploring financing options. There is a potential for further Competent Authorities to pass on cost through their charging regimes though due to the uncertainty the costs are accounted as a cost to government.

Additional compliance costs of reporting to competent authorities

Nearly 20 percent of organisations responding to the consultation mentioned compliance costs when asked about whether the security principles would impose additional costs. While it is not yet clear on what level of evidence organisations will be required to provide to competent authorities to demonstrate they a meeting the requirements of the directive, respondents set out their expectations. These include providing evidence through auditing, providing risk assessments, certifications, and setting up new systems and processes to do this.

Only essential service providers will be required to provide evidence in this way to competent authorities. In order to estimate the expected costs associated with this activity we assume reports are produced by IT professionals where the costs are included in Table 8 with activities such as audits and conducting the risk assessment. To report to the competent authority it is expected the evidence and reports will be reviewed and discussed by senior management and legal professionals.

Table 8: Compliance administrative costs for essential service providers

	Micro/Small	Medium	Large
Number of hours			
Legal professional	1.5	5	10
Senior manager	2	7	14
Costs			
Legal professional	£38	£149	£297
Senior manager	£42	£126	£252
Total costs per organisation	£80	£275	£549
Total costs	**£160**	**£5,216**	**£231,703**

The total costs of providing evidence to the competent authority are estimated to be **£237,080**.

Additional security spending

This section explores the potential additional spending that organisations may need to undertake as part of demonstrating they meet the security principles and guidelines. Principles

and guidelines are the preferred approach in the UK as this gives flexibility to firms to implement security that is most appropriate for their network systems.

Security Principles

The principles and guidelines are still in development and the draft principles are set out in full in the consultation document. A summary of the principles is provided below:

a) appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to essential services. Covers: governance, risk management, asset management, and supply chain.
b) proportionate security measures in place to protect essential services and systems from cyber-attack. Covers: identity and access control, data and service security, information protection policies and processes, protective technology and staff awareness and training.
c) capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services. Covers security monitoring and anomaly detection.
d) capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary. Covers response and recovery plans.

It should be noted that these security principles will be similar to those proposed for Data Protection regulation and are expected to align to a certain extent with other existing standards such as ISO 27001. Where businesses have implemented security measures in response to Data Protection this may reduce additional security spending, if any, in response to the Directive. Even where these networks are separate from those providing the essential service, there may be spillovers due to an improved cyber security culture in response to Data Protection. The consultation responses indicates a number of firms are investing in response to the new Data Protection Bill with some outlining at a high level their planned investments in staff and IT network security. Respondents also indicated where they already comply with standards including ISO 27001. There is not enough data from the consultation to determine the proportion that have this standard in place, survey evidence suggests this could be around 7 per cent of all businesses, and could be higher in the sectors in scope of the Directive.

Additional security spending may also be limited where there are other existing requirements and standards and this will depend on the extent to which the principles go beyond what is already required. For example in the Health sector it is expected additional costs would be minimal as providers already have to meet security guidelines.

Areas of cyber security spending

Security spending in general may include any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, risk assessments, staff salaries, outsourcing and training-related expenses. All these areas of spending were mentioned in consultation responses with the most prevalent area of new spending being on staff resources. There was no specific mention of set up costs in responses though it would be reasonable to assume that there may be initial spending to bring some organisations up to standard to meet the principles. As set out in option 1, the current level of average spending for all businesses is £4,590, rising to £387,000 for large businesses though it is expected businesses providing

essential services will be at the upper end of the range in the survey. No source of data has been identified that breaks down security spending into the individual components outlined above and responses to the consultation were limited in number to provide a representative view.

The next two sections review the existing security measures likely to be in place and the costs of additional security spending in response to the Directive.

Businesses will be expected to demonstrate they have conducted an appropriate risk assessment and determined what security measures they need to have in place, and therefore if any new measures are required. This could include security audits conducted by the competent authority or an outsourced security provider. The administrative costs of providing evidence of risk assessments or audits is covered as part of the administration costs associated with enforcement section. The costs of actually conducting those assessments is included as part of the overall security spending analysed. Digital service providers are exempt from the requirement to demonstrate they have conducted risk assessments or audits and will only be subject to reactive enforcement by the competent authority.

Existing security measures in place

Any additional security spending by individual businesses will vary by the existing measures and technical controls they have in place, and the extent to which they judge the risks justify additional spending. Businesses commented in the consultation they have sufficient security in place to manage the commercial risks. They stated more information is needed to determine whether government's risk appetite is different from the commercial level, and therefore whether additional measures are needed.

The Cyber Security Breaches Survey asks businesses whether they have a number of different security measures or controls in place. For example the overwhelming majority of businesses across all size bands continue to have certain cyber security rules or controls in place. Nine in ten regularly update their software and malware protections, have configured firewalls, or securely backup their data.

Responses on security measures were mapped against 10 Steps to cyber security guidance to give an indication of the overall level of security practices in place. The guidance is intended to outline the practical steps that organisations can take to improve their cyber security. Table 6 brings together responses from across the survey. It shows that while most businesses have the technical controls, fewer have taken a more sophisticated approach in terms of senior-level risk management, user education and incident management.

Table 6: Proportion of businesses undertaking action in each of the 10 Steps areas

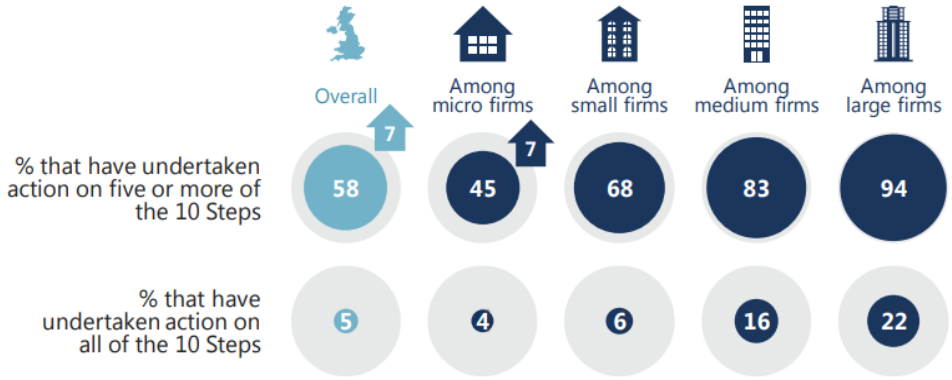
	Step description – *and how derived from the survey in italics*	**%**
1	Information risk management regime – *formal cyber security policies or other documentation and the board are kept updated on actions taken*	39%
2	Secure configuration – *organisation applies software updates when they are available*	92%
3	Network security – *firewalls with appropriate configuration*	89%
4	Managing user privileges – *restricting IT admin and access rights to specific users*	79%

5	User education and awareness – *staff training at induction or on a regular basis, or formal policy covers what staff are permitted to do on the organisation's IT devices*	30%
6	Incident management – *formal incident management plan in place*	11%
7	Malware protection – *up-to-date malware protection in place*	90%
8	Monitoring – *monitoring of user activity or regular health checks to identify cyber risks*	56%
9	Removable media controls – *policy covers what can be stored on removable devices*	22%
10	Home and mobile working – *policy covers remote or mobile working*	23%

Source: Cyber Security Breaches Survey 2017

As Figure 2 highlights, three-fifths (58%) of all businesses have undertaken action on five or more of the 10 Steps, which represents an improvement since 2016 (when it was 51%). However, very few have made progress on *all* the steps.

Figure 2: Progress in undertaking action on the 10 Steps by size of business



Source: Cyber Security Breaches Survey 2017[13] (diagrammatic arrows indicate changes from last year)

Estimating additional security spending

At the consultation stage the 10 steps to cyber security were used as a proxy for the measure that may be required to meet the security principles. It should be noted the NCSC state the NIS security principles will go beyond the 10 steps and may therefore require businesses to implement more stringent, and possibly more costly security measures.

While providing limited information on additional costs it is considered more appropriate to use consultation responses to provide an estimate of the total security spending likely to comply with the Directive.

Of the 108 organisations that responded to the question on whether they believe NIS security principles would impose additional costs, three quarters (74%) thought they would incur additional costs while 11 per cent stated no additional resources and 15 per cent said they don't know.

However, when asked whether they had plans to make additional security related investments as a result of the directive, only 43 per cent of the 102 respondents said yes. Nearly a third

[13] Bases: 1,523 UK businesses; 506 micro firms; 479 small firms; 363 medium firms; 175 large firms

(28%) replied no and the same proportion said they didn't know. Several businesses stated they already invest in cyber security and expected their existing measures to be sufficient, although that this would depend on the detailed guidance on requirements. Others said they planned further spending on security but that this was in response to other regulation, such as Data Protection, and the increasing threat landscape. Businesses also highlighted where they were compliant with ISO27001, further indicating that they are unlikely to incur costs beyond those incurred through compliance activity.

Digital service providers that responded stated that they already had sufficient security measures in place and therefore didn't expect any additional spending in this area.

Where businesses outlined their expected costs these were generally at a high level, in some cases indicating what this would be spent on including the number of additional staff, specific IT spending such as malware detection or systems monitoring, certification to appropriate security standards, training, and risks assessments or auditing. In some responses it was not clear whether figures provided related only to additional spending or the whole IT security budget. Additional spending ranged from at the low thousands to one or two exceptional cases where millions of pounds were anticipated to be required. It was most common for businesses providing essential services to expect spending between £50,000 and £200,000 per year. Digital service providers generally did not indicate any costs, with some indicating no additional spending on security.

Given these responses the table 7 sets out the estimated additional spending with high and low estimates. Descriptions are included to illustrate the scale of additional spending and are based on the information in consultation responses.

Table 7: Cyber security spending estimates by size and type of organisation.

	Micro/Small	Medium	Large	Medium/Large (DSPs)	Total
High estimated additional costs per business	£1,400	£75,000	£200,000	£50,000	-
Low estimated additional costs per business	£500	£50,000	£100,000	£5000	-
Comments	High costs - costs for implementing all of the 10 steps. Low costs relate to certification, for example cyber Essentials	High costs – two additional staff members. Low costs – hiring one additional staff member and investing in IT software changes. Both estimates include any additional risk assessments/audits and training staff.	High costs – three new staff members, investment in operation technology security (new software protection), testing and monitoring systems, training staff, risk assessments. Low costs – Two new members of staff, testing and monitoring, training and risk assessments.	DSP additional costs are reduced from Large essential service providers as it is not clear how many are either medium or large, and it is expected that they are more likely to have appropriate security measures in place.	-
Percentage of organisations expecting to make additional investments	One company has been identified, percentage figure is not applied	43%	43%	43%	-
Number of essential service providers	2	19	422	-	443
Number of digital service providers	n/a	-	-	172	172
Total additional costs (**high** estimate)	£2,800	£612,750	£36,292,000	£3,698,000	**£40,605,550**
Total additional costs (**low** estimate)	£1000	£408,500	£18,146,000	£369,800	**£18,925,300**

There are some caveats to the above. First, as already stated the security principles may go beyond the 10 steps so higher spending may be required. Second, the security principles are closely aligned to GDPR security principles and ISO 27001. For businesses that are already complying with GDPR and have already implemented the ISO standard the additional security spending may be significantly lower.

Spending varies by sector and with existing sector requirements on risk assessments and provision of essential services in health[14], transport and energy, security spending may not need to increase as much in response to the directive as those with no existing requirements. It is therefore difficult to tell how close the estimates are to likely additional security spending, though it is thought given overlaps with other requirements the high estimate represents a reasonable upper bound. This figures above also relate to ongoing annual spend as responses did not provide enough information to break out one off costs.

Incident reporting

This section estimates the additional costs businesses will face due to the incident reporting requirements included in the Directive. It first looks at the potential number of cyber security incidents that will need reporting, and then at the costs of making a report to the competent authority. This makes note of any other reporting that a business would have done already, for example under the Data Protection Regulation and existing reporting to the NCSC.

Incident reporting is intended to highlight incidents that may lead to, or have a significant disruptive effect on the provision of an essential service. The aim is to prevent such a disruption which could have wider economic or societal impacts. There will be some incidents that are generic to all network and information systems, and others that are specific to individual sectors. For each sector, the definition of what is a significant disruptive effect will be different, depending on the nature of each sector. For example it could be loss of supply to a certain number of customers or loss of a percentage of national energy supply.

Number of incidents

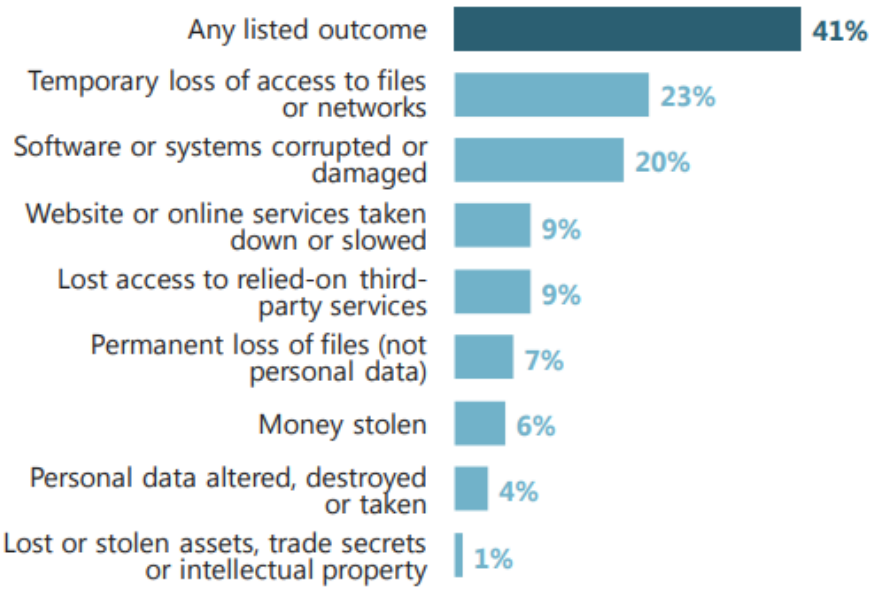
The threshold for incident reporting is specific to each sector covered by the Directive. However there is no known available source of data on the number of incidents that aligns with these definitions and therefore we have not attempted to estimate the number of incidents at the sector level.

Just under half of businesses (46%) identified a breach or attach in the last year. For medium and large businesses this figure rises to around two thirds (66% and 68% respectively). However not all breaches result in an outcome, or have an impact on the business. Four in ten businesses (41%) who experienced at least one breach in the last 12 months report an outcome. To put this another way, one in five of all UK businesses (19%) say they have experienced a breach resulting in some sort of material loss as highlighted in figure 3.[15]

[14] Health organisations make up the majority of essential service providers and while recent reports indicate they need to do more to implement basic security measures, they are already required to have these protections as part of their data security standards. Therefore the Directive is not expected to impose significant additional burdens.

[15] Cyber Security Breaches Survey 2017

Figure 3: Outcome of breaches among those who identified a breach in the last 12 months



Source: Cyber Security Breaches Survey 2017

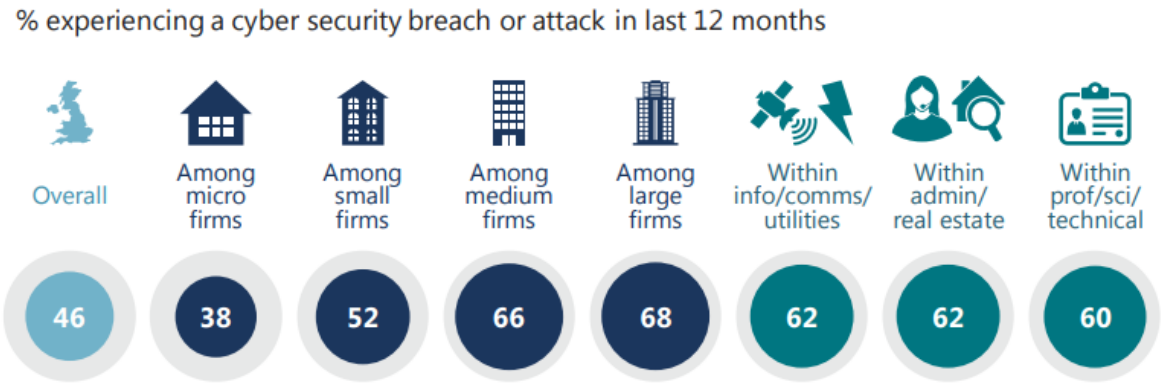
We can narrow down the list of outcomes posed in the Cyber Security Breaches Survey to those that seem to have the greatest link to network security and the provision of an essential service. This includes just over two in ten (23%) breaches or attacks that resulted in a temporary loss of access to files or networks, one in five (20%) had software of systems that were corrupted or damaged, 9 per cent had their website or other online services taken down or made slower, and 9 per cent that lost access to any third party services, and 7 per cent that permanently lost files (other than personal data).[16]

Businesses were also asked about whether the breach or attack impacted their organisation. Impacts asked about included for example, additional staff time to deal with the breach or attack, new measures to prevent future breaches or attacks and preventing staff carrying out their day to day work. The most relevant response code to the Directive is the breach or attack prevented provision of goods or service to customers (7% of those that identified a breach).

Analysis of the data for these outcomes provides an estimate of 17% of all businesses that identified a breach or attack that resulted in an outcome relevant to the Directive or prevented the provision of goods or services. This can be broken down by size of business as shown in figure 4.

[16] Ibid.

Figure 4: Businesses that identified a breach that resulted in an outcome relevant to the Directive



Source: Cyber Security Breaches Survey 2017 analysis[17]

We make the assumption that some of these breaches or attacks would be significant enough that they are considered an incident under the NIS Directive. As mentioned this figure is unable to take account of the different incident thresholds for each sector and is likely to include breaches that are not NIS reportable incidents. It should also be noted that some breaches above the NIS thresholds will also lead to the alteration or loss of personal data. This will result in simultaneous reports to the ICO and relevant NIS competent authority. The reporting requirements under the new Data Protection Bill to the ICO are expected to require more administrative input that those for NIS incidents. Thus in these cases there will be no additional costs of reporting as the Data Protection Bill is taken as the baseline. The estimated proportion of businesses required to report NIS incidents is therefore likely to be an overestimate.

The total number of incidents is harder to estimate as the Breaches Survey asked businesses to estimate the total number of all breaches or attacks. Respondents are likely to include breaches and attacks that don't result in an outcome or have no impact on the business. It is unclear from the survey why there is no impact but there are a number of likely reasons such as firms systems automatically detect and reject the attack or staff recognise the attack and report it. The data also shows that a large number of businesses experiencing a breach or attack reported no financial costs, in part supporting the hypothesis that most do not have an impact but it could also be because businesses find it hard to estimate the monetary value of loss. Only 6 per cent have in place processes to monitoring of the costs.

The mean and median number of breaches or attacks reported in the survey is summarised in the table below for all breaches and for those with an outcome relevant to NIS (for all businesses not just essential service providers).

[17] Bases: 1,523 UK businesses; 506 micro firms; 479 small firms; 363 medium firms; 175 large firms; 140 information, communications or utilities firms; 96 administration or real estate firms; 126 professional, scientific or technical service firms

Table 9: Average number of breaches among those that identified a breach or attack in the last 12 months

	All businesses	Micro/small [18]	Medium	Large
	All breaches			
Mean number	998	891	2,258	7,997
Median number	2	2	4	8
Base	757	414	230	113
	Breaches with an NIS outcome			
Mean number	150	51	1255	4293
Median number	1	1	2	8
Base				

Source: Cyber Security Breaches Survey 2017 analysis

This shows that the mean number[19] of breaches or attacks is substantially higher than the median number. What this indicates is that the typical business is likely to only experience a handful of breaches in the space of a year, but that a minority experience hundreds of breaches or attacks in this timeframe. Of course, a very small number of businesses are experiencing considerably more, indicating hundreds or even thousands of breaches per week.

Given the thresholds for reporting a breach under the Directive are expected to be set to exclude most small scale attacks it seems sensible to take the median number of breaches or attacks for this analysis. From the estimated 443 essential service providers and 172 digital service providers and the information above, there may be up to 1348 incidents. The detailed analysis by firm size is summarised in table 10 below.

Table 10: Number of incidents under NIS for essential service providers and DSPs

	Micro/Small	Medium	Large	Medium/ Large[20]	Total
Proportion having a breach or attack that results in an outcome	17%	31%	33%	32%	Weighted average 17%
Number of breaches or attacks per business	1	2	8	4	Weighted average: 1
Number of expected incidents under NIS					
Essential service providers	0.3	12	11	-	1126
Digital service providers	N/A	0.6	5	216	222

[18] Data from micro and small firms have been combined to align with the similar analysis on spending data in Chapter 4.

[19] It should be noted that the mean results here are driven up by a very small number of respondents across all size bands reporting an extremely high number of breaches in the past year (in the thousands). The median figures are therefore also shown to give a sense of what the typical business is likely to face.

[20] This category captures businesses that are medium or large but where the specific size group is not known.

As a lower bound we used data from the National Cyber Security Centre (NCSC) on incidents reported voluntarily. For the four months period between 1st October 2016 and 31st January 2017 there were a total of 188 incidents recorded by NCSC. These are assigned to one of three different categories[21]:

- category 3 incidents - NCSC routine operations: may include sophisticated network intrusion, cybercriminal campaign for financial gain, or the large scale posting of personal employee information;
- category 2 incidents - A significant incident or threat requiring coordinated cross-government response; and
- category 1 incidents - national emergency - an incident or threat which is causing or may cause serious damage including loss or disruption of critical systems or services.

There were 176 'category three' incidents, 12 category two incidents and no category one incidents.[22] This may include incidents reported by sectors out of scope of the Directive. We assume that category one and two incidents are the most likely type to be covered by NIS as having significant disruptive effects and therefore required to be reported. Using these figures and scaling up for the whole year gives just 39 incidents per year.

Costs of reporting

This is estimated based on the actions required to notify the competent authority that an incident has occurred. Actions required to minimise the effects of the impact on the provision of essential services are not included as it is assumed that these would be carried out as part of normal business, and may include support from the NCSC.

The cost per incident is estimated based on the amount of time it would take to gather the information required, process it through the relevant clearances such as legal and send to the competent authority.

The information required is basic (and similar to that required for the new Data Protection Bill set out above) and therefore it is not expected to take long to collect and collate. We have assumed 45 minutes of an IT professional's time to collect and present the information. For clearances we assume the same time again for lawyers and 20 minutes for managers or senior directors to approve the notice.

The Annual Survey or Hours and Earnings has been used to obtain the median average gross hourly earnings for the three occupations above. This is summarised in table 11 below.

Table 11: Incident reporting wage costs

Occupation	Median hourly wage	Time spent on incident notification	Total cost of incident notification (including 30% uplift)

[21] The NCSC has launched a new categorisation system consisting of six categories on 12th April 2018. As a result, any re-categorisation of incidents already mentioned in this impact assessment will be reflected in future post-implementation publications due to time limitations.
[22] Some incidents may get reclassified as more information is gathered during the response to the incident.

Information technology and telecommunications professionals	£20.95	45 minutes	£20
Legal professionals	£25.17	45 minutes	£25
Corporate managers and directors	£21.24	20 minutes	£9

Median hourly wage source: ONS - Annual Survey of Hours and Earnings, 2016 provisional estimates.

The total costs include a 30% uplift in the hourly wage to reflect non-wage costs such as accommodation and IT.[23] This gives a total cost of **£54 per incident reported**.

Total cost of incident reporting

The total cost for all expected incidents is therefore **£72,921** per year. This breaks down as £60,904 for essential service providers and £12,017 for digital service providers.

Using the number of incidents recorded by NCSC (39) this gives a **total cost of £2,110.** However as it is not clear from the NCSC data how many incidents would have already been recorded, and may in fact also have led to the loss or alteration or personal data.

Other administrative costs from enforcement activity

Firms that have had an incident may be required to engage with the relevant competent authority if there is further investigation into the incident. This may entail providing further information following initial reporting as more becomes known about the incident and any effects it has had on the provision of the essential service. Given the uncertainty and lack of detail about what this activity might entail for businesses it has not been possible to quantify or monetize the burden to businesses.

It should be noted that where incident response activity involves the NCSC, this is considered as part of normal business as it would happen regardless of the Directive being in place.

Costs to Government

The NIS Directive requires a number of institutions and groups to enable the regulation to function. The costs to government includes setting up the Computer Security Incident Response Team (CSIRT), single point of contact, and a cooperation group.

Of these the only additional costs that are expected to arise are from the competent authority that will enforce the regulation, and act as the single point of contact. The UK already has a cyber emergency response function in the form of Cyber Emergency Response Team which is part of the NCSC. CERT already forms part of a network with other CERTs globally and is therefore understood the have the necessary communication infrastructure as required by the Directive. The cooperation group is expected to require minimal additional resource.

Single point of contact

Each Member State is required to designate a single point of contact to act as a liaison on NIS matters within the EU and between different national competent authorities. The single point of contact's core tasks will include preparing a summary report of incident notifications and

[23] This is in accordance with the OECD International standard costs model manual.

forwarding cross-border incidents to the single points of contact in other Member States. The National Cyber Security Centre is proposed as the Single Point of Contact.

The NCSC has not provided any estimate of additional resourcing requirements to carry out this function. It is expected there will be some set up costs, for example producing guidance on security measures, and ongoing costs of handling incidents.

Total costs of implementation

The total **set-up costs** for option 2 is £23,410,341 for government, and £32,483,885 for businesses, in **year 1**. Annual ongoing costs to businesses are £21,786,176 (from Year 2) in the high estimate (considered a best estimate to be conservative though is likely to reflect the upper bound), and **£11,629,926** in the low estimate.

Table 13: Total one-off and average annual costs (indicated for year 1 and high costs).

	Familiarisation /one-off costs	**Additional security spending**	**Compliance reporting**	**Incident reporting costs**	**Competent authority costs**	**Total (year 1)**
Costs to business						
Essential service providers	£115,534	£13,859,550	£89,932	£22,642	£14,572,657	£28,660,315
Digital service providers	£113,553	£3,698,000	N/A	£12,017		£3,823,570
Total costs to business	**£229,087**	**£17,557,550**	**£89,932**	**£34,659**	**£14,572,657**	**£32,483,885**
Costs to government						
Essential service providers	£176,931	£23,048,000	£147,148	£38,262	£0[24]	£23,410,341
Total costs to government	**£176,931**	**£23,048,000**	**£147,148**	**£38,262**	**£0**	**£23,410,341**

Benefits

This section explores a number of potential benefits from implementing the Directive.

The key benefit of the Directive is expected to be an improvement in security that leads to a reduction in the risks posed to essential services relying on networks and information systems. This in turn will benefit the UK's economic prosperity as we rely on these services to support economic output. It is expected these benefits derive from both a reduction in the number of incidents that have significant disruptive effects due to improved protective measures, and by a reduction in the impact where appropriate incident response plans are put in

[24] 'Competent authority cost' element under Costs to Government has been moved under Costs to Businesses.

These two expected benefits of the Directive are explored from the perspective of the whole economy, (in other words the benefits external to the companies in scope of the Directive) and to individual businesses in scope.

Further benefits are also expected in the cooperation of member states through information sharing.

External benefits of reduced breaches (economy level)

Given that information networks are now pervasive in our economy, cyber breaches that disrupt these networks can have consequences for those using or relying on the networks to provide essential services. This includes households, businesses, and public sector organisations and these aren't restricted in geographic area. In the 2017 World Economic Forum Global Risks report, a massive incident involving data fraud and theft was ranked 5th in terms of probability.[25]

The frequency of breaches that result in an incident with a significant disruptive effect are expected to be very low. It is therefore difficult to find evidence of impact from such incidents and the potential benefits if such an incident was prevented due to better security. The insurance industry also finds it challenging to accurately model expected losses due to limited data and the nature of cyber security breaches meaning the impacts can be far reaching.

Due to the number of sectors covered and the complexity and number of different significant disruptive effects it is not reasonable to consider the benefits of each sector in turn. As incidents that cause a significant disruptive effect are low in frequency two case studies are used to show the scale of the potential benefits if such an incident were avoided due to better security and that these benefits could be substantial.

Case study 1: Ukraine power grid hacked

On the 23 December 2015 three power distribution companies suffered from a sophisticated cyber attack that led to 225,000 residents being without power. Power was lost for between one to six hours for the areas hit, but while the outage wasn't long more than two months after the attack control centres were still not fully operational according to experts. The attack used a number of approaches to gain access and cause disruption and destruction. While this attack is not representative of the risks to networks in the UK it does provide an indication of the scale of disruption and economic impact a successful attack can result in.

If one incident of this scale is prevented, benefits through the avoidance of costs are expected to be significant and an order of magnitude greater than the costs borne in implementing measures to comply with the Directive's requirements.

Further insight is provided in research that modelled the economic costs for a sophisticated cyber-attack on the electricity distribution network in the South East of the UK. The modelled scenarios show a loss of electricity supply from an attack affecting between 9 million and 13 million electricity customers. The knock on effects include disruption to transportation, digital communications, and water services for 8 to 13 million people.

[25] http://reports.weforum.org/global-risks-2017/the-matrix-of-top-5-risks-from-2007-to-2017/

The economic losses to sectors were modelled to be in the range of £11.6 billion to £85.5 billion in the different variants of the scenario. The overall GDP impact of the attack amounts to a loss between £49 billion to £442 billion across the UK economy in the five years following the outage, when compared against baseline estimates for economic growth.[26]

Case study 2: WannaCry ransomware attack

In May 2017 ransomware given the name WannaCry hit hundreds of thousands of computers across the world. This included computers at 81 out of 226 NHS trusts which included:

- 37 infected and locked out of devices, and
- 44 not infected but reporting disruptions. For example these trusts shut down their email and other systems as a precaution meaning they had to use pen and paper for activities usually performed digitally.

While patient data was not lost and lives were not put at risk, thousands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments. This incident highlights the potential for significant disruption which could have gone on for much longer and could have been prevented with software updates.

Internal benefits to businesses

The average costs to businesses of all cyber security breaches or attacks in the last year was, £1,570 (this does not include wider costs to the economy). As Table 14 shows, larger firms tend to incur much more substantial costs from all the cyber security breaches that they experience, possibly reflecting that they may be incurring more complex or challenging breaches, or have more sophisticated systems that are harder to repair.[27]

The median cost of all breaches is zero, reflecting the fact that the majority of breaches have no actual outcome. Considering only breaches with an outcome,[28] again it can be seen that larger firms incur more substantial costs.

The mean cost of breaches is substantially higher than the median cost. This highlights that the majority of businesses do not experience breaches with significant financial consequences, but for the minority of firms that do experience these serious breaches, the costs can be extremely high.

It is worth noting that the lack of certainty around the likely cost of any breach can make it difficult for businesses to fully understand the return on their investment in cyber security. Businesses are likely to underestimate the costs of breaches, and only 6 per cent have monitoring of the financial costs in place.[29] This is in part because a cyber security breach in theory could affect all parts of the business that rely in some way on information flows over

[26] Integrated infrastructure: cyber resilience in society, Cambridge Centre for Risk Studies, 2016

[27] Cyber Security Breaches Survey 2017

[28] This is all outcomes asked about in the Survey and not those limited to relevance with NIS.

[29] Cyber Security Breaches Survey 2016 and 2017

networks. This can included lost staff time, damaged or destroyed physical assets or the loss of data.

Table 14: Average cost of all breaches identified in the last 12 months

	All breaches			
Mean cost	£1,570	£1,380	£3,070	£19,600
Median cost	£0	£0	£0	£1,470
Base	737	413	218	106
	Breaches with an outcome			
Mean cost	£2,330	£2,070	£5,950	£13,200
Median cost	£300	£300	£1,000	£8,230
Base	321	167	102	52

Source: Cyber Security Breaches Survey 2017

Determining whether security measures implemented by businesses will lead to a reduction in the number of breaches is difficult. Little research has been conducted to quantify the link between good cyber security and the number of breaches. It faces challenges of limited data, and that not all breaches are detected, even by those with state of the art cyber security. The relationship between security measures and breaches is also not always in the direction expected.

The Breaches Survey 2016 found that firms who spend money on cyber security were more likely to have identified breaches or attacks.[30] This positive association was also found in research that investigated the relationship between board level technology committees and reported security breaches.[31] If found that boards with technology committees are more likely to have reported breaches in a given year, than those without technology committees. This could be because the technology committees are relatively young and also due to external breaches. As technology committees become more established, its firm is not as likely to be breached.

One piece of laboratory research found that the Cyber Essentials measures would mitigate 99 per cent of commodity exploits across a number of different IT systems setups that were modelled. A commodity exploit targets known vulnerabilities and with tools available online do not require extensive specialist knowledge to conduct.[32]

Assuming the avoidance costs of breaches is proportional to the level of security measures in place, the benefits of the Directive to the individual firm will depend on the security measures in place before the Directive. For example if a high level of cyber security and resilience already exists the potential benefits from increasing it further are likely to be relatively small for the businesses.

[30] Cyber Security Breaches Survey 2016

[31] Julia L. Higgs, Robert E. Pinsker, Thomas J. Smith, and George R. Young (*2016*) The Relationship between Board-Level Technology Committees and Reported Security Breaches. Journal of Information Systems: Fall 2016, Vol. 30, No. 3, pp. 79-98.

[32] Lancaster University: Cyber Security Controls Effectiveness: a qualitative assessment of Cyber Essentials. http://eprints.lancs.ac.uk/74598/

Benefits of improved information on attacks and breaches

There is expected to be greater information sharing on threats and vulnerabilities as well as attacks and incidents through the cooperation group with each EU member state represented. This information may help reduce the scale of impact, for example through implementing preventative measures in other member states, and also the likelihood of attacks becoming successful through updating guidance and advice to businesses.

Conclusions

While it has not been possible to quantify the benefits for use in the cost benefit analysis it is clear that these could be substantial where even just one significant incident is prevented. The recent events following the 2017 ransomware attack demonstrate a need for improved security and that there are likely external costs from the unavailability of network information systems.

The costs of implementing the Directive largely fall to businesses and certain public sector organisations such as NHS trusts. The largest proportion of these costs is additional security spending. Administrative costs in the initial reporting of a breach are fairly small and will be smaller still if the breach is already required to be reported under data protection regulations. The costs of providing evidence to competent authorities have been estimated though this will depend on the detailed guidance to be set out. Cost to government are focused on the set up and running of the competent authorities and the NCSC's function as single point of contact.

The main expected benefits are a reduction in the level and scale of cyber security breaches. This has benefits for the companies controlling the networks, other organisations operating on the network and the wider economy where breaches would otherwise disrupt everyday activity.

As there are insufficient data and models to estimate the expected benefits, the best estimate of total net present benefit value of option 2 is **-£402.59 million** (equivalent to the low estimate), assessed over 10 years. The high net benefit estimate based on the lower estimates of cyber security spending is -**£215.98 million**. It is not felt the negative NPV is a good reflection of the overall benefits of the regulation so it should be viewed in the context set out in this impact assessment.

Small business assessment

Micro and small businesses are only subject to the directive where they are in a sector within scope and providing essential services that if disrupted due to network outage will cause significant impact. This is justified because of the potential for a significant disruptive effect to an essential service caused by a network outage and the resulting impact this could have for the economy and life. Micro and small businesses are not included in the definition of Digital Service Providers.

Only two micro/small essential service providers have been identified by Departments, one in the transport sector and one in digital infrastructure. The costs have been calculated using the same source information as set out above[33] and are summarised in the table below.

[33] Including the Cyber Security Breaches Survey and other estimates from the consultation.

	Micro/Small
One-off transition costs	£1340
Ongoing annual costs (high)	£2,979
Ongoing annual costs (low)	£1,179
Total present value costs over 10 years	£300,000

The overall net present value over ten years to small businesses is £-0.03 million.

The Breaches Survey indicates that smaller businesses spend less on average than larger businesses and therefore the additional security spending is estimated to be a lot lower than for larger businesses. The security principles and guidelines approach will enable businesses to take a risk based approach to security and will be designed to be proportionate to the nature and scale of the business operations. Costs also only relate to those systems that the essential service relies on. The additional costs will also depend on whether they have put in place security measures to comply with the new Data Protection Bill or other existing requirements.