Title: Network and Information Security Directive **IA No:** **BIS ShEx 001** **Lead department or agency:** Department for Business, Innovation and Skills (BIS) **Other departments or agencies:** Cabinet Office, DfT, DH, DECC, HMT,	**Impact Assessment (IA)** **Date:** 20/09/2013 **Stage:** Development/Options **Source of intervention:** EU **Type of measure:** Primary legislation **Contact for enquiries:** Caroline Lehmann CyberSecurity@bis.gsi.gov.uk

Summary: Intervention and Options

RPC Opinion: RPC Opinion Status

Cost of Preferred (or more likely) Option				
Total Net Present Value	**Business Net Present Value**	**Net cost to business per year** (EANCB on 2009 prices)	**In scope of One-In, One-Out?**	**Measure qualifies as**
£-131.5m	£-131.5m	£15.28m	No	NA

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

Increasingly functions of our societies and economies are 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), which is the aim of the Directive proposed by the European Commission. 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 and public administrations 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 'Implementing the Directive' option assumes that the measures in the proposal for an EU NIS Directive is implemented into UK law. These proposals are then compared to the 'Do nothing' case of making no changes to current arrangements. Alternatives to regulation have been considered but if the NIS Directive is passed at EU level then 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?			N/A		
Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base.	**Micro** No	**< 20** 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 SELECT SIGNATORY: ..... Date: .....

Summary: Analysis & Evidence

Policy Option 1

Description: Option 2: Introduce the NIS Directive in the UK

FULL ECONOMIC ASSESSMENT

Price Base Year 2012	PV Base Year 2012	Time Period Years 1	Net Benefit (Present Value (PV)) (£m)		
			Low: Optional	**High:** Optional	**Best Estimate:** -£131.5m

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low				
High				
Best Estimate				**-£992.1m**

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

Additional security spending. Main affected groups: energy sector, health sector, transport sector, finance sector, information society enablers and public administrations. These costs could be considered to be transitional as lower costs might need to be incurred in following years as a higher security level only needs to be maintained rather than established. However, given technology developments and a lack of detail in the Directive, this is rather difficult to estimate for future years.

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

Additional administrative costs due to monitoring of networks and information systems and reporting of incidents, costs to establish the national competent authority, monitoring and enforcement costs: Main affected groups: energy sector, health sector, transport sector, finance sector, information society enablers and public administrations.

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low				
High				
Best Estimate				**£860.6m**

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

Potential benefits might arise assuming that the Directive leads to a reduction in the costs associated with security incidents. Main groups affected: energy sector, health sector, transport sector, finance sector, information society enablers and public administrations. The benefits depend on a variety of assumptions and this should be borne in mind. The best guess assumes that between 5,000 and 10,000 small companies achieve medium benefits for 50% of the incidents that they suffer from. .

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

Other potential benefits could be derived from preventing crimes using the information that was stolen if actions can be taken to prevent these, wider benefits to the UK economy due to becoming a safer cyber environment to do business, benefits from information sharing across EU Member States. Main groups affected: consumers, other businesses in the UK.

Key assumptions/sensitivities/risks **Discount rate (%)** N/A

Proxies had to be used to provide indicative figures for the potential security spending and associated additional costs as well as for potential benefits. The key reason for this is the lack of information/ data in this space as well as a lack of detail in the Directive. Hence the values included here should only be seen as indicative and not as final. Key assumptions and limitations of the data used are outlined in detail on pp. 12-13.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			In scope of OIOO?	Measure qualifies as
Costs: 115.3	**Benefits:** 100.0	**Net:** -15.3	No	NA

Evidence Base (for summary sheets)

Executive Summary

- This Impact Assessment appraises the potential costs of the Commission Network and Information Security Directive proposal in the UK if it were passed into law in its original form. The final EU law is likely to differ from the proposal but we have carried out this IA to inform UK negotiators and other stakeholders of the potential costs and benefits based on the currently available evidence. An updated IA will be produced for the final EU Directive, providing there is a need for UK regulations to transpose it.
- We consulted stakeholders in preparing this IA through a Call for Evidence and conducting a series of meetings. However, key details of the Commission proposal are unclear, so our estimates should be considered only indicative at this stage. We have asked the Commission to clarify some matters (see Annex 4).
- The number of affected businesses in the UK is a maximum of 22,935 in our estimate, created by adding up companies within standard industrial categories that match the terms in the Directive. There are differences in the market operator definitions used in the Directive and the Commission's Impact Assessment, which leads to differences in the figures of the institutions affected. Furthermore, the figures used in the Commission's Impact Assessment differ from these as well. It is important therefore to be aware of the differences arising and the causes for these. See Annex 5 for further details on the differences and the derivations of the various figures.
- In most of the sectors covered by the Directive, there are already measures in place which are tailored to meet the risk profile and nature of each sector, and either through general or specific measures, cover the disclosure of cyber security incidents in the operators and owners of the Critical National Infrastructure (CNI).
- Baseline scenario UK: for the sectors identified in the proposal for an EU NIS Directive, we estimate that they already spend £1.98 billion on security per year. Of the sectors, finance and public administration spend the most on security (with £706.3million and £869.5 million respectively). Large organisations took up the most significant amount of these figures spending £1.45 billion while SMEs accounted for £533 million. Spending per large organisation is estimated on average at £540,000 and for smaller organisations at around £26,000 on average. It should be noted though that the spending varies per sector on average as well.
- We estimate potential additional security spending of at most £1,984.2m in the High scenario and £992.1m in the Medium case in the year of the implementation of the NIS Directive. This means that in the High scenario affected organisations might need to spend an additional £540,000 in the case of large ones and an additional £26,000 on average by smaller companies. In the medium scenario this translates into an additional £13,000 per small organisation on average and £270,000 for larger institutions. It should be noted again that these averages can vary by sector.
- Potential benefits were estimated in terms of the value that affected institutions would need to be able to realise under the Directive to outweigh the potential costs. These estimates are highly dependent on the assumptions made. For illustrative purposes an overall benefit of £860.6m is assumed. This assumes that 5,000-10,000 affected institutions would achieve medium sized benefits of £27,000 for 50% of cyber security incidents. Other non-quantifiable benefits could arise for the customers of the affected institutions, the wider economy and from benefits derived from better communication amongst Member States under this Directive.

Background

Context

The European Commission highlighted the importance of Network and Information Security (NIS) in 2001 in its Communication Network and Information Security: Proposal for a European Policy Approach (see EC1, 2001). This proposal was followed by the adoption in 2006 of a Strategy for a Secure Information Society (see EC2, 2006). In line with this the Council then also adopted on 18th December 2009 a Communication on Critical Information Infrastructure protection (see EC3, 2009).

The European Community also established in 2004 the European Network and Information Security Agency (ENISA) with the aim to ensure a high level and developing a culture of NIS within the EU. In July 2012 (concluding in October), the Commission held a Consultation on Network and Information Security. The Commission have published the results of that consultation, which were used to help inform the proposal for the Directive (EC4, 2013).

On the 7th February 2013, the draft 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and Information Security (NIS) across the Union (see EC5, 2013)' was published, alongside a European Commission Impact Assessment of the Directive and the proposed 'Cyber Security Strategy of the European Union: An Open, safe and secure cyberspace' (see EC7, 2013).

In order to better understand the impact of the proposal for the EU NIS Directive, the UK Government issued a Call for Evidence to UK stakeholders to provide views and evidence on the proposed measures included in the Directive. This ran between 22nd May – 21st June 2013.

This Impact Assessment will consider the proposal for the EU NIS Directive published by the European Commission on the 7th February 2013.

Existing European Union Provisions in this area

As part of the reform of the EU legal framework for electronic communications (see European Parliament, 2009) which was adopted in 2009 and which had been transposed at the national level in most countries by May 2011, further requirements were added around the security and integrity of public electronic communication networks and services (Articles 13a and 13b specifically). In particular:

'Member states shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services'.

In practice this currently means that certain types of information about breaches to telecoms networks (for example on impact and cause) need to be communicated to the National Regulator (Ofcom in the UK). The regulator then passes these on to ENISA for their annual publication of those incidents that meet the required thresholds.

Security measures also need to be applied to 'All assets which when breached and or failing can have a negative impact on the security or continuity of electronic communications networks'. Article 13a also requires communication service providers to ensure the integrity of the network and 'to take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services'. Most of these requirements are already covered in existing standards such as ISO/ IEC 27001 for example (further details on the requirements around Article 13a can be found in Annex 1). There is also an array of other regulations which relate to Network and Information Security, where only the most important ones are included in Annex 2.

In the proposal for an EU NIS Directive, the Commission is now planning to extend similar measures to other sectors with substantial/ critical networks including Energy, Finance, Health, Information Society Enablers, Transport and Public Administrations. It remains slightly unclear how this extension might be implemented, which leads to a high level of uncertainty with respect to the implementation of the Directive overall and the potential impact. Nevertheless, we can assume for simplicity that requirements similar to those placed on the telecoms sector will be extended to the other sectors under consideration including for example reporting requirements or thresholds that need to be met for incidents to be reported.

Problem under consideration

The proposal for the EU NIS Directive (as of 7th February 2013) outlines the problem under consideration.

The functions of our societies and economies are increasingly underpinned by the Internet and private network and information systems. Hence the aim of the Directive proposed by the European Commission 'is to ensure a high common level of network and information security (NIS)' (EC5, 2013, p. 2). The European Commission also highlights that the 'magnitude and frequency of deliberate or accidental security incidents is increasing' (EC5, 2013, p.11). 'Lack of NIS can compromise vital services depending on the integrity of network and information systems. This can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect social welfare' (EC5, 2013, 2).

Network and information systems are also gradually contributing 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. According to the Commission 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).

There has been no overarching legislation or regulatory requirements covering all Member States in regards to ensuring a high common level of network and information security. In the absence of legislation, Member States have developed solutions on a country by country, and sector specific basis. In order to develop network and information security, some Member States have developed a voluntary approach, providing and supporting best practice while raising awareness of potential risks and threats to NIS. At the current time, the Netherlands and Germany are both considering national legislation to further support their efforts on this issue.

Furthermore, only the telecommunication sector is currently required to adopt risk management steps and to report serious NIS incidents at an EU level, whilst other sectors also have some measures in place, which, though not specific to NIS incidents, would require that anything which disrupts their services should be reported. Given the widespread use though of ICT and technologies in other sectors, the proposal suggests that it would make sense for them to consider NIS as well, given the dependence on correctly functioning networks in some sectors in particular. Therefore, the Commission considered it to be necessary to undertake regulatory steps in this area.

Objectives of the EU Directive

The Commission considers that the current purely voluntary approach followed so far does not provide sufficient protection against NIS incidents. Member States are seen to have very different levels of capabilities and preparedness, weakening the whole system due to the high level of interconnectedness. Hence at a 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 and public administrations concerned to be able to respond effectively to challenges of the security of network and information systems (EC5, 2013, p. 3).

The explanatory memorandum of the proposal for the EU NIS Directive sets out the objectives the EU Directive seeks to achieve;

'The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies' (EC5, p, 2).

Furthermore, the Directive is linked to the European Cyber Security Strategy, which was published alongside the proposed Directive on 7th February 2013. The objective of the Strategy is to ensure a secure and trustworthy digital environment, while promoting and protecting fundamental rights and other EU core values (see EC7, 2013). As the Directive supports the overall strategy, this should be considered a secondary objective of the Directive.

The Commission's proposal

The proposal for the Commission's NIS Directive (see EC5, 2013, p.4) seeks to address the problem outlined above by introducing measures in the following areas;

- Requiring all Member States to ensure that they have in place a minimum level of national capabilities by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs), and adapting national NIS strategies and national NIS cooperation plans.
- Creating a framework to enable national competent authorities to cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level. Through this network, Member States should exchange information and cooperate to counter NIS threats and incidents on the basis of the European cooperation plan.
- Ensuring a culture of risk management develops and that information is shared between the private and public sectors. Companies in the specific critical sectors and public administrations would be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. These entities will be required to report to the competent authority any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods.

To develop the options and to be able to analyse the various aspects of the Directive, the Commission consulted with a variety of stakeholders including (see EC6, 2013, p.7):

- Member States representatives for example in the context of the European Forum and in separate meetings.
- The private sector, which included individual electronic communications service and network providers, Internet service providers and industry associations, suppliers of hardware and software components for electronic communications networks and services and industry associations, providers of products and services for Network and Information Security and representatives from the banking and financial sector and from the energy sector. Discussions took place in various contexts including for example the European Public-Private Partnership for Resilience or the Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids as well as bilateral meetings.
- The European Parliament and especially the Industry, Research and Energy and Security and Defence Committees
- The European Network and Information Security Agency (ENISA) and the Computer Emergency Response Team (CERT) for the EU institutions (CERT-EU)
- Online public consultation, which fed directly into the IA and for which a total of 169 responses were received via the online tool and 10 more in writing by the Commission, leading to overall 179 responses.

Given this wide-ranging number of stakeholders that the EU consulted with, there remains a question mark about some of the stakeholders referred to. To begin with some of the stakeholders outlined in the private sector are not likely to be affected by the suggestions of this Directive except for the finance and the energy sector that were consulted. Hence it appears that responses from the unaffected group could provide a more biased opinion and potentially skew the results in favour of the Directive.

As mentioned above one of the data sources for the Commission's Impact Assessment was a consultation held by the Commission in October 2012. The UK Government participated in this consultation and its response can be found at the following weblink;

http://www.bis.gov.uk/assets/BISCore/business-sectors/docs/u/12-1222-uk-response-ec-consultation-network-information-security.pdf

In terms of their public consultation the Commission received 169 online responses in total of which 97 were classed as individuals and the others were answering on behalf of an organisation or an institution. Of 96 respondents that identified themselves either as a private company or as a business association (please note there is some overlap with individuals who were classified as such but who were answering on behalf of a company) in one of the fields provided, only 16 and 15 respectively were in the sectors that will be affected by the NIS Directive. Hence there appears to be a slight imbalance in the sample which could have also influenced the selection of the sectors suggested for inclusion under the NIS Directive as this appears to be heavily based on this public consultation.

The results being used in the Commission's proposal highlights that 'A high number of respondents thought that it would be important to adopt NIS requirements in particular in the following sectors:

banking and finance (91.1% of respondents), energy (89.4%), transport (81.7%), health (89.4%) Internet services (89.1%) and public administrations (87.5%)' (EC5, 2013, p.7). Given the weight given to these results, and the consultation in general with respect to the sectors chosen and throughout the impact assessment, it seems rather important to understand better what the impact on these results might be of the potential imbalance in the sample.

In addition to the Commission's proposal for the NIS Directive, the Commission has also published an Impact Assessment accompanying the Directive, providing further information on the measures in the proposed Directive. More information on the Commission's Impact Assessment is included in Annex 3. Where appropriate, our impact assessment references its EU counterpart, highlighting any differences in figures used or assumptions. Furthermore, Annex 4 provides a summary of the questions asked of the Commission by the UK, which relate to the Commission's proposal and Impact Assessment where the UK would like to see further information.

Rationale for Government intervention

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

- Public Good: security and resilience of networks could be considered to have the characteristics of a public good. The consumption of the good does not reduce availability for others (non-rival) and it is not possible to exclude someone from consuming the good (non-excludable).
- 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. Through the interdependent nature of these networks, negative effects associated with these externalities can potentially also spread more widely.

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

Sectors and groups affected

Under the existing proposal, requirements for network and information security would not be extended to all sectors in the economy but rather to those which make use of comparatively large and critical networks. The requirements will not be applied to micro businesses, which are excluded (also from the figures in Table 1), but will still apply to SMEs in the sectors covered. The European Commission outlines that 'the requirements are proportionate to the risk presented by the network of information system concerned' (EC5, 2013, p.9). However, it seems slightly unclear at this stage what the requirements might be and what this means in practice for smaller companies.

It should be noted that the estimated numbers of institutions affected used in this Impact Assessment vary from the ones provided by the Commission. The key reason for this is that different sources were used in some cases as well as due to issues of 'translating' the terms used by the Commission's Impact Assessment and Directive to the Standard Industrial Classification (SIC) codes used in the UK. Furthermore, it seems that the Directive uses a different definition of market operators than the one used to estimate the number of companies affected by the NIS Directive in their Impact Assessment (IA). A more detailed outline of the SIC codes used, the read across to the terms used by the Commission as well as an outline of the definition used in the Commission's Impact Assessment is provided in Annex 5. The figures derived under the Directive's definition, the Impact Assessment's definition and the figures used in the Commission's Impact Assessment the numerical difference to the Commission's IA are outlined in Table 1, 2 and 3 below. These are divided into the following headings/ categories:

- 'Directive': this reflects the figures that will be used in this Impact Assessment. This is derived using the definition in the NIS Directive and finding the most appropriate SIC codes.
- Commission's IA definition (SIC): These figures are derived using the definition in the Commission's Impact Assessment and finding the most appropriate SIC codes
- Commission's IA data: These are the figures used in the Commission's Impact Assessment

Depending on which definition or figures used the numbers can vary quite considerably. As one can see for example the difference between the figures using the Directive's definition and that in the Commission's impact assessment mainly arises due to a variation in the definitions used for the Health and the Energy sectors.

Table 1 – Comparison of the number of UK firms falling within the definitions used by the Directive and the Commission's Impact Assessment respectively

Sector	Energy	Transport	Health	Finance/ Banking	Information society enablers	Public Administration	Total
Directive	240	2,535	16,665	2,350	350	795	22,935
Commission's IA definition (SIC)	140	2,535	10,410	2,350	350	795	16,580
Difference	100	0	6,255	0	0	0	6,355

A difference that also arises, as mentioned above, is one between the figures derived under the SIC code using the Directive's definition and the figures used in the Commission's Impact assessment for the UK where provided. These numerical differences are outlined in the Table 2 below. Table 3 also outlines the difference between the figures in the Commission's Impact Assessment and the figures derived under the definition in the Commission's Impact Assessment using SIC codes. Again, in both cases these figures differ due to different sources being used, different definitions and the attempted translation to the SIC codes. The largest differences appear to arise in the Health sector as well as the Finance Sector in both cases.

Table 2 – Comparison of the number of UK firms falling within the definitions used by the Directive and the figures used in the Commission's Impact Assessment

Sector	Energy	Transport	Health	Finance/ Banking	Information society enablers	Public Administration	Total
Directive	240	2,535	16,665	2,350	350	795	22,935
Commission's IA data	60	2,028	1,860	396	N/A	N/A	4,344
Difference	180	507	14,805	1,954	N/A	N/A	

Table 3 - Comparison of the number of UK firms falling within the definitions used by the Commission's Impact assessment and the figures used in the Commission's Impact Assessment

Sector	Energy	Transport	Health	Finance/ Banking	Information society enablers	Public Administration	Total
Commission's IA definition (SIC)	140	2,535	10,410	2,350	350	795	16,580
Commission's IA data	60	2,028	1,860	396	N/A	N/A	4,344
Difference	80	507	8,550	1954	N/A	N/A	

For the purpose of this impact assessment the definition as used in the Directive will be applied here, leading to potentially 22,935 institutions being affected. Due to the limitations around the data available in some cases the figures will overestimate or potentially underestimate the number of companies affected. An overestimation is potentially arising as a higher level of the SIC code was used in some cases to represent the respective category as some information needed was not available at lower

levels. In the case of the Information Society enablers the number of companies affected might be underestimated as some of the categories included are not fully captured by a separate or any SIC code.

For example a short search of the internet has shown that there are potentially more companies than the 350 mentioned above that could be affected in the information society enabler category. There are around 50 internet payment gateways that are listed in the directory of a price comparison website for electronic payments (see Electronic Payments, 2013) and around 20 cloud computing service providers operate in the UK (Computer Weekly, 2013). These companies are not necessarily fully captured by the SIC code used. Furthermore the share of companies selling online is also gradually increasing. In 2011, around 17% of companies sold over a website and 8.4% sold via EDI (which is the computer-to-computer exchange of documents in a standard electronic format) across all company sizes (ONS, 2012, p.6 & p.8). As these categories are not necessarily captured by the SIC code used in this impact assessment to represent the information society enablers, this indicates that the number of companies affected in this category could potentially be larger. It should be borne in mind though that it was not possible to divide the aforementioned figures from the internet search by company size and therefore, it is possible that the figures presented still include micro enterprises, which are currently not affected by the Directive. Furthermore, some of these companies are also likely to operate not only in the UK but also in other European countries or globally.

Furthermore, this total figure of institutions potentially affected needs to be considered as the possible maximum number of companies under the Directive's definition, which is used here. The key reason for this is that it seems that the potential impact on smaller companies is likely to depend on the interpretation of the NIS Directive in particular with respect to ensuring that 'the requirements are proportionate to the risk presented by the network of information system concerned' (EC5, 2013, p. 9), the requirement to 'take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations' (EC5, 2013, p.24) as well as the level at which reporting thresholds are likely to be set. Furthermore, the final figure of institutions affected will also depend on the definition that the Directive will eventually settle on and so far it is unclear whether this will be the same as in the Directive or the level of detail at which this might be specified. As definitions become clearer, further work will be required to establish a final figure of companies and the number of public administrations affected.

Options

The European Commission's Impact Assessment considered three policy options (see EC6, 2013, pp.36- 58) including

- 'Do nothing' option, which was also used as the baseline scenario (Option 1) in their Impact Assessment. This involves the continuation of a voluntary approach to ensure a minimum common level of NIS. Measures here would include the issuing of communications addressing the member states as well as encouraging them for example to set up well –functioning CERTs, to adopt a national cyber security strategy and to stimulate the creation of a culture of risk management and improve the sharing of information.
- Regulatory approach (Option 2): Option 2 involves the establishment of a legal framework for NIS in Member States around capabilities, mechanisms for EU-level cooperation and requirements for key private players and public administrations. This requires Member States specifically to set up a national/ Governmental CERT, appoint a national competent authority for NIS with a coordination role and responsible for cross-border cooperation, adopt national contingency plans as well as a national cyber security strategy.
- Mixed approach of regulation and voluntary initiatives (Option 3): Again the Commission would attempt to reach a minimum common level of NIS across the EU through voluntary measures as outlined in Option 1 (i.e. build national capabilities; establish a network of CERTs and to share information). In addition though regulatory requirements would also be developed to close existing regulatory loopholes 'and create a level playing field across the EU' (EC6, 2013, p. 44). These would be identical to those outlined under Option 2 with respect to the sectors and the obligations.

It seems though from the outline above that more or less only two real options were considered i.e. Option 1 and 2 given that Option 3 is not very much distinguishable from Option 2 except for some

additional voluntary measures. A more distinctive third option would have helped to distinguish between potential benefits and costs in slightly more detail.

Based on an assessment of these options, the Commission considered the regulatory approach to have 'the strongest positive impacts as it would considerably improve the protection of EU consumers, business and Governments against NIS incidents' (EC5, 2013, p.7). According to their quantitative estimation of the potential costs, they also consider that this option would not 'impose a disproportionate burden on Member States' and that the costs for the private sector 'would also be limited since many of the entities concerned are already supposed to comply with existing security requirements' (EC5, 2013, p.8). The Commission also considers them to be set at the minimum level necessary to achieve a better level of preparedness and cooperation. Nevertheless, Member states would still be able to implement the Directive to reflect the actual risks faced at national level and to focus on critical entities and incidents with a significant impact (EC5, 2013, p.8).

For the purposes of this impact assessment we will consider similar options to the Commission's IA including the following policy options;

- **Option 1: Continue with status quo (individual Member State Activity) - 'Do Nothing'**

  The 'Do Nothing' option assumes that current arrangements on security, reporting and monitoring will continue and that the measures in the proposal for an EU NIS Directive are not implemented. 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 'Implementing the Directive' option assumes that the measures in the proposal for an EU NIS Directive is implemented into UK law.

As highlighted above the third option appears to very similar to Option 2 and therefore was not considered in this IA.

Regulation

Alternatives to Regulation

The proposed Directive by the Commission seeks to introduce regulation to address the identified problem. An alternative to the proposed regulation could be the use of a voluntary approach; this approach is currently being used throughout EU Member States, including the UK. Through education, information exchanges and awareness campaigns, organisations recognise the risk to their business from NIS incidents and take appropriate decisions to develop a culture of cyber security in their organisations to mitigate that risk. Where regulation is required, it is performed on a highly targeted, sector specific area (such as the nuclear sector). Over a period of time, through greater awareness of the risk to business continuity and incentives (such as via cyber security requirements in contracts) the level of capability would rise. Through the sharing of best practice and capability across the EU, the disparity of capabilities would fall and minimum levels of cyber security would be developed through business led requirements. It is also important to note that requirements and initiatives are likely to be implemented better on a sector by sector basis, where the specific issues of each sector can be addressed through targeted actions, rather than the horizontal approach which is currently suggested in the Commission's proposal. This approach is one which we are already conducting in the UK.

The UK's approach is primarily delivered through supporting and incentivising businesses and consumers to take action, rather than imposing regulation before businesses have been given the guidance needed and the opportunity to raise their capabilities. Our approach is characterised by far-reaching cooperation and collaboration between Government and the private sector. We understand that we need to identify and strengthen the cyber networks and systems on which we depend for the secure delivery of critical services, but these responses also need to be tailored to the various risks in each sector accordingly. The UK's National Cyber Security strategy, along with the one year on update, can be found at the following link:

https://www.gov.uk/government/publications/cyber-security-strategy

Key measures in this programme include for example:

- Much work has been done in the UK to reach out to the private sector in order to raise awareness of the threat and to encourage business to embed effective cyber security risk management practices, including through the 10 steps to cyber security guidance for business launched last year. The Government is currently working with several sectors (including Professional Business Services, ISP, Universities, Life Sciences and Retail) to raise awareness on cyber security across the sector base and to support these businesses to communicate effective cyber security messages to their clients.

- The Cyber-security Information Sharing Partnership ('CISP'), launched on 27 March 2013, brings public and private sector partners together to voluntarily share real time threat information in a trusted environment. It will allow each organisation to build up a richer picture of the threats posed by cyber space. The pilot, Project Auburn, facilitated information sharing between 160 companies, and these companies have now transferred to CISP.

- The Government intends to launch a National Computer Emergency Response Team (CERT) to improve national co-ordination of cyber incidents and act as a focus point for international sharing of technical information on cyber security.

- Encouraging the industry-led development of standards and guidance to enhance – and inform – relative levels of cyber security. The Government, through consultation with industry, has launched a call for evidence to select and endorse an organisational standard that best meets the requirements for effective cyber risk management. The aim of the call is not to create a new standard, but to provide clarity to the private sector on what good cyber security looks like, and which organisational standard to invest in to best manage their cyber risk – this might be a new one or it might be an existing and well-established one.

For further information on UK Government activities to develop cyber security capability in the UK, please visit https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace.

A second alternative is to significantly reduce the scope of the regulation proposed in the Directive. This would entail a much narrower scope of critical infrastructure, identified on a sector by sector basis that would be subject to regulation, with a continued emphasis on voluntary measures for organisations not covered. In addition to any reduction in scope, any new regulation could be specific to the sectors covered in the Directive, and not horizontal.

Another alternative to regulation is for the EU to cease all activity on developing Cyber Security capability. While organisations would develop capability as identified by its perception to business risk, this would not address the problem under consideration, namely to address the disparity of capability across the EU and encourage a culture of risk management in NIS issues. We therefore do not consider this as an option in this Impact Assessment.

One-In-Two-Out (OITO)

Under the UK's One In, Two Out rule, a measure of net cost to business (a "In") cannot be implemented unless equivalent regulation of twice the net cost is removed or simplified (a Two Out). As this is an EU Directive this rule does not apply to the implementation of UK regulation that is necessary to meet EU standards, although it would apply to any extra obligations that the UK could choose to add.

Evidence Base

To develop the various options and to be able to analyse the various aspects of the Directive, we have consulted with various stakeholders and used a variety of documents including;

- Online Call for Evidence for UK stakeholders on the proposed EU Directive on Network and Information Security. A Summary of the Responses by key themes is also available in a separate document. Overall the Call for Evidence received 88 responses of which 55 were made online and 33 were provided manually. With respect to the manual responses only 12 were used though in this Impact Assessment, which were the ones that filled in the form fully. The other responses were also analysed though qualitatively in the Summary of Responses. This is a separate document but should be read in conjunction with this impact assessment to obtain the full picture.
- Bilateral meetings with organisations that would fall under the scope of the Directive

- Submissions of views to the EU on the proposed EU Directive from UK and EU stakeholders
- The EU Directive and the EU Impact Assessment on the proposed Directive
- Outcomes from a workshop with UK stakeholders on the proposed Directive held on 22nd May 2013
- Further desk research to cross-check information gathered and to provide additional evidence

All documents used or referred to in this Impact Assessment are also included in the references in Annex 8.

Cost - benefit analysis

Limitations of the calculations/ estimates

The figures included in this Impact Assessment should only be seen to provide an initial and high level indication of the potential costs and benefits associated with this Directive, given that some of the key details required for the implementation of this Directive are not yet fully available. The data available in terms of network and information security is also in general rather limited and therefore, sometimes information and proxies were used which only provide an indication but not firm and robust evidence in relation to the potential costs and benefits. Furthermore, in some cases additional assumptions were needed to develop a potential estimate.

Limitations and issues related to the information and/or proxies used and assumptions made include:

- The Directive does not provide clear information or details on the scope since the definitions used in the Directive and the Impact Assessment differ. Furthermore, the definition of information society enablers remains rather unclear.
- The Directive does not provide any details on the guidance around standards that they would expect to see in relation to security. Without this guidance it is rather difficult to establish whether companies follow these already or whether further security expenditures would be required to achieve these.
- The Directive is not very clear on the thresholds for reporting, and therefore, it is rather difficult to assess how many incidents would need to be reported on. The number of incidents that a sector/ company suffer from in one year is also uncertain in itself, which will complicate in general any estimation of the potential costs.
- Secondary costs, which could be incurred as an indirect result of reporting, such as through companies redistributing or diverting resources to reporting breaches are also not considered here, partially due to the limited nature of the data available.
- The Directive is not very clear on the reporting mechanisms and the information that will need to be reported. This could affect any costs associated with respect to monitoring the systems as potentially different functions are required to report on a different set of information.
- Information on security spending is in general rather limited as it often forms part of other spending such as IT and is often not reported or calculated as a separate cost. Therefore, very little information on current security spending is available. Furthermore, estimating any future trends in spending is also not possible given that no historical values are available and technological changes would make this rather difficult. Hence, as a proxy, information from a UK survey and a global survey were used to obtain an indication of what the current security spending might be. Forecasts of security spending in future and the potential impact of the Directive were not attempted in this Impact Assessment due to the aforementioned reasons.
- Some of the estimates presented in this IA are based on global or national survey information. In particular in the case of surveys based on self-selection, these figures are likely to be biased and could either over- or underestimate the true costs and benefits. Given that the nature of the bias is not fully known these figures should only be seen to provide a potential indication of the estimated costs and benefits as they are used as a proxy. Global surveys used might also not be fully representative of the situation in the UK as regulations and characteristics of the industry could differ from that in the UK, which could also influence security spending.
- Assumptions were made with respect to the turnover of some businesses, when only the total value and some for the various business sizes were available. In most cases the assumption was

made that the difference that exists is used to fill the gaps for the other company sizes. Therefore, the turnover values sometimes used in these cases are the total revenue value for the sector despite the fact that not all companies might be included. Therefore, some of the costs are likely to be an overestimate. Furthermore, for the Finance Sector and for Public Administrations no turnover figures were available and therefore, a proxy in the form of operating expenses was used. However, these figures were not split by institution size and therefore, the share earned by micro enterprises could not be excluded. Hence this could potentially lead to an overestimation of the current security spending.

- The potential costs and benefits are also likely to be related to the number of security breaches currently occurring (i.e. a sector that suffers from more incidents might be required to spend more on resilience and security than others in proportion to the risks that they are facing). This has not been taken into account here as the current number of incidents taking place in the UK in each of the affected sectors is not known in detail.
- With respect to the benefits assessment the implicit assumption is made that institutions affected would benefit from the implementation of the NIS Directive in the form of reduced severity of potential incidents. However, how strong this link might be or the impact of the Directive on the severity of incidents is rather unclear at this stage due to the lack of detail around the practical implementation of the Directive. Therefore, these figures should only be considered as a proxy for the size of the potential benefits that affected companies need to receive to outweigh the potential estimated costs.

Therefore, the figures presented in this Impact Assessment should only be seen as indicative and not considered to be the final estimates for potential costs and benefits under this Directive.

Option 1: 'Do nothing' – Current arrangements on security, reporting and monitoring

To be able to establish the effect of the proposed NIS Directive on the UK, we need to establish a 'Do nothing' case first as a baseline. This should reflect the current costs/ spending of companies and the public sector in relation to their network and information security. We will provide estimates by sector and by company size given that the spending is likely to depend on this. Given the uncertainty of these estimates though, we will initially outline qualitatively the current security, reporting and monitoring arrangements by sector.

Using the definitions in the Directive and attempting to transfer these into the SIC codes used leads to a total number of 22,935 institutions, which are potentially affected (excluding micro businesses). A division by sector is provided in Table 4 below.

Table 4 – Number of companies potentially included under the Directive

Energy	Transport	Finance	Health	Information Society Service providers	Public Administrations	Total
240	2,535	2,350	16,665	350	795	22,935

Source: BIS, Business population estimates 2012 (BIS: business population estimates 2010 to 2012 - Publications - Inside Government - GOV.UK) except for Public Administrations where numbers were taken from ONS, 2012, UK Business: Activity, Size and Location; UK Business: Activity, Size and Location, 2012

As mentioned before, this is different from the figures gathered in the Commission's Impact Assessment, which is mainly down to different definitions and sources being used, but also the fact that in some cases no specific UK figures have been provided (see Tables 1- 3).

The key costs to these sectors are likely to arise from additional costs associated with the compliance under the new NIS Directive. This will be in particular reflected in changes to their current security and resilience spending but also in their administrative spending. In some sectors security and resilience is highly regulated or included in industrial codes and some examples of the areas for compliance by sector are briefly outlined below.

Current Reporting Requirements by Sector

As outlined below there are existing regulatory requirements currently in place across sectors in the UK, which provide critical services. These requirements are tailored to meet the risk profile and nature of each sector, and either through cyber specific measures, or through more general measures cover the

disclosure of cyber security incidents in the operators and the owners of the CNI. The respective sectoral regulators work closely with the companies in each of the sectors where applicable and have developed a good understanding of the various sectors and the challenges that they face. The UK believes that this sector by sector approach ensures that measures are focussed and proportionate, and that any cyber security incidents that may take place can be understood in relation to the wider operations of the sector. In general it seems from the brief analysis below that in most cases each of these sectors has already requirements in place that could contribute to the compliance of the affected institutions with the NIS Directive. However, in certain cases this is likely to also depend on the intended use of the regulation and/ or the purpose for which it was written. This can differ from the aim to prevent potential cyber security incidents but could still be applied in some cases to these incidents as well. This should be borne in mind though for the following section.

Before considering the measures placed on each sector, it must also be taken into account that 'all data controllers have a responsibility under the Data Protection Act to ensure appropriate and proportionate security of the personal data they hold' but 'there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data'. The Information Commissioner though 'believes serious breaches should be brought to the attention of his Office' (ICO, 2012, pp. 2-3). Serious breaches are actually not defined although guidance is available on the ICO website in terms of what this might mean in terms of reporting this to the ICO (see ICO, 2012, p.3). If a company considers that an incident needs to be reported it provides the required information to the ICO via a form on their website (see http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Forms/security_breach_notification_form_v3_012012.doc for further information).

Again if the company is a data controller then at least incidents that involve the loss of personal data can be reported to the ICO and a reporting mechanism could already be in place. Information that needs to be provided includes for example (amongst other items of information):

- Time of the incident
- Description of the incident
- Personal data at risk, how many data subjects are affected and whether these have been informed of the incident
- Actions taken to minimise mitigate the effect on data subjects affected

It seems that in terms of data incidents if the company is a UK data controller (also in any of the listed sectors below) then the required security level to do so is likely to be already in place, at least for protecting personal data. However, it is not the case that those incidents that might be related to the network but not to customer data would be included (e.g. loss of availability) and therefore, there is still the potential for additional security spending that might be needed.

It should also be noted that the EU is looking to introduce a new data protection regulation and changes to the aforementioned requirements are likely to be made. This could introduce a reporting and monitoring mechanism for data controllers. Hence additional administrative costs to add additional functions to this system could potentially be rather small under the NIS Directive, depending on what the requirements might be.

Information society service providers

In general it seems that UK information society service providers could potentially face a higher level of additional costs, since the existing requirements on this sector compared to all the other ones which are included appears to be less obvious. Hence larger differences could potentially arise between existing requirements and those needed under the Directive compared to other sectors. Additional extra costs could be limited, provided the Directive reporting rules are relatively flexible. However, the extent to which this might be the case will also depend on the implementation of the Directive.

The picture with respect to existing requirements for companies in this sector regarding security and resilience unfortunately is less clear. There is currently no clear regulator for these companies, although loose links might be in place with Ofcom for some, given the remit that some of the affected companies have and given their cross-cutting nature. Some companies in this sector may also be already covered by the existing requirements of Article 13a of the revised E-Communications Framework Directive.

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 cyber security 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 cyber security incidents as well although they were not originally intended or written for this purpose.

With respect to the oil and gas sector (upstream only) DECC 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 DECC. 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.

Given the implied high scrutiny level already by regulation and the regulator, the current level of security spending could potentially be high already. It seems that only some slight alterations or additions might be required to the existing system to comply with the NIS Directive and report the required information to the national competent authority. However, this is likely to depend on the implementation of the Directive and in particular the planned thresholds over which firms will be required to report incidents. Without these details it is not possible to assess fully whether there will be more or less reporting required and whether the security spending is at the required level to comply with the Directive.

Finance

It seems that most UK finance companies could potentially face limited extra costs, providing the Directive reporting rules are relatively flexible.

Firms in the Finance Sector that are regulated are obliged to adhere to the rules set out by their regulator about how they should operate and what they are required to report. Specifically, 'A firm must deal with its regulators in an open and cooperative way, and must disclose the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice' (Principle 11, Principles of Business). This includes any significant failure in a firm's systems or controls, including those reported to the firm by the firms' auditors.

For example, a firm must notify the appropriate regulator immediately it becomes aware, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future:

- The firm failing to satisfy one or more of the threshold conditions; or
- Any matter which could have a significant adverse impact on the firm's reputation; or
- Any matter which could affect the firm's ability to continue to provide adequate service to its customers and which could result in serious detriment to a customer of the firm; or
- Any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms.

Apart from these requirements, firms with which BIS have held discussions indicate that they already share information amongst themselves around cyber risks and issues to a large extent on a voluntary basis. The requirements outlined above indicate that regulated firms in the financial sector could potentially have already reporting requirements with which they have to comply. However, the impact the Directive may have on this is entirely dependent on the scope of the Directive and the thresholds

over which firms will be required to report incidents. Without these details it is not possible to assess fully whether there will be more or less reporting required by the regulated sector than is currently the case, or the resource and costs implications of any changes to the reporting requirements as well as whether the level of security spending is meeting compliance requirements. Equally it is not possible to say how unregulated firms with no current disclosure requirements might be affected.

Health

It seems that UK companies in the health sector could face limited additional costs, providing the Directive reporting rules are relatively flexible.

The Information Governance (IG) Toolkit is a performance tool produced by the Department of Health and now hosted by the Health and Social Care Information Centre, which draws together a range of legal rules and central guidance in one place as a set of information governance requirements. These include for example The Data Protection Act 1998, The Confidentiality NHS Code of Practice, The international information security standard ISO/ IEC 27002:2005 or the Information Security NHS Code of Practice For further information see

https://www.igt.hscic.gov.uk/about.aspx?tk=414656154148624&cb=14%3a47%3a12&clnav=YES&lnv=5

There are different sets of information governance requirements for different organisational types but all of them have to assess themselves against requirements for

- Management structures and responsibilities (i.e. assigning responsibility for carrying out the IG assessment, providing staff training, etc)
- Confidentiality and data protection
- Information security

All Health and Social care service providers, commissioners and suppliers must have regard to the Information and Governance Toolkit standard approved by the Health and Social Care Information Standard Board. This includes for example amongst others the NHS organisations, NHS England, Local Authority Adult Social Care etc. Each organisation needs to assess themselves against various criteria where at the minimum for example documented and approved processes for reporting, investigating and managing information security incidents / events need to be in place. This indicates that at the minimum a reporting and monitoring system should already be in place in most organisations in this sector in England and Wales to which these requirements apply.

Given the existence of this toolkit it seems that most of the health sector is likely to already have a high level of security spending as well as a reporting and monitoring system in place that could also be used under the NIS Directive. However, the actual impact of the Directive will depend on its final implementation and without further details it is not possible to fully assess whether companies in the health sector are already compliant with the NIS Directive.

Transport

It seems that UK transport companies could face limited extra costs, providing the Directive reporting rules are relatively flexible.

Primary legislation is already in place to regulate Counter Terrorism regimes in the land, maritime and aviation industries. In addition, work is ongoing to identify cyber security risks to the transport sectors and build these into the existing risk assessment process. International regulation also exists for the aviation and maritime industries. Given the increased interest here around incidents that would be covered by Article 14 and the existing legislation which is likely to require a similar level of security and resilience as by Article 14, it seems likely that any additional security spending required could be rather small. However, this is also likely to depend on the final form of the Directive and how similar this might be in relation to the current requirements.

Public Administration

The UK has long standing and effective arrangements in place to ensure the security of Government assets. The Security Policy Framework (SPF) is a central body of policy and standards that Departments, their Agencies and suppliers are mandated to follow and is enforced through a centrally co-ordinated programme of reporting and compliance.

The Government Security Secretariat (GSS) within Cabinet Office is responsible for developing and maintaining the Security Policy Framework.

More information on the SPF can be found at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200552/HMG_Security_Policy_Framework_v10_0_Apr-2013.pdf).

GSS also works closely with the Critical National Infrastructure (CNI) to develop and monitor standards. Common standards have been agreed and are in operation with our EU partners.

Given these various existing requirements security spending is likely to vary by sector and company size. Overall the aforementioned requirements seem to imply that security spending could already be quite high in each of the sectors in proportion of the potential risks that they are facing. However, the impact that the Directive may have on these sectors will depend on the final form of it.

Baseline estimates – Current security spending

Actual information on security spending is rather difficult to find and therefore proxies will need to be used. The call for evidence unfortunately did not shed much more light on this question with only a limited number of responses that provide some evidence on the current level of security spending.

The responses are divided into whether companies responded to the online survey or manually in a document that was sent to the Department. It should be noted that these responses needed to be separated to avoid potential double counting as some people indicated that they provided an online as well as a manual response. Furthermore, the numbers presented below are smaller in terms of the responses provided than overall numbers, given that not all respondents provided answers to the questions included but rather provided comments and views more generally on the Directive. These were captured and analysed in a separate document (see Summary of Responses). The responses received on the current level of security spending are outlined briefly below:

- Out of 55 responses to the online survey 35 did not provide an answer and 3 out of 12 responses that were provided manually did not do so either
- 4 of the respondents to the online survey highlighted that they are either not able to disclose this figure or they don't know it. In the manual responses four of the participants said the same.
- 3 of the respondents to the online call for evidence said that this was not applicable or relevant to them and one respondent indicated this in the manual responses.
- The rest or the respondents to the online survey provided values ranging from 0.1% to 23% or actual values in various currencies were provided. The median of the percentage range is 5% and average is 6.5%. The range from the manual responses was much smaller from less than 0.001% to 2% provided by 4 respondents.

Given the rather low response rate though unfortunately these figures will not be used for this impact assessment and therefore, we will consider other sources and proxies to establish an estimate of the current security spending.

The information around current security spending by sector and by company size remains rather patchy. The latest Information Security Breaches Survey (2013) conducted by PWC and commissioned by BIS indicates the following spending on security as a share of the IT budget by sector (using the most appropriate definitions) and by company size as outlined in Table 5 and 6 below. There are two potential issues with these proxies though that need to be borne in mind:

- The survey is based on self selection and therefore companies which have a higher level of interest in cyber security or have a higher awareness of it as a risk are more likely to respond. This could also mean that they have by association a higher level of security spending as a share of their IT budget. However, to which extent this might be the case is unfortunately not known. Furthermore, the shares presented below are not necessarily representative for the UK for the reasons mentioned above as well.
- The security spending outlined below only relates to the IT budget. There might be other relevant security spending that does not fall into the IT budget and is therefore, not included in the figures mentioned below. This could potentially lead to a lower share of security spending. To which extent this might be the case though is not known.

Table 5 – Security spending as a share of the IT budget by sector

Utilities, Energy and mining	Travel, leisure and entertainment	Financial Services	Health	Technology	Government
9.1%	6.3%	8.4%	11.1%	10.9%	12.6%

Source: PWC, 2013, Information Security Breaches Survey, https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

Table 6 – Security spending as a share of the IT budget by company size

	None	1% or less	2-5%	6-10%	11-25%	25% or more
Large	1%	14%	35%	26%	16%	8%
Small	10%	8%	32%	25%	11%	14%

Source: PWC, 2013, Information Security Breaches Survey, https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

These figures seem to imply that security spending varies by sector, whereas spending variations by size of company appear to be less pronounced given that most large and small companies appear to spend around 2-10% of their IT budget on information security. Nevertheless, there is also a slightly larger number of smaller companies (circa 18%) which either spend nothing or 1% or less, indicating that some of the smaller companies are likely to spend potentially much less than large companies. On average the PWC Information Security Breaches Survey (2013) shows that SMEs spend on average 12% of their IT budget on security. This seems potentially slightly counter-intuitive as smaller companies appear to be less at risk compared to larger ones. However, the same survey also showed that around 87% of the small companies that responded to the survey suffered from a security incident, only slightly behind large companies, where 93% of respondents said that they had a security incident in the last year. Smaller companies can also become of interest to cyber criminals as they can be part of the supply chain for a larger company which is the main target and the SMEs connections to it are used as a way to gain access to the larger company.

To be able to turn the aforementioned figures into a measure of security spending we will need to establish a link between security spending as a share of the IT budget and IT spending as a share of revenue. Gartner provides some measures for this in one of their reports called 'IT metrics: IT Spending and Staffing report (2013). The figures for the most appropriate sectors are outlined in Table 7 below in %. To provide a proxy for the Information Society service providers it was assumed that they are likely to have a similar spending to the telecoms sector and software publishing and internet services. Hence the respective values from Table 7 were used by BIS to calculate an average to represent the Information Society Service providers with IT spending as a share of revenue of 6.1%. Similarly for Public Administration values were available from Gartner in terms of operating expenses in relation to National/ International Government and State/Local Government. These were then used by BIS to calculate an average of 6.4% to represent IT spending as a share of operating expenses for Public Administrations overall.

Given that these percentages are based on a global survey these need to be treated with caution as different countries will have different regulations for these sectors, which can have an impact on the IT spending as well as considering IT spending to be of varying importance to their business in different countries. Hence in some cases the IT spending might be under- or overestimated. However, the extent to which this might be the case is rather unclear and in which direction the potential bias is tending is also not known.

Comparing these values though to those used in the Commission's Impact assessment (see Table 8), the difference does not appear very large in most cases. The only exceptions with bigger differences are Information Society Services and Public Administrations. Given the lack of any other information solely for the UK, the figures provided by Gartner will be used as a proxy here, which are also outlined in Table 7 below.

Table 7 – IT Spending as a Percent of Revenue, by Industry, 2012 in Gartner publication

Energy	Transport	Healthcare	Banking and Financial Services

1.0%	2.8%	3.9%	6.6%

Source: Gartner, February 2013, IT Metrics: IT Spending and Staffing report. These figures are not for onward distribution. If you would like to use these figures for any purpose outside this document then please contact Gartner for approval.

Software publishing and internet services	Telecommunications	Government – National/ International (as share of operating expenses)	Government – State/ Local (as share of operating expenses)
8.1%	4.1%	9.2%[1]	3.6%[2]

Source: Gartner, February 2013, IT Metrics: IT Spending and Staffing report. These figures are not for onward distribution. If you would like to use these figures for any purpose outside this document then please contact Gartner for approval.

Table 8 – IT spending as a share of revenue as used by the Commission's Impact assessment

	Energy	Transport	Healthcare	Banking and Financial Services	ICT sector (excl. telecom)	Public Administration (as share of operating expenses)
Commission's IA	1.1%	3.0%	3.3%	6.5%	7.6%	3.6%

Source: EC6, 2013, p.86

Using the figures in Table 7 (including the averages) as well as information provided by the PWC survey leads to the figures in Table 9 below. As mentioned earlier the Call for evidence did not provide sufficient data to draw conclusions on the share of the IT budget of companies that is spent on security.

Given the information above, we will make the assumption that smaller companies are likely to spend more of their IT budget on security but given that their IT budget is likely to be a much smaller share of their revenue it will be assumed that SMEs spend half of the assumed share of turnover on security as outlined above i.e. in the energy sector smaller companies are likely to spend around 0.05% of their revenue on security. This leads to the results in Table 9 below for 'small' and 'large' companies by sector.

Table 9 – Share of revenue spent on security

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration
Large	0.09%	0.18%	0.55%	0.43%	0.66%	0.81%
SMEs	0.05%	0.09%	0.28%	0.22%	0.33%	0.40%

The turnover figures by sector were taken from the Business Population Estimates publication by BIS (see BIS, 2012) which provides these by SIC code. Due to issues around the data in some cases being too disclosive (i.e. individual companies could be identified from the figures) in some cases the numbers were not available for all categories by company size. Therefore, where figures were missing but the overall amount for the industry was available, it was assumed that the residual is evenly distributed among the remaining categories i.e. the value was evenly split between the remaining categories. In some cases this could mean that the turnover for the SMEs and larger companies is overestimated given that the share for existing micro enterprises is still included as well.

For the Finance sector and the Public Administrations no turnover figures were available from the same source. For these sectors we are using ONS data on their intermediate consumption (see ONS, 2010) which reflects to a certain extent the value added of these sectors and which we are using as proxy for

[1] IT Key Metrics Data 2013: Key Industry Measures: Government: National and International Analysis: Current Year, 14 December 2012, G00245619, **Analyst(s):** *Jamie K. Guevara* | *Linda Hall* | *Eric Stegman*

[2] IT Key Metrics Data 2013: Key Industry Measures: Government: State and Local Analysis: Current Year, 14 December 2012, G00245621, **Analyst(s):** *Jamie K. Guevara* | *Linda Hall* | *Eric Stegman*

turnover here. This data has some additional issues though as we are unable to divide the figure by company size i.e. only a total value for the sector is available and in the case of the Finance sector we are also unable to exclude the Activities of holding companies, which is covered by SIC 64.2. Therefore, the estimated current security spending could be overestimated for the Finance sector and the Public Administration. This should be borne in mind when considering these figures. A further assumption was made with respect to medium sized companies, where larger ones of these are more likely to behave like large companies rather than small ones. Therefore we assume that 50% of the medium sized companies and the associated turnover have similar security spending rates as large companies and the other 50% the same as small companies.

Using the analysis and assumptions outlined in this section, while also taking into account the limitations of the data, the current estimated security spending by sector is outlined in Table 10. Table 11 also provides an overview of the current estimated security spending per large and small organisation. It should be noted that large companies include those with employees of more than 250 but also 50% of the medium-sized companies as some of the larger medium companies are more likely to behave like large companies as well as to accommodate the fact that 50% of the revenue of middle-sized companies was taken into account in the calculations for the estimated security spending level.

Table 10 – Estimated current security spending by sector – Baseline estimates (in £m)

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration	Total
Large	121.6	113.1	543.3	59.3	33.5	579.6	1,450.6
Small	14.9	16.3	163.0	46.2	3.3	289.8	533.7
Total	136.5	129.4	706.3	105.6	36.9	869.5	1,984.2

Table 11 – Estimated current security spending per institution by sector and size – Baseline estimates (in £m)

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration	Total (on average)
Per large institution	1.57	0.25	1.44	0.047	0.67	1.26	0.54
Per small institution	0.09	0.008	0.08	0.003	0.011	0.86	0.026

For the sectors identified in the proposal for an EU NIS Directive, we estimate that they spend £1.98 billion on security spending per year. Of the sectors, finance and public administration spend the most on security spending (with £706.3million and £869.5 million respectively). Large organisations took up the most significant amount of these figures spending £1.45 billion while SMEs accounted for £533 million.

We also estimate that on average a large institution spends £540,000 currently on security and smaller organisations around £26,000 on average. This amount does vary also by sector where large companies in the Energy sector are estimated to spend the most on security with around £1.57m on average and the Health sector the least with only £470,000 on average. In the case of smaller institutions, public administrations seem to spend the most on average with around £860,000 and again the Health sector the least with only around £3,000 on average.

Option 2: Costs - Implement the proposal

In this section we will look at the various additional costs that institutions might need to incur if the NIS Directive is implemented as currently proposed. The potential additional costs will be split between those

for the institutions affected as well as potential additional costs to Government due to monitoring and enforcement. With respect to the costs under investigation we will look specifically at:

- Additional costs to affected institutions from potential additional security spending
- Additional costs to affected institutions from potential additional administrative costs for reporting and monitoring
- Additional potential costs to Government through the establishment of a national competent authority
- Additional potential costs to Government through monitoring and enforcement

Each of these will be looked at in more detail below, after outlining briefly what the NIS Directive currently proposes in each case.

Security spending (Article 3 and 14)

The Directive currently defines security (Article 3 section 1.2) as the 'ability of a network or information system to resist, at a given level of confidence, accident or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.' Furthermore, Article 14 of the Directive outlines that 'Member states shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations'. In addition the Explanatory Memorandum highlights that 'The risks will have to be identified in the first place by the entities subject to these obligations which will have to decide on the measures to be adopted to mitigate such risks' (EC5, 2013, p9). Article 16 also indicates that the use of 'standards and/or specifications relevant to networks and information security shall be encouraged'. According to the Directive (Article 16 s2), the Commission committed to provide a list of standards but unfortunately this list has not been published in time for this Impact Assessment. The IA undertaken by the Commission provides a bit more detail by highlighting that requirements would be similar to guidelines on security measures in Article 13a of the Framework Directive. This includes as requirements regular risk analysis, governance and risk management, human resources security, security of systems and facilities, operation management, incident management and business continuity management (EC6, 2013, pp.38-39).

On the one hand this approach recognises that these requirements can differ between sectors but it also does not yet provide very clear specifications which criteria might apply in practice under these requirements. This makes the estimation of the potential additional costs for security spending rather difficult as it could be assumed to reflect current industry standards and level of security spending but might also imply a much higher level than the current one used by the institutions affected.

The call for evidence did not produce much quantitative data on the potential increase in security spending under the Directive. The call for evidence specifically asked what the potential impact might be on their organisation in relation to security spending if they had to report all incidents of 'significant impact' as currently defined in the Directive but using as an indication the thresholds under Article 13, which currently applies only to telecoms companies. The results show that

- 42 of the respondents to the online survey did not provide a response and one respondent that provided a manual answer did not respond either
- 6 of the online participants indicated that costs are likely to increase and so did 3 respondents that provided a manual response
- 3 of the online participants indicated that this impact would depend on the implementation of the Directive and so did 5 in the manual responses
- One respondent each in the online and the manual survey indicated that no additional or only minimal costs would be incurred
- Two respondents in the online survey replied that this is not applicable to them and one did so in the manual responses
- One respondent in each the manual and the online survey indicated that the impact was not known to them.

The responses did not provide much quantitative data unfortunately, although in some cases information was provided but it cannot be used here due to the relatively small sample size.

Some surveys though can shed some light on the level of security spending and the security policies that are already being implemented, which could then potentially indicate whether security spending would need to increase significantly or not.

The Information Security Breaches survey conducted by PWC (2013) and commissioned by BIS only refers to one specific security standard which is ISO 27001, which provides a framework to establish, maintain, monitor and review an Information Security Management System. Of the responding large companies who are aware of this standard 31% had implemented this standard fully, 45% had done so partially and 7% were planning to do so over the next 12 months. With respect to small companies that participated the numbers are smaller with only 18% having this standard fully implemented, 18% partially and 21% were intending to do so over the next 12 months (Please note: based on 132 responses to this question). Furthermore another survey commissioned by the FSB indicates that small companies are already taking actions against online crime with the 5 highest ranking measures being regular updates of virus scanning software (59%), having a firewall between the company and the rest of the world (47%), introducing spam filtering software (43%), introducing or improving data back-up and recovery routines (36%) and the regular installation of security patches (35%).
A further study by Quocirca also showed that around 30% of respondents said that they had suffered from a targeted attack and this also had a significant impact. It is not possible to tell from this information though what actions might have been taken or what type of attack these companies suffered from, which are two examples of the factors that can influence the ability of a company to defend themselves against cyber incidents. It also showed though that 25% of the respondents were able to discover and stop the attack (Quocirca, 2013, p.4).

This seems to indicate that large and small companies are already taking measures to protect themselves and ensure that their services are resilient. However, it also seems to indicate that larger companies are potentially ahead of small companies, which is not surprising given that they are likely to have larger budgets and presumably consider themselves more at risk as well. Therefore, it could potentially be the case that large companies will need to increase their security spending by only a small amount, whereas smaller companies might need to increase their security spending by much more.

Furthermore, in the previous section we looked briefly at the various security arrangements by sector. Given the potentially well developed measures in each sector it could be the case that the level of security spending is already rather high and therefore companies could potentially be satisfying the level of security needed to comply with the Directive already. Hence any additional costs associated with increased levels of security spending under the Directive could potentially be rather small. This is likely to depend on the details related to the implementation of the Directive though as well, which are unfortunately not yet available. Nevertheless, we will attempt to estimate below the potential additional security spending in various scenarios. The limitations though highlighted at the beginning of this section should be borne in mind here as any figures presented in this Impact Assessment are only indicative.

Estimate of the potential additional security spending

A high level of uncertainty remains with respect to the extent to which security spending might increase. The extent to which security spending might increase is likely to depend on:

- The current level of security spending and whether this already meets the required level. This in turn will depend on the interpretation of the phrase ‘appropriate technical and organisational measures to manage the risks posed’ (see Article 14). As it remains unclear what this might mean in practice and how companies will need to show that they are compliant will influence by how much the level of security spending might need to increase.
- The guidance around standards that the EU might publish and whether sectors already adhere to these. If this is the case then additional security spending is likely to be rather small.

Hence given the high level of uncertainty these initial estimates are only to be seen as indicative and not as final estimates, given that further details around the Directive and its interpretation will still need to be determined. The figures presented here are mainly based on assumptions due to a lack of more quantitative information.

The following assumptions will be made to cover a range of the potential increase in security spending. It should be borne in mind though that these assumptions would need to be tested if the Directive is

implemented to obtain a more robust evidence base. Hence further evidence should be collected once there are plans to implement the Directive. The assumptions made here will range from a high to a low scenario comparing these increases to the scenario outlined in the baseline case. In the high scenario we will assume that small companies will need to increase security spending to the same level (in terms of share of revenue) as large companies in the baseline scenario i.e. we will assume that they will need to double their security spending to meet the requirements of the Directive. With respect to large companies we will assume something similar i.e. that they will need to double their security spending as well. A doubling in security spending is likely to represent the most extreme case, given that we indicated already earlier that sectors already appear to have a high level of security spending in general. Hence this scenario is rather considered to be unlikely and could therefore be seen as the potential maximum increase in security spending required as a result of the Directive.

In contrast in the low scenario companies will need to only increase their spending by a negligible amount and therefore we will assume that companies will need to spend the same amount as in the baseline scenario and therefore the increase is potentially zero for companies in this scenario or of negligible size. For the medium case i.e. where companies are likely to increase their security spending as a result of the Directive by a certain amount but smaller than for the High case, we will take the median between the security spending in the High case and the low/ baseline case. The level of security spending as a share of revenue for each sector and split again by company size is outlined in Table 12 below.

Table 12 – Increased level of security spending as a share of revenue for the High and Medium case respectively

	Energy	**Transport**	**Finance**	**Health**	**Information Society Service providers**	**Public Administration**
High – Large	0.18%	0.35%	1.11%	0.87%	1.33%	1.61%
High - Small	0.09%	0.18%	0.55%	0.43%	0.66%	0.81%
Medium - Large	0.14%	0.26%	0.83%	0.65%	1.00%	1.21%
Medium - Small	0.07%	0.13%	0.42%	0.32%	0.5%	0.60%

Using these figures as well as the same turnover figures as before provides us with the increased level of security spending under the Directive for both the Medium and High case (as we are assuming the Low case is the same as the baseline) and the additional level of security spending (which is the difference between the increased level of security spending and the baseline) as outlined in Tables 13 & 15 below. In total this leads to potential additional security spending of £1,984.2m in the High scenario and £992.1m in the Medium case in the year of the implementation of the NIS Directive. It should be borne in mind though that this is only an indicative estimate of the potential additional security spending that might be required under the Directive. Table 14 shows in the High case that large organisations are estimated to spend on average around £540,000 and smaller institutions around £26,000 on average in addition to their current security spending level on average. In the medium case, large companies are estimated to spend on average £270,000 and smaller ones around £13,000 additionally as shown in Table 16.

Spending could be spread potentially over several years leading up to the implementation of the NIS Directive depending on the date when this might be finally implemented. However, it would have been rather difficult to represent the distribution of the potential costs over a number of years, which could vary as well. Hence it is assumed that at the latest institutions will need to incur the total costs in the year when the NIS Directive is being implemented.

Furthermore, the estimated value could only be seen as transitional if it represents the spending needed to upgrade the security system. Further expenditure might be required in future years for further upgrades and maintenance. However, it is rather difficult to estimate this level of spending as it will depend on technological developments, the specific implementation of the NIS Directive and on the guidance provided by the Commission on the level of standards that need to be satisfied to comply with the Directive. Therefore, the spending on upgrades and maintenance of the security system could potentially be either small or negligible if companies already have the required systems to upgrade and maintain security levels in place or it could lead to much higher levels of spending if this is not the case. Given the current uncertainty around which of these cases might be more likely as well as the difficulties to predict technological developments, no attempt was made to represent these costs in future years. However, it could be assumed that the estimated value for security spending could be seen as the potential maximum value that affected sectors might need to spend in future years as well. Any future forecasting using this particular value though is likely to overestimate the potential costs and therefore to avoid misrepresenting these, no attempt was made to do so.

Table 13 – Potential additional security spending (in £m) – High case

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration	Total
High case – security spending - Large	243.2	226.3	1,086.6	118.6	67.1	1,159.3	2,901.1
High case – security spending small	29.9	32.6	326.0	92.5	6.7	579.6	1,067.3
Additional security spending - Large	121.6	113.1	543.3	59.3	33.5	579.6	1,450.6
Additional security spending - small	14.9	16.3	163.0	46.2	3.3	289.8	533.7

Table 14 – Potential additional security spending by sector and size (in £m) – High case

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration	Total (on average)
Additional security spending per large organisation	1.56	0.25	1.44	0.047	0.67	1.26	0.54
Additional security spending per small organisation	0.09	0.008	0.083	0.003	0.011	0.86	0.026

Table 15 – Potential additional security spending (in £m) – Medium case

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration	Total
Medium case – security spending - Large	182.4	169.7	815.0	89.0	50.3	869.5	2,175.8
Medium case – security spending small	22.4	24.5	244.5	69.4	5.0	434.7	800.5
Additional security spending - Large	60.8	56.6	271.7	29.7	16.8	289.8	725.3
Additional security spending - small	7.5	8.2	81.5	23.1	1.7	144.9	266.8

Table 16 – Potential additional security spending by sector and size (in £m) – Medium case

	Energy	Transport	Finance	Health	Information Society Service providers	Public Administration	Total (on average)
Additional security spending per large organisation	0.78	0.13	0.72	0.023	0.335	0.63	0.27
Additional security spending per small organisation	0.04	0.003	0.041	0.0015	0.005	0.43	0.013

Administrative costs for Reporting and Monitoring

According to Article 14 s2 market operators and public administrations will need to notify to the competent authority incidents which have a significant impact on the security of the core services they provide. Furthermore, according to Article 14 s7 'the Commission shall be empowered to define, by means of implementing acts the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.3'.

Article 15 also implies additional costs in relation to being required to undertake a 'security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority'. This is required in addition to having a certain level of security spending and overview of their system, which seems to imply potential additional costs in relation to monitoring the network, reporting incidents that qualify to the competent authority as well as having to provide funding for security audits if required to undertake these.

In cases where personal data might be involved with security incidents, 'Member States shall implement the obligation to notify security incidents in such a way that reduces/ minimises the administrative burden' (EC5, 2013, p.15). This could imply that companies that suffered from an incident that also involves personal data might only need to notify one authority or the reporting requirements are so similar that only one notification needs to be produced.

As outlined before some sectors already have a certain level of scrutiny under which they are required to maintain a certain standard of security and report incidents. In these cases it is likely that additional spending for monitoring and reporting could be relatively small. However, this will also depend on the existing reporting and monitoring requirements and how similar these are to any requirements under the Directive as well as the level at which thresholds are likely to be set. Unfortunately it currently does not outline what these reporting requirements might be and only indicates that they are likely to be similar to those that currently apply to the telecoms sector i.e. Article 13 (of the revised E-Communications Framework Directive) (EC6, 2013, p. 68). Under these requirements the information that needs to be reported on incidents is:

- Services impacted (selection)
- Number of users (percentage, national customer base)
- Duration (hours)
- Root cause category
- Emergency calls or interconnections impacted
- Details about the incident

In addition the cause of outages needs to be recorded which can be due to:

- Natural phenomena
- Human errors
- Malicious attacks
- Hardware/ software failures
- Third party failures

Whether this information is already collected under existing reporting and monitoring requirements is likely to depend on the sector. As outlined in the section on current monitoring and reporting arrangements (see pp. 14-17) we have already identified some of the various reporting mechanisms that are used in each sector. In each case it appears that some level of reporting and monitoring systems that collect similar data as required under Article 13 could be already in place. Therefore it seems that additional administrative costs associated with reporting and monitoring systems could potentially be quite small. The extent to which institutions might need to report incidents will also depend on the level at which thresholds will be set. At the moment there is no indication where these levels might be set for each sector, which also makes the estimation of the potential additional administrative costs rather difficult. Furthermore, in the case of currently unregulated firms and sectors, an assessment of the costs is currently too difficult without further details on the Directive. However, it seems likely that they will need to incur higher costs compared to companies that are already regulated and therefore, might have some of the required reporting and monitoring systems already in place. Some further general evidence

that seems to support the indication that the additional costs could potentially be rather small is outlined below.

General evidence

In general the most recent Information Security Breaches Survey conducted by PWC (2013) and commissioned by BIS highlights that 67% of the large companies that participated in the survey carry out security risk assessments for information and physical security and 18% for information security only. For small businesses that responded these shares are slightly smaller with 42% and 18% for information and physical security and information security only respectively (Please note: based on only 146 responses) (PWC, 2013, p. 4). The survey also highlights that 99% of large companies that responded have a formally documented information security policy but only 54% of small businesses do (Please note: based on 152 responses only) (PWC, 2013, p. 6).

Companies also provide some level of training to staff to ensure that they are aware of security threats. 58% of responding large companies provided ongoing education and 32% at induction only. Similarly 48% of small companies that participated provided ongoing education and 29% at induction only (PWC, 2013, p.6). It should be noted though that this survey is based on self –selection and thus might not necessarily be representative for the whole of the UK as it is possible that mainly companies responded to the survey which are already quite sophisticated in their approach to cyber security or which might have a keen interest in this particular area. This can bias the results upwards in particular since also the number of responses to these particular questions was rather small.

Other administrative costs

Additional costs could also arise from having to undertake security audits in case these are requested by the national competent authority. The level of these costs is likely to depend on the sector as well as the size of the institution, assuming that larger ones would incur higher costs as the network and the information systems that would need to be checked are likely to be more complex and extensive. Furthermore, these costs are unlikely to necessarily arise on an annual basis as they would only need to be incurred if the competent authority requests this.

Given this dependence on these characteristics of the institution and the lack of information in the Directive around what constitutes a security audit, no quantification of the potential additional administrative costs was possible. Furthermore, no baseline could be established i.e. the extent to which institutions already undertake security audits by sector and company size and associated annual costs to which these additional requirements could be compared to.

A question on additional costs in relation to the impact if all incidents that companies had needed to be reported and the costs associated with an audit undertaken by the National Competent Authority was asked in the Call for evidence but only a few responses were received, which unfortunately do not provide a robust basis to provide a cost estimate here either. Results are presented briefly below for information only.

- The three answers to the online survey ranged from indicating only that costs are likely, that this depends also on the frequency and the scope of the audit to a specific figure of taking around 2-3 man-days.
- In the manual responses similarly three of the answers indicated that additional costs would be likely for various reasons to providing some more specific numbers. These highlighted that this might take up two weeks of one Full time equivalent employee (FTE) to 20 man-days or potentially around £50,000.

Additional administrative costs could also arise from incidents that occur outside of the EU but have a significant impact on core services and networks in the EU. From the current draft Directive it appears that these incidents are likely to be included with respect to reporting these to the national competent authority as well. However, given that it is currently not known how many of the incidents/ breaches are currently caused by incidents outside of the EU with a potential knock-on effect for networks/ systems and core services in the EU it is not possible to provide an indication of the potential administrative costs related to reporting that could arise from this.

Potential Costs to Government

In addition to these requirements on sectors the Directive also highlights the following requirements:

- National NIS strategy: According to Article 5, each member state will need a NIS strategy, which defines the 'strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security'.
- Computer emergency response team (CERT): This team will need to be established according to Article 7, and required then to follow a well-defined process.

A National Security Strategy (see HMG, 2010) has already been established and published in October 2010, and a UK Cyber Security Strategy (see HMG, 2011) was published in November 2011.

With respect to the establishment of a national Computer Emergency Response Team (CERT), GovCertUK already exists for the UK Government and assists public sector organisations in the response to computer security incidents as well as providing advice to reduce the threat exposure. They also gather data from all available sources to monitor the general threat level. In December 2012 it was also announced that the national approach to cyber incident management is under review in the UK, particularly in the light of the successful Olympics response. The intention is to move towards the establishment of a UK National CERT. This will build on and complement our existing CERT structures (which includes CSIRT UK, Gov CERT and MOD CERT), improve national co-ordination of cyber incidents and act as a focus point for international sharing of technical information on cyber security. Hence no significant additional costs are likely to be incurred under Article 5 and 7.

The Directive also requires member states to provide early warnings within the network on risks and incidents that fulfil certain criteria including that they grow too rapidly in scale (or may do so) and that they exceed national response capacity (Article 10), ensure a coordinated response in accordance (Article 11), publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website, discuss and assess (at the request of one Member State or the Commission) NIS strategies and NIS cooperation plans, jointly discuss and assess (at the request of a Member State or the Commission) the effectiveness of the CERTs, cooperate and exchange information on all relevant matters with the European Cybercrime Centre and other relevant bodies, exchange information on best practices and assist each other in building capacity on NIS, organise regular peer reviews on capabilities and preparedness and organise NIS exercises. This implies that the national competent authority would need to monitor persistently their networks very closely to be able to provide early warnings and ensure the required response when needed. In addition cooperation between NIS and a good understanding of other countries' NIS and capabilities will be required. As these functions are likely to be part of their (or the national CERT's) core function it is rather unlikely that significant additional administrative costs would be incurred.

In addition to this Article 9 of the Directive requires that the 'exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure'. Article 9 does not fully outline what this might mean in practice i.e. what requirements this infrastructure would need to fulfil to be considered secure. Hence if existing infrastructure is not sufficient then further additional costs might need to be incurred to raise the standard of the infrastructure to the required level where needed. The potential level of these costs though remains uncertain and therefore, no attempt has been made here to estimate these. Further details on the criteria to be met will be required to establish these in the future.

<u>Monitoring and enforcement costs for Government (Article 6 and 15)</u>

Article 6 requires each Member state to designate a national competent authority on the security of network and information systems. It will need to monitor the application of this Directive at national level and will receive the notifications of incidents from the various sectors and public administrations.

Article 15 provides some further indication around implementation and enforcement. According to this section Member States shall ensure that the competent authorities have the 'power to require market operators and public administrations to

a) provide information needed to assess the security of their networks and information systems including document security policies
b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority'.

In addition the competent authority has the 'power to issue binding instructions to market operators and public administrations', 'shall notify incidents of a suspected serious criminal nature to law enforcement authorities' and 'shall work in close cooperation with personal data protection authorities in cases resulting in personal data breaches'.

The costs associated with respect to the national competent authority (Article 6) are currently unclear but two potential options could be considered here.

a) An existing authority takes on the responsibilities of the national competent authority in addition to their existing ones
b) A new institution is set up to become the national competent authority

Existing authority as the national competent authority
Costs associated with the first option could be limited if an existing authority would be allowed to take on this function and reporting requirements are very similar to those currently in place in the respective sector as not completely new processes would need to be developed. Additional administrative spending to ensure appropriate monitoring and enforcement of the Directive are still likely to be required but could be expected to be less than if a new institution needs to be established.

However, the costs could increase if new reporting requirements are added to the existing ones even if a current regulator is chosen and reporting requirements are in place. Various steps that are likely to be required to establish a new reporting system could include the development of a reporting system including templates, a web portal, etc. A function/position would need to be set up to monitor the data/ information that is provided through this new reporting system. One regulator indicated that this could take the employment of one FTE as an ongoing administrative cost. In addition processes would need to be established to assess the provided information, undertake investigations and audits where required as well as reviewing any remedial actions needed after an audit or processes for warning and fines if these are not fully implemented. Hence additional costs could arise even if an existing regulator would be managing a new reporting system under the Directive.

As an indication of potential costs a previous assessment undertaken by Detica (2011), commissioned by the Department for Culture, Media and Sport, of the application of Article 13 to the telecoms operators indicated that for the monitoring activities a minimum annual resource of 0.2 FTE at Principal level and 0.8 FTE at Associate level would be required leading to a total cost of £43,000 per annum (Detica, 2011, p.38). In terms of compiling the information received the study indicates an annual cost of £7,000 requiring around 2 months of work (Detica, 2011, p. 40). The costs to Ofcom for receiving the outage information and reports including potentially developing a sophisticated management system was not quantified at the time in the Detica study. In terms of costs associated with investigations the study assumed that Ofcom might require an approximate 0.4 FTE at Principal level and 1.6 FTE as Associate level for 5 months for each investigation, leading to a cost for an investigation of £36,000. If more than one audit is being undertaken simultaneously then the costs are assumed to increase to £144,000 per annum in their medium scenario and to £360,000 per annum in their high scenario (Detica, 2011, p. 44). Additional background resourcing costing around £55,000 per annum might also be required as assumed in the Detica study (Detica, 2011, p. 48). Hence in total this leads to a potential cost of around £250,000 per annum, assuming the costs for investigations of £144,000 as in the medium scenario. It should be borne in mind though that the potential costs as outlined in the Detica study relate only to one sector.

The extent of the costs under the NIS Directive though are likely to depend on various factors including:

- Knowledge and understanding of the various sectors included under the Directive as additional personnel might be required to develop an understanding of the various sectors
- the experience of the regulator in setting up any new processes that might be required
- how adaptable existing processes are to any new requirements under the Directive
- the level of the thresholds as this will affect the number of incidents that will need to be reported, the amount of information that will need to be reviewed and the number of cases to be potentially investigated

Hence the potential costs cannot be assessed here yet in detail as considerations with respect to which institution might take on this task have not been made yet given the early stages of this Directive.

Establishing a new institution
The costs are likely to increase significantly if a completely new authority is established which will need to develop the aforementioned processes from the beginning but which potentially could draw on some support from existing regulators to learn from their experience as well as drawing on their knowledge of the sector. The Commission's IA indicates that on average 6 FTE would be required to carry out the tasks of a competent authority (i.e. developing and implementing a cyber – incident contingency /cooperation plan and a national cyber security strategy) with an associated cost of around £360,000 EUR per member state (EC6, 2013, p.50).

Given the aforementioned potential list of responsibilities to ensure implementation and enforcement under Article 15 as well as potentially the need to develop new processes and enforcement systems it seems that the figure of around 6 FTEs might potentially be on the low end to be able to cover these and therefore costs could potentially be higher than those assumed by the EU IA. However, this is also likely to depend on which particular functions the national authority would be taking on specifically and at which level of detail.

However, the various options with respect to which institution might take on the additional responsibilities or whether a new authority will be created and what shape it might take still need to be considered and then the potential costs and benefits of these need to be assessed in more detail.

Benefits – Implement the proposal

It is also rather difficult to assess the potential benefits from this Directive. These could potentially include (and which will be looked at in turn):

- Customers are informed of breaches/ outages if the national competent authority concerned determines that disclosure of the breach is in the public interest. There could be a certain value to the customers from the information if they are able to prevent criminal activities linked to the breached information.
- Companies might become more aware of potential security and resilience issues which are addressed earlier i.e. before an incident occurs. This could save them some costs in the long-run as incidents are prevented and the associated costs (for example customer compensation).
- Other UK companies linked into the respective networks in the various sectors also benefit due to network effects (i.e. a network is only as strong as the weakest link). This could lead to wider resilience in the UK economy as well and associated benefits.
- Wider benefits that are derived from an increased level of EU cooperation in relation to cyber security

<u>Potential benefits for customers</u>

Any potential benefits for customers as outlined above are likely to be dependent on various factors. One deciding factor would be how secure and resilient the company was to begin with, where customers of companies with a low initial level of security and resilience are likely to benefit more than those who are customers of companies with already a much higher level. It would be rather difficult to establish the size of this potential benefit though as it would require a very detailed understanding of each business and their customer base. Benefits here would also only be additional if it could be compared to what would have happened without the implementation of this Directive. However, establishing this counterfactual is rather difficult as we will not know what might have happened without the Directive. Additional benefits to customers are also likely to be dependent on whether they are able to use the information that they receive in cases where the national competent authority decides that the public needs to be informed. Customers will only receive any benefits from this information if they have the knowledge to use it to plan and prevent potential risks to them. Therefore, the overall potential positive impact on customers remains rather uncertain.

<u>Benefits to affected businesses</u>

With respect to the benefits outlined above for businesses, which might be able to benefit from improved cyber security and resilience are potentially uncertain. General evidence outlined below implies that there are potential benefits from the prevention of incidents happening or reducing their severity as the

associated costs of these could be seen as a proxy for the benefits that could be received. However, this is likely to depend on the effectiveness of existing measures already being implemented. If a high level of cyber security and resilience already exists then potential benefits that could be gained from increasing it further are likely to be relatively small for the businesses and might potentially not outweigh the costs associated with making the investments needed to raise this level further.

Furthermore, as part of the Call for evidence participants where asked various questions on potential benefits from the Directive. Responses to each of these are briefly outlined below

Do you think the measures as proposed in the Directive may decrease the number of incidents of significant impact your organisation may expect to receive over a year period?

- 43 of the participants in the online survey did not provide a response to this question and neither did one respondent in the manual survey
- 8 respondents in the online survey said that there would be no decrease in incidents due to the Directive, although one noted that it could help to raise awareness and 7 participants in the manual survey noted the same. Some also stated the opinion that the reporting might rather divert resources.
- Three respondents in the online survey noted that there could be a decrease but only if for example pro-active actions were taken as a result or through a concerted effort.
- 4 respondents in the manual survey noted that this would depend on the implementation of various aspects of the Directive
- One respondent in the online survey noted that this was not applicable.

Do you think the measures as proposed in the Directive may reduce the seriousness of incidents that your organisation experiences over a year period?

- 43 participants did not provide a response in the online survey and one did not in the manual responses
- 8 of the respondents to the online survey did not think that the suggested Directive would reduce the seriousness of incidents and neither did 7 of the manual respondents
- 2 respondents to the online survey indicated that it might provide benefits
- 4 of the participants that responded in a paper version considered it possible but were uncertain about the likelihood
- One respondent to the online survey indicated that this was not applicable to them

Do you think the measures may potentially increase uptake/revenue as customers perceive the Directive as improving the resilience and security of your organisation/supply chain?

- 43 respondents to the online survey provided no response to this question and neither did 2 of the manual ones
- 5 respondents to the online survey indicated that they did not see such a benefit and 6 respondents to the manual survey noted the same
- 6 respondents indicated in the online survey that these benefits could potentially occur and four in the manual responses
- One respondent in the online responses indicated that this was not applicable to them

Can you also indicate whether the Directive could provide you with any potential cost savings that are usually associated with incidents such as customer compensation, etc?

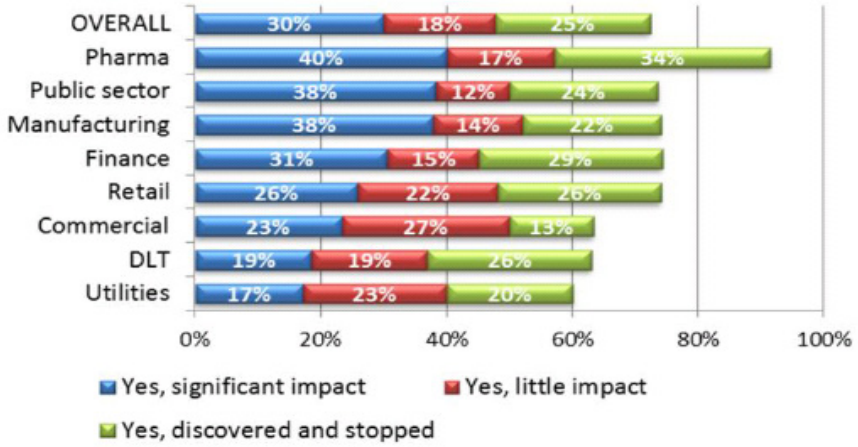
- 44 participants did not respond to this question in the online survey and neither did 2 in the manual responses
- 9 respondents indicated in the online survey that they did not see this benefit occurring and neither did 8 in the manual responses. One respondent to the manual survey highlighted that this was not known to them.
- Only one respondent in the manual responses indicated that this might be a possible benefit
- Two respondents to the online survey indicated that this was not applicable to them and so did one of the manual responses.

The Summary of Responses, which was also prepared to provide a wider overview of the contributions received from stakeholders, provides a wide range of views. It also provides some more specific points on the reporting requirements, which indicate that stakeholders thought that in particular mandatory

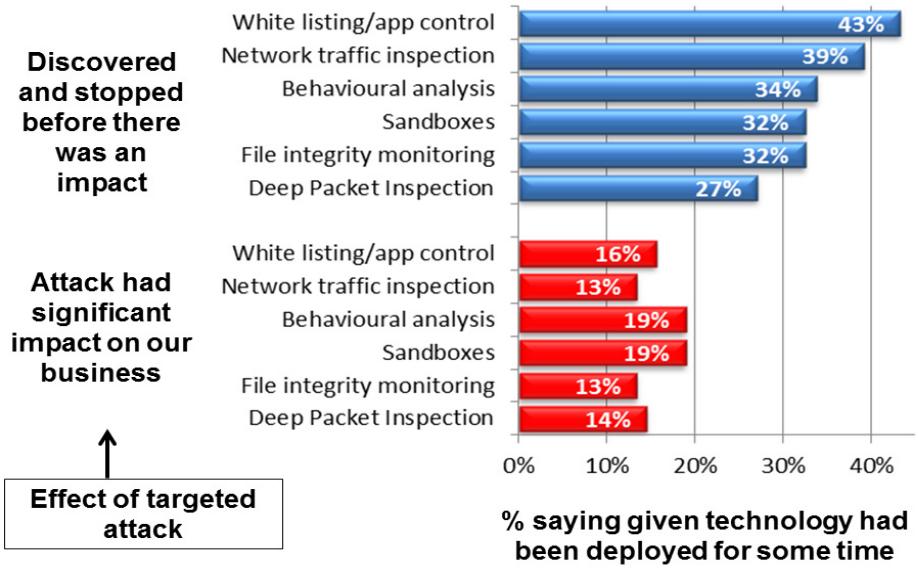
reporting and the potential for audit and sanctions would penalise organisations with strong NIS capabilities. They also indicated that this might have the effect of lowering NIS capability as organisations might only implement a minimum tick box compliance exercise instead of focussing their cyber security capability in general. They also voiced concerns that mandatory reporting might stifle existing voluntary information sharing and that resources could be diverted to comply with the Directive rather than be invested in cyber security. For further details and quotes please see the Summary of Responses to the Call for evidence.

The responses outlined above appear to be in slight contradiction to the general evidence below, which indicates potential benefits associated with increased security and resilience.
It seems that in general some simple actions could help to prevent quite a few of the cyber incidents. For example Verizon suggests in their Data Breach Investigations Report (2013) that the level of difficulty of the attacks undertaken was either low or very low for three quarters of these. They admit that a certain level of subjectivity needs to be applied here to asses whether an attack was of high or low quality (Verizon, 2013, pp. 48-49) but it might provide some level of indication that cyber criminals do not necessarily always need to apply very sophisticated methods to gain access to a system. It should also be noted that some incidents are much more difficult to prevent than others as for example with respect to incidents caused by insiders, which can be malicious but also accidental. According the PWC Information Security Breaches Survey (2013, p.14) around 84% of the large respondents suffered from a staff-related incident and 57% of the small companies that participated suffered these as well. The likelihood of staff related incidents also seems to be affected by the understanding of staff of security policy as 'companies with a poorly understood policy were twice as likely to have a staff-related breach as those with a very well understood policy'. Therefore, it should be borne in mind that not always technology or products are required but that it might be rather services and training (PWC, 2013, p. 14)

A further study undertaken by Quocirca is also providing an indication with respect to the potential effectiveness of measures taken. In a survey with around 300 responses from enterprises across Europe, they found that around 25% of the respondents had been the target of targeted attack and was able to stop this. The report also points out that a third of respondents said that they had deployed specific technology to deal with targeted attacks (slightly higher for larger organisations). However, they also found a potentially significant lack of understanding with respect to specific technology needed to protect themselves and their effectiveness as much of the technology selected against targeted attacks (such as anti-malware and firewalls) was ill suited for this purpose (Quocirca, 2013, p.10),.



There are technologies as well though which are potentially more focussed on detecting and stopping targeted attacks. This is shown in the graph below (Quocirca, 2013, p.10), outlining to which extent cyber incidents had been stopped by technology. Again though this information does not provide us with any information on the type of incident, which was either stopped or wasn't. It does seem to indicate though that potentially some incidents could be prevented by taking action.



Overall though this evidence should only be seen to provide an indication that benefits could be derived from the prevention of cyber incidents as actions are taken.

General evidence

With respect to benefits, examples of studies undertaken previously on wider economic benefits related to security and resilience (mainly from the US) appear to imply that there could be benefits from improved resilience and security. Studies have mainly focussed on transport and energy. However, it should also be borne in mind that the US has different characteristics and more importantly different requirements and policies with respect to resilience and security. Hence this could have an impact on the potential benefits estimated.

To provide an indication of the potential benefits to the UK economy i.e. the costs that could be prevented assuming that the NIS Directive leads to improved security levels and resilience of network and information systems, some examples are outlined below.

- An analysis for example in the US on storm-related energy outages implies that the US economy loses $20-55bn annually due to these events (Campbell, 2012, p.8).
- According to one provider of business continuity services power failure was the single biggest cause for invoking their services in the UK in 2011 (SunGard, 2012).
- According to one estimate the snow disruptions to the transport system in winter 2011 cost the UK £280m a day[3].
- Other estimates of transport disruptions in the US range from $400,000 to $71,000-220,000 per day in relation to the costs associated with the collapse of a bridge over the Mississippi (see Zhu, Shanjiang & Levinson, David, 2011 for details).
- The cost of metal theft, leading to transport disruptions, has been estimated to cost the UK around £1bn a year (see Evening Standard, 2011 for further details).
- Gales appear to have caused significant transport disruptions in the UK in 2007 with around 226 road traffic incidents being reported, several households were reported to have no power, flights being cancelled (BA supposedly cancelled more than 100 domestic and short-haul flights) and disruptions to several train services (see Telegraph, 2007 for further details).

Some indication of the potential benefits could also be provided by the costs that businesses currently incur due to cyber incidents and which might be reduced if either the severity of incidents is reduced or their disruptiveness.

[3] The Weather Club

The latest of PWC's Information Security Breaches surveys (2013), commissioned by BIS highlights that larger companies that responded had around 113 incidents and smaller ones around 17 in one year (Please note: This is the median not an average). Among these the most predominant form of incidents for large companies were attacks by an unauthorised outsider (around 106), followed by a distance by incidents caused by staff (18). For smaller companies incidents caused by staff were the main cause (11) but closely followed by attacks by an unauthorised outsider (10) (PWC, 2013, p. 11). In terms of the level of disruptions that the worst security incident caused the majority still said that it caused none (37%) followed by 10% of respondents saying that is caused a minor disruption which either lasted less than a day or between a day and a week respectively. Another 10% highlighted that serious disruptions caused problems for a time period of between one day and a week (PWC, 2013, p. 16). Further details are outlined in the table below.

How much disruption to the business did the worst security incident cause?

Figure 35 *(based on 104 responses)*

	None	Less than a day	Between a day and a week	Between a week and a month	More than a month
Very serious disruption	37%	2%	4%	2%	1%
Serious disruption		5%	10%	4%	1%
Minor disruption		10%	10%	5%	1%
Insignificant disruption		5%	2%	1%	0%

In terms of the financial costs to companies from the worst security incident the figures below from PWC's Information Security Breaches Survey (2013) outline these and show that for large companies the worst incidents is estimated to have costs participants between £450,000 -850,000 and for smaller companies, these are £35,000-65,000. (Please note: This result is based on only 104 responses) (PWC, 2013, p.18). These figures can provide an indication of the potential maximum costs that companies could potentially save if no incidents disrupt their services. The survey was conducted on a self selection basis though and therefore, the figures might have an upward bias as it is likely that mostly companies responded who had suffered an incident or which have a much keener interest in cyber security in general. In addition to this the response rate to this question is much smaller than the overall sample, which indicates potentially that quite a few companies were unable to estimate these costs or that the figures are potentially based on a few high outliers, which could increase these estimates as the number of companies that responded is so small. Nevertheless, they can provide a very general indication of the potential costs to business and simply that there are costs to businesses from incidents generally.

What was the overall cost of an organisation's worst incident in the last year?

Figure 39 *(based on 104 responses)*

	ISBS 2013 small businesses	ISBS 2013 large organisations
Business disruption	£30,000 - £50,000 *over 3-5 days*	£300,000 - £600,000 *over 3-6 days*
Time spent responding to incident	£2,000 - £5,000 *6-12 man-days*	£6,000 - £13,000 *25-45 man-days*
Lost business	£300 - £600	£10,000 - £15,000
Direct cash spent responding to incident	£500 - £1,500	£35,000 - £60,000
Regulatory fines and compensation payments	£0	£750 - £1,500
Lost assets (including lost intellectual property)	£150 - £300	£30,000 - £40,000
Damage to reputation	£1,500 - £8,000	£25,000 - £115,000
Total cost of worst incident on average	**£35,000 - £65,000**	**£450,000 - £850,000**
2012 comparative	*£15,000 - £30,000*	*£110,000 - £250,000*
2010 comparative	*£27,500 - £55,000*	*£280,000 - £690,000*

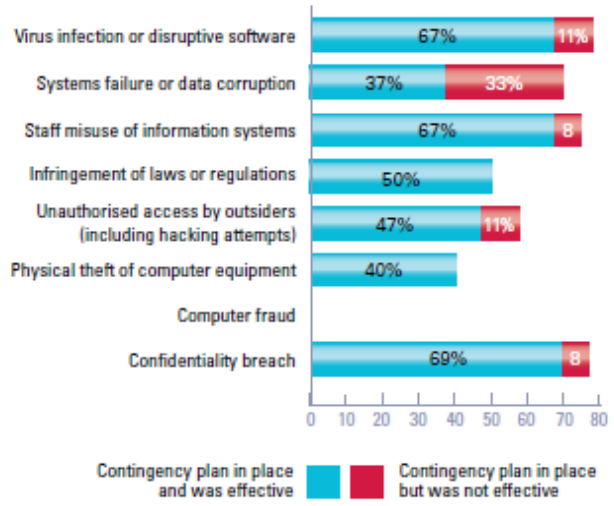
A further survey by the Federation for Small Business (see FSB, 2011 for further details) around fraud and online crime provides an additional figure on the potential costs to small businesses, which estimates that the average annual cost to small businesses of fraud and online crime at just under £4,000 per year (FSB, 2011, p.13). They also found that around three in 10 members have been a victim of online crime over the last year, with virus infections (20%) being the most common (FSB, 2011, p.17). This indicates a potentially much smaller figure compared to the PWC Information Security Breaches Survey (2013). It is a bit unclear though from the report whether companies selected themselves from the 'Voice of Small Business' Survey panel to fill in the survey or whether they were randomly selected from this panel. From the little information that is provided around methodology it seems that it was based on self –selection and therefore, the survey potentially suffers from the same issues as the PWC Information Security Breaches Survey (2013). In addition it potentially also leads to an overestimation of the potential costs given that the costs associated with fraud are also included, which are not necessarily linked to cyber security issues or disruptions to the network that is being used. Nevertheless, it provides a different perspective on the issue and a further proxy on the potential costs.

Potential benefits with respect to the reduction of these costs will also depend on the effectiveness of the measures already being implemented. If companies are already very good or effective at implementing existing measures then any additional measures are likely to render benefits that are rather small due to so-called decreasing returns to investment. This implies that benefits start to decrease with the increasing level of the associated level in security spending.

According to PWC's Information Security Breaches Survey (2013) companies are already planning for a variety of security incidents and consider how effective these might have been. The graph below reflects the results and indicates that in the majority of incidents recorded here organisations and contingency plans are rather effective except for systems failures or data corruption where 33% of the respondents indicated that they had not been (PWC; 2013, p.18).

What type of security incidents do organisations plan for, and how effective are those contingency plans?

Figure 40 *(based on 99 responses)*



The low response rate and the other potential issues related to this survey mentioned before should be taken into account here. Overall though it seems to indicate that benefits from increased resilience measures could potentially be rather small as companies are already rather effective at dealing with incidents as these occur. However, on the other hand it can be rather difficult to assess fully the potential damage that might have been done to the system sometimes and some issues might only appear after a certain while. Hence businesses could potentially overestimate the effectiveness of their own contingency plans.

Estimate of the potential benefits for affected businesses

Given the high level of uncertainty around the potential benefits one possible approach to obtain an indication of the size of these, is to estimate the size of the potential benefits that could just cover the costs of the measures that need to be taken or in other words by how much would the current costs of incidents or the number of incidents need to decrease under the implementation of the Directive to ensure that the costs under the Directive are covered?

Any potential benefits for affected businesses are likely to depend on:

- The number of incidents and whether the Directive has an impact on the number of these. It would be very difficult to establish this in practice though as the number of incidents that a company suffers from is also dependent on other factors such as knowledge level of the staff with respect to cyber security, business circumstances that might change such as M&A intentions or expansions of the business that would make it potentially a more attractive target, etc but also the development of new techniques used by hackers and whether measures to counter these are already or easily available.
- The extent to which the Directive might help to reduce the severity of incidents. Again this is likely to also depend on other factors and in particular on technology developments and whether new defence mechanisms can be developed quickly enough as well as passed on amongst them.
- The number of companies for which the Directive might potentially reduce the number of incidents and the associated costs. This is likely to be very company specific as it depends on the measures already taken and how effective these already are. Therefore it would be difficult to establish this level of detail for all the affected companies.

Hence it is rather difficult to provide a full estimate of the benefits. What we will try to provide though is the potential size of the benefit needed and the number of companies that would need to receive it under the Directive to ensure that the benefits would outweigh the costs. This could provide an indication of whether this might be achievable i.e. whether only a small number of companies would need to see a small fall in the costs associated with security incidents or whether a large number of companies would need to see a relatively large fall in costs associated with security incidents.

To be able to provide an indication of the size of the potential benefits required, we will need to make assumptions and develop proxies for the number of companies that would need to benefit, by how much the costs of the incident is reduced and the number of incidents for which this will be the case.

Number of incidents

In terms of the number of incidents this can again vary depending on the survey used. A survey undertaken by Verizon (2013, Data Breach Investigations Report) showed that 621 incidents occurred globally in 2012 (Verizon, 2013, p. 4). This survey is based on evidence collected during paid external forensic investigations and related intelligence operations conducted by Verizon. They attempt to make the collection and verification of this data as consistent as possible through the use of a framework (Verizon, 2013, pp.8-10). This is a global survey though and therefore, the number of incidents is not fully representative for the UK.

According to the Symantec's Internet Security Threat Report (2013), using a network of 69 million attack sensors, which monitor threat activities in over 157 countries and territories (Symantec, 2013, p.3), reflects that targeted attacks in 2012 increased by 42% compared with the preceding 12 months (p.20) and the average per day was 116 globally (p.14). In terms of the impact the average number of identities exposed per breach in 2012 was 604,826 (p.17) and web attacks blocked per day in 2012 were 247,350 (p.47) according to this report.

As mentioned before the PWC Information Security Breaches survey (2013, p.11) indicates a median in terms of incidents for larger companies that responded had around 113 incidents and smaller ones around 17 in one year (Please note: This is the median not an average).

The Call for evidence also asked about the number of incidents that companies reported in the last financial year. As before these results are more for information and completeness as they cannot be used due to the relatively small sample size. Results are outlined below briefly for information.

- 39 respondents to the online survey did not provide an answer to this question and three in the manual responses
- 6 participants indicated that they had no incidents during this period in the online survey and three in the manual ones
- Four institutions indicated that this was not applicable to them in the online questionnaire and one in the manual responses
- The others provided sometimes quantitative information and others just indicated that they did report incidents but not how many. 6 respondents in the online survey did so and 5 in the manual responses. The numbers ranged from 200 on average in a year but only 1% were considered to be significant to around 2-5 per year.

Unfortunately it is not possible from the global studies to deduce how many of these incidents included were in the UK and therefore, it is not possible to use these figures as an indicator for the potential maximum level of incidents in the UK. Hence the incident figures from the PWC Information Security Breaches Survey 2013 will be used here. However, it seems unlikely that companies are able to avoid any incident from ever occurring and therefore, we will also assume that for only 50% and 25% of the incidents respectively it will be possible to reduce the associated costs. These numbers are potentially rather arbitrary but should at least represent a range between the costs for all security incidents being reduced to only this being the case for a much smaller number.

Cost of incidents

The cost of incidents can vary widely depending on the report/ survey chosen, which can be in partial due to the definition used for incidents, the timeframe used or the research methodology.

One example of a benchmarking exercise undertaken by the Ponemon Institute for the UK (2013 Cost of Data Breach Study: United Kingdom) using 38 companies indicates that:

- Malicious attacks are most costly at a per capita cost (i.e. the costs per record lost) of £102, while companies experiencing system glitches or employee mistakes had a per capita cost of £79 and £76 respectively (p.7).
- Average detection and escalation costs were £0.45million in 2012. According to the study such costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors (p.11).

- Average notification costs were £0.16 million. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up (p.11).
- Post –data breach costs were £0.51 million in 2012. Ponemon indicates that these costs typically can include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions (p.12).
- Lost business costs were £0.92 million in 2012. Such costs include abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill (p.12).

The same study also indicates that per capita costs can vary by industry with services, financial services and communications suffering from the highest costs (Ponemon, 2013, p. 6). It should be borne in mind though that they acknowledge that due to the very small sample size and the fact that this is only a benchmarking exercise and not a survey, the results can only be seen as indicative but not as fully representative for the UK (Ponemon, 2013, p.20).

In contrast the Symantec Threat report indicates that the average cost per capita of a data breach was $124 in the UK in 2012 (Symantec, 2013, p.19).

As mentioned before the PWC Breach Survey indicates that for large companies the most serious incident is estimated to cost participants between £450,000 -850,000 and for smaller companies, these are £35,000-65,000. (Please note: This result is based on only 104 responses) (PWC, 2013, p.18). The survey undertaken by the FSB estimates the average annual cost to small businesses of fraud and online crime at just under £4,000 per year (FSB, 2011, p.13).

In the Call for evidence one question was related to the average cost of an incident except for the associated reporting costs of this incident.

- 39 of the participants in the online survey did not provide a response and 2 did not in the manual survey
- Six respondents indicated online that these costs were not known and three indicated the same or their inability to disclose these in the manual responses
- Three participants said that this was not applicable to them in the online survey
- Three of the manual responses said that it would depend on the type, severity of the incidents, etc.
- The other seven respondents to the online survey and the other 4 to the manual survey provided some quantitative information. This ranged from simply indicating that costs would be minimal to one respondent saying it could be either in the low thousands or in the high millions. In terms of numbers these ranged from £1,000 per incident to an average of £20,000. One organisation indicated that a particular cyber incident had cost them £70,000.

Therefore we will assume a range of potential costs for large and small companies respectively to reflect the uncertainty associated with the costs related to security incidents as these are likely to be very company specific. Given the fact that the Ponemon Institute' research is mainly a benchmarking exercise and the Symantec Report looks at per capita costs (i.e. the costs per record lost and not per incident), unfortunately these figures do not provide a good proxy for our cost estimates.

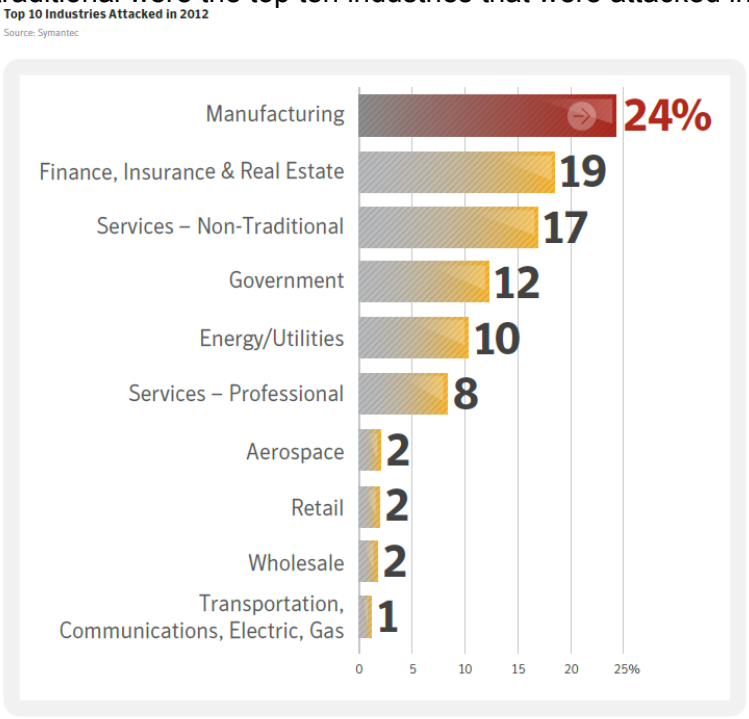
For smaller companies the FSB survey seems to provide a good indication of a lower estimate for the potential costs of £4,000 per year. We will also assume that this is the cost per incident as the number of incident this relates to is unknown. This could mean that we are overestimating the associated costs at the lower end of the spectrum. For the higher estimate the range from £35,000 – 65,000 per incident seems to be potentially suitable. However, it seems unlikely that all small businesses would suffer costs of around £65,000 per incident and therefore, we will take the median of this range of £50,000 as the highest estimate for costs. To obtain an estimate in the middle we will again use the median between £4,000 – 50,000 of £27,000.
With respect to large companies we will similarly assume that the median of the range presented in the PWC breach survey provides an indication of the upper limit for the potential cost associated with a security incident, which is £650,000. Given that there is no indication of a lower bound from the breach survey we will assume that large companies that are more similar to medium companies might suffer similar costs from an incident and thus this leads to a lower estimate of £50,000, which is the same value as used for small

businesses to represent a high level of costs per incident. The median of this range to provide an estimate for the medium case is £350,000.

In addition we would need to assume to which extent the costs could potentially be reduced. Given the uncertainty of this we will assume a range from 10- 100% i.e. 100% implying that no incident occurs as no costs are incurred.

Number of companies affected

The number of companies affected by sector is rather uncertain as it is not mentioned by any of the aforementioned surveys. The Symantec Internet Security Threat Report (2013, p.15) indicates as outlined in the graph below that manufacturing, finance, insurance & real estate and services – non-traditional were the top ten industries that were attacked in 2012.



Manufacturing was the most-targeted sector in 2012, with 24 percent of targeted attacks destined for this sector, compared with 15 percent in 2011. Attacks against government and public sector organizations fell from 25 percent in 2011, when it was the most targeted sector, to 12 percent in 2012. It's likely the frontline attacks are moving down the supply chain, particularly for small to medium-sized businesses. (Categories based on Standard Industrial Classification codes.)

The PWC Information Security Breaches Survey (2013, p.10) indicates that 93% of large organisations that responded and 87% of small businesses that participated had a security breach in the last year. Given the potential self-selection bias this is not completely representative for the UK either.

Given the high level of uncertainty around the number of companies affected we will make assumptions around how many companies would need to see a reduction in their costs associated with security breaches to cover the potential costs associated with the Directive. With respect to the sectors affected around 21,875 were SMEs and around 1,060 are large companies. Therefore, we will assume a range of the number of companies that would need to see an improvement ranging from 500 – 20,000 for small companies and ranging from 50 – 500 companies for large ones. This should provide an indication of whether only a very small number would be required or whether almost all affected companies would need to see a reduction in the costs associated with security breaches.

Potential benefits

Using the assumptions as outlined above potential benefits can be calculated for varying levels of cost reduction for all incidents, 50% and 25% of incidents respectively. Given that a reduction for all incidents due to the Directive is considered rather unlikely, the results for a reduction for 50% and 25% of incidents are considered to be potentially more likely, given that so-called zero-day vulnerabilities exist. This means that new software can have already weaknesses that cyber criminals might be able to exploit before the vulnerability is public knowledge and prior to a patch for it being available. Some of these vulnerabilities are only discovered over time and solutions to these are then provided. This also

seems to indicate though that not all cyber incidents can always be prevented. For example 14 zero-day vulnerabilities were reported in 2012 according to the Symantec Report on Breaches (2013, p.5). Furthermore, new techniques to enter systems illegally are continuously being developed against which new defences also need to be designed. For completeness though the results for all incidents are provided as well. Due to the length of the tables all results can be found in Annex 6.
It should be noted that whether the estimated benefits are large enough to cover the potential costs depends very much on the assumptions made and in some cases they do not outweigh these. As an illustrative example the median of £860.6m was chosen as the benefits figures. This assumes that between 5,000 and 10,000 small companies would require obtaining medium sized benefits (of £27,000) under the Directive for 50% of the cyber incidents. This is considered to be an already challenging target but is roughly the middle estimate of all those provided and hence it was chosen for illustrative purposes.

Benefits to the wider economy/ EU system

Wider benefits to the UK economy could also arise from an increased level of cyber security and resilience due to the fact that the Directive is aimed mainly at companies that have an extensive network. Due to the interdependent nature of the economy and the underpinning networks and systems, the costs from cyber security incidents or a lack of resilience in systems can be magnified beyond the affected company to other companies that are connected to these. It might be possible to reduce these wider costs due to an increase in the level of cyber security and resilience by companies with extensive and important networks.

Furthermore, it might also improve the competitiveness of the UK as information/ innovations held by UK companies are not leaked abroad or stolen by hackers. This could potentially benefit the economy more widely as companies are able to do business in a secure environment.

Despite this being the main aim of the Directive i.e. improve security and resilience across Member States and establish a minimum level of capabilities, it is not possible to provide an estimate for either of these wider potential benefits as the extent of interconnections between company networks, and levels of IP theft are not yet fully understood. Further information though should be collected to attempt to capture these potential benefits in more detail in the next Impact Assessment when details of the Directive have become clearer.

Benefits from increased EU cooperation

An increased level of EU cooperation could help to improve cyber security across the EU, provided that information shared between Member States remains secure. Furthermore the requirements for a national strategy as well as technical and organisational capabilities within the national competent authorities could potentially create more confidence in EU businesses with respect to trading within the EU and thus also help to further the development of a Digital Single Market. Increased levels of information sharing around incidents could also help to improve the level of preparedness as other Member States receiving the information are likely to be in a better position to do so as well as potentially preventing the spread of incidents across borders. The extent to which these benefits might appear though depends for example on the types of incidents (with respect to some information on them might help to prevent and prepare against these), the type of information shared, etc. Given the uncertainty around these factors though, this IA does not attempt to quantify these here. Again though this is one of the main objectives of the NIS Directive and further evidence should be collected to reflect these potential benefits better in the next Impact Assessment.

Conclusions
Overall further information and research would be required with respect to the various costs and benefits identified to be able to establish a relatively robust baseline and to be able to assess the additional costs and benefits from this Directive quantitatively. Furthermore, the Directive requires further practical details around implementation that could help to assess the potential costs and benefits of this Directive. Until then this IA should be considered only to provide a high level indication of the potential costs and benefits under the Directive.

At this stage though, the impact assessment indicates that the number of affected businesses could be 22,935 as a maximum. In most of the sectors currently included under the Directive, there are already measures in place in most cases, which are tailored to meet the risk profile and the nature of each sector, and either through general or specific measures could cover the disclosure of cyber security incidents in the operators and owners of the CNI. These affected businesses might need to spend

potentially an additional £1,984.2m in the High scenario and £992.1m in the Medium case. If the Directive is highly flexible and existing measures can be used to comply with the Directive, then companies might only need to incur negligible or potentially no costs at all. The estimated potential benefits from taking actions against cyber incidents are very dependent on the underlying assumptions where an attempt was made to quantify these. In some cases though it was not possible to quantify these benefits and therefore no attempt was made to do so through proxies either.

Annex 1 – Background on Article 13

Services that are currently captured under Article 13 are only in the telecommunications sector and include specifically (see ENISA 1&2, 2013 for further details):

- Fixed telephony services
- Fixed internet services
- Mobile telephony services
- Mobile internet services
- Message services
- E-mail services

The information that needs to be reported on incidents is:

- Services impacted (selection)
- Number of users (percentage, national customer base)
- Duration (hours)
- Root cause category
- Emergency calls or interconnections impacted
- Details about the incident

In addition the cause of outages needs to be recorded which can be due to:

- Natural phenomena
- Human errors
- Malicious attacks
- Hardware/ software failures
- Third party failures

Thresholds need to be passed for incidents to qualify for reporting if the incident:

- Lasts more than an hour and the percentage of users affected is more than 15%
- Lasts more than 2 hours and the percentage of users affected is more than 10%
- Lasts more than 4 hours and the percentage of users affected is more than 5%
- Lasts more than 6 hours and the percentage of users affected is more than 2% or of it
- Lasts more than 8 hours and the percentage of users affected is more than 1%

A non-exhaustive list of assets includes:

- Information: Databases and data files, configuration setups, contracts and agreements, documentation and manuals, operational procedures and plans, audit trails, logs, archives (personal information excluded as part of Data Protection Act).
- Software assets: Network and information systems software, application software, software for subscribers, development tools, operational tools, operational software
- Physical assets: Facilities, switches, cables, terminal equipment, network and information systems hardware, network equipment, removable media
- Services: Computing services, network services, general utilities such as power supply, temperature and humidity control
- People: Telecommunications engineers, customer service staff, IT support staff and users of service providers

Security measures needed can include (non-exhaustive list):

- Information security policy
- Governance and risk management framework

- Security roles and responsibilities
- Managing third party networks or services
- Background checks on personnel
- Security knowledge and training
- Personnel changes
- Handling violations
- Physical and environmental security of facilities
- Security of supplies
- Control of access to network and information systems
- Information security of network and information systems
- Operational procedures and responsibilities
- Change management procedures
- Asset management
- Standards and procedures for incidents
- Incident detection capability
- Incident response and escalation processes
- Incident reporting and communication plans
- Service continuity strategy and contingency plan
- Disaster recovery capability
- Monitoring and logging policies
- Exercise contingency plans
- Network and information systems testing
- Security assessment and security testing
- Compliance monitoring and audit policy

Most of these measures are already required under certain standards. In particular relevant for telecoms and other sectors are the following:

- ISO/ IEC 27001: This is an international standard that defines an information security management system providing a framework for security risk management within an organisation. It can be applied to any organisation and it is possible to obtain certification against the standard. It does not stipulate any specific technical measures.
- ISO/ IEC 27002: This standard complements the ISO 27001 standard by listing a control set comprising 133 technical, procedural, personnel and physical controls that can be selected to manage risk, and includes the implementation guidance on each. It is not possible to certify against this standard.
- BS25999: This is a British standard that defines business continuity management systems. It can be applied to any organisation and it is possible to obtain certification against the standard.

There are other standards that mainly relate to the telecoms sector and which are therefore not relevant for other sectors.

Annex 2 – Other relevant EU documents

Data protection
Data controllers are obliged by the data protection regulatory framework to place security measures to protect personal data. Furthermore data controllers would have to report breaches of personal data to the national supervisory authorities under Commission proposals for a General Data Protection Regulation in 2012.

Critical Infrastructure
The European Programme for Critical Infrastructure Protection (EPCIP) sets out the overall approach to the protection of critical infrastructures in the EU (Directive 2008/114). The EPCIP does not require operators though to report significant breaches of security and does not set up mechanisms for the Member States to cooperate and respond to incidents.

European Cybercrime Centre
The Commission adopted in 2012 a Communication on the establishment of a European Cybercrime Centre, which will act as the focal point in the fight against cybercrime in the EU.

Annex 3 – Further details on the Commission's Proposal

The Directive outlines clearly the reasoning and the evidence for the impact of NIS incidents including natural disasters and human errors as well as malicious attacks. The Commission's IA also highlights the proportionality of the measures outlined and states that the costs of the preferred option would largely have to be incurred by the Member States that are less advanced and appear to be small in relation to the economic and social losses and damages which could be caused by NIS incidents. Furthermore, they note that most companies are already data controllers and they only need to ensure a basic level of protection proportionate to the risks faced (EC6, 2013, p.27). The Directive applies to all relevant incidents and risks and all network and information systems, except for those providing public communication networks or publicly available electronic communication services, which are already subject to specific security and resilience requirements (see Article 13 of Directive 2002/21/EC). All measures also apply to SMEs except for micro businesses. Furthermore, the Commission outlines that any requirements should be proportionate to the risk presented by the network or information system concerned. This is to avoid in particular disproportionate financial and administrative burdens on smaller companies (EC6, 2013, p. 38).

The Directive also requires the setting up of a well-functioning national/ Governmental CERT. They would deal with security risks and incidents and would need to have adequate staff and financial resources to fulfil their tasks (see Article 7). A national contingency and cooperation plan also needs to be adopted for the protocols for communication and cooperation amongst the relevant institutions in case of NIS incidents of a larger scale. The strategic objectives of Member States would also need to be outlined in a national cyber security strategy and adopted by the Member States respectively.

In addition a national competent authority for NIS needs to be appointed to take on the coordination and cross-border cooperation role. Again it needs to have appropriate technical, financial and human resources and is responsible to elaborate the national cyber security strategy (see Article 6). This authority could be the CERT but the CERT would act under the supervision of the competent authority. They should form a network to be able to cooperate at the EU level and to be able to exchange information on threats and incidents as well as reacting to those that cross borders. Sensitive and confidential information between these competent authorities would need to take place through an infrastructure that provides security and confidentiality (see Article 8 and 9).

Related measures

Given a wide range of measures cited by the Commission's IA that are already related to security and the argument that a lot of the costs would not be caused by this Directive as those companies which are data controllers already collect a lot of the information. Under the respective Directive (Directive 95/46/EC) controllers of personal data need to implement appropriate technical and organisational measures to protect these, where the level of security needs to be 'appropriate to the risks presented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation' (EC6, 2013, p.26). Under these measures, personal data is protected against accidental or unlawful destruction or accidental loss and any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access or alteration of personal data (EC6, 2013, p26). Hence incidents involving personal data can already be reported but any other breach affecting the provision of a service by these companies that is not related to personal data is not. The Commission's IA highlights that 'all players who are data controllers (e.g. a bank or a hospital) are already obliged to put in place security measures that are proportionate to the risks faced but only need to report on those where security breaches are related to personal data' (EC6, 2013, p. 27). Therefore, additional security spending might be required that is not related to personal data as well as needing to put in place processes and systems to supervise other areas of these that are not linked to personal data. This does not seem to be considered by the Commission's IA.

Furthermore, the preferred option also proposes 'to impose NIS risk management and reporting requirements on public administrations (e.g. central ministries, local authorities, land registries) and key private players' (EC6, 2013, p. 38). This in particular applies to operators in 'specific critical sectors i.e. banking, energy (electricity and natural gas), transport, health, enablers of key Internet services and the public administrations' (EC^, 2013, p. 38). It excludes though micro businesses (companies with less than 10 employees) within these sectors (EC6, 2013, p. 38). It should be noted though that the list of market operators included in the Commission's IA slightly differs from that presented in the NIS

Directive. This could impact on the estimates of costs and benefits and needs to be clarified by the Commission as more details associated with the Directive continue to be developed.

The Commission's IA does not provide more specific information on the details of the various requirements outlined above. However, they highlight that the ENISA guidelines on the security measures in Article 13a of the Framework Directive could be seen as an indication of these. Activities required therefore, are likely to include (EC6, 2013, p. 38-39):

- Regular risk analysis of specific assets. This can be based on standard methodologies such as ISO 27005 for example.
- Governance and risk management, which includes an appropriate security policy, a governance and risk management framework to identify and address risks and an appropriate structure of security roles and responsibilities.
- Human resources security, including for example background checks, regular security training, process for handling of security breaches, etc. This applies to employees, but also contractors and third-party users.
- Security of systems and facilities focused for example on physical and environmental security of facilities, security of supplies or appropriate security of network and information systems.
- Operation management including operational procedures and responsibilities or assess management procedures for the verification of asset availability and status for example.
- Incident management including required procedures as well as having capabilities to detect incidents, clear responsibilities for dealing with these and a set time frame to do so, etc.
- Business continuity management. This can include monitoring, testing and auditing of network and information systems, facilities and security measures.

Only incidents that seriously compromise 'the operation of network and information systems and thus having a significant impact on the continuity of services and supply of goods which rely on network and information systems' will need to be reported to the national competent authority, (EC5, 2013, p.39) similarly to Article 13a &b. This is likely to require organisations though to implement a level of capability deemed 'appropriate' to the risks that they face and also report incidents of 'significant impact' (EC5, 2013, p.24) . Neither the term 'appropriate' nor 'incidents of significant impact' seems to have been defined in detail in the Directive. The newly formed National Competent Authority would act as the regulator. The sanctions for not meeting these requirements are also not defined, although the Directive states that they should be 'effective, proportionate and dissuasive' (EC5, 2013, p.25).

Currently no Member State has a non sector specific national structure in place for mandatory reporting on network and information systems incidents, although both the Netherlands and Germany are looking at this structure for critical infrastructure, which again though is likely to be sector specific to a certain degree. On a sector basis, the telecoms sector has a requirement for incident reporting that would lead to impact on consumers; this would include NIS incidents – this proposed Directive utilises the reporting structures of this example as a model for the measures it seeks to introduce.

This regulation directly seeks to address the disparity between capability by establishing minimum capacity building and planning requirements as highlighted in the problem this Directive is attempting to address. The regulatory measures set out could however have a potentially negative impact on general capacity building and create perverse incentives for organisations to deliberately keep their capability at the minimum requirements rather than foster a culture of risk management, which is identified as one of the objectives of the Directive.

Nevertheless, they consider that the additional costs remain rather limited given that many measures have already been taken based on existing regulatory obligations (EC6, 2013, p.49).

In terms of estimating the potential costs, they highlight that estimates around NIS spending can be difficult to separate from other associated costs such as general IT spending or given its confidential nature companies are less willing to disclose the details (EC6, 2013, p. 50).

In terms of the potential costs they investigate (see EC6, 2013, pp.50-54 for further details):

- Costs for the Member States associated with building up NIS capabilities and cooperation at EU level, which includes:

- the establishment of a national/ Governmental CERT
- establishment of a NIS competent authority, where they mainly assume that Member States would choose existing bodies to take on the additional tasks to be executed by this body.
- Pan-European cyber incident exercises using experts from the various Member States
- Costs related to the cooperation between competent authorities within the network. They assume this to be limited to travel and subsistence expenses only for two participants per Member State and 3 meetings per year.
- Costs related to the common website to publish non-confidential information on threats, incidents and response adopted. Linked to this website, there might be other tasks that will need to be carried out.
- Costs for establishing the physical infrastructure necessary for the sharing of information in the network of competent authorities and CERTs. There might be a possibility to adapt existing infrastructure for this purpose and thus would limit the associated costs.

- Compliance costs for public administrations and key private players. This was calculated as the difference between spending according to best practices and the current actual spending in the various relevant sectors. They estimate that the total additional NIS compliance costs would reach around €1-2bn for both the public and the private sectors. This value also takes into account that most of the affected entities are already supposed to be compliant with existing security requirements such as those obligations for data controllers. Given the difficulty to assess this potential impact, an assumption is made that a range from 40-70% can be applied to the cost estimates of the private sector, which then reduces the initial value of €3.12bn. A further estimation is being undertaken for SMEs specifically to show compliance costs per SME would only reach around €2,500-5,000. They do acknowledge that given the changing threat picture and changes in technology as well, it is rather difficult to estimate how these costs might evolve over time (EC6, 2013, pp. 51-53).
- Costs for public administrations and key private players associated with reporting NIS incidents with a significant impact, which includes:
  - The expected cost per breach notification
  - Costs associated with investigations related to breach notifications such as security audits for example that need to be undertaken by market operators at the request of the national competent authority for example.

Assumptions

Overall the assumptions being made to underpin the values appear to be rather opaque as a full explanation for the choice of values appears to be lacking sometimes. This is in particular of importance in relation to the estimation of the compliance costs, which is significantly reduced by a range of 40-70%. This assumption is made as companies are often already data controllers and therefore are already obliged to put in place security measures that are proportionate to the risks faced and they need to report on those where security breaches are related to personal data (EC6, 2013, p. 52). However, it seems rather unclear why this particular range was chosen compared to for example 10-30%. Furthermore, the underpinning assumption related to the targeted security spending, which represents the 'best in class' appears to be mainly based on a report undertaken by Gartner. Overall Gartner estimates that security spending will increase by 8.4% in 2012 (EC6, 2013, p.86). A breakdown by sectors or company size was not considered nor any form of sensitivity analysis of this value in the IA, which would have been helpful. In addition to this the IA assumes that this increase in security spending is certain to take place in the next year and therefore, deducts the associated amount from the compliance costs, thus reducing the overall value further. Given that they stress earlier that making assumptions about changing threat pictures and technological development is rather difficult it seems rather surprising that they do something related here. This leaves them with an overall estimate for the costs of €937.2 -1,874.5 Mio where supposedly also half of the costs are incurred by the public sector (€577.4 – 1,154.8 Mio) (EC6, 2013, p.90).

Given the two key assumptions outlined above (i.e. 40-70% reduction and the assumed increase in security spending) we will look briefly here at what the figures might look like without these assumptions.

Reversing the assumption of a 40-70% reduction only would give us an overall cost of €3,124 Mio. for all of the 42,000 companies in the EU that they include. In addition to this we can reverse the assumed increase in security spending of 8.4%. Table 4 below outlines the values for ICT security spending as a % of total ICT spending before and after this assumed increase.

Table A.1 – Share of ICT security spending as % of total ICT spending

	Energy	**Transportation**	**Banking and financial services**	**Healthcare providers**	**ICT sector (excl. telecom)**	**Public sector**
Before	6.1%	2.8%	5.0%	4.0%	5.5%	3.9%
After	6.61%	3.04%	5.42%	4.34%	5.96%	4.23%

Similarly to the Commission's IA we will assume that the Energy sector represents the 'gold standard' and that other sectors should aspire to the same level of security spending as well as assuming the same share of IT spending as a % of total revenue for each of the sectors and overall revenue for each of the sectors. The various components used to provide an indication by how much the assumed increase in security spending decreases the overall amount in security spending are outlined in Table A.2 below. This leaves us in total with a reduction in the potential additional security spending by around €585Mio across the EU 27.

Table A.2 – Decrease in security spending

	Energy	**Transport**	**Banking and financial services**	**Healthcare providers**	**ICT sector (excl. Telecom)**	**Public sector**
Difference between before and after figures	0.5%	0.24%	0.42%	0.34%	0.46%	0.33%
IT spending as % of total revenue	1.1%	3%	6.5%	3.3%	7.6%	3.6% (as% of operating costs)
Additional share of IT spending as % of total revenue	0.0056%	0.0072%	0.0273%	0.0112%	0.035%	0.01188%
Revenue (in € Mio.)	876,009	366,509	731,129	298,961	30,000	2,241,853
Additional costs (in € Mio.)	49.1	26.4	199.6	33.5	10.5	266.3

Options

Furthermore, the third option considered in the IA is dismissed as they argue that it is unlikely that Member States would reach similar levels of national capabilities and preparedness via voluntary initiatives at the EU level. Therefore, Member States that are closely working together on these issues already would continue to do so but not others as there is also no coherent framework to do so. On a

national level though Member States would introduce requirements for public administrations and key private players, leading to some of the benefits earlier identified (EC6, 2013, pp.55-56).

Overall though this option does not appear to be a very distinct alternative as it is not very different from their preferred option as only the mechanism at the EU level has been changed to become voluntary. Hence it seems that a more distinguished third option would have been helpful for a comparison.

.

Benefits

The potential associated benefits for the preferred option are only outlined qualitatively but not quantitatively. The key reason for not assessing the potential benefits are various difficulties that arise including a lack of information on the frequency, pace and gravity of NIS incidents as well as the lack of knowledge in terms of the extent to which the implementation of the Directive would mitigate the impact of security incidents (EC6, 2013, p.58).

The IA refers to potential economic and social impacts including for example improvements in business and consumers' confidence in the digital world as they potentially feel more secure and improvements to risk assessments and management in the respective sectors (EC6, 2013, pp.48-49).

In addition they highlight potential improvements in the competitiveness of the affected sectors. This includes for example the potential for product/ service innovation in light of the Directive as well as competition in the internal market due to increased harmonisation (EU IA, pp. 49). They also include some estimates around actual or potential costs related to security incidents to reflect the scale of the issue and to indicate that the Directive could contribute to reducing these (EC6, 2013, p.58). None of these benefits though were fully quantified.

Annex 4 – Summary of the questions posed to the Commission

These questions can also be found in the Summary of Responses for the Call for evidence.
In summary, the specific questions and further detail we request of the Commission are as follows:

1. Further clarification of the market operators that will be subject to the Directive.
2. Further justification for why specific sectors have been included, in particular enablers of information society services.
3. A more developed assessment of significant impacts including social/employment impacts, competitiveness, data protection and international aspects.
4. More detail on the potential unintended consequences of the proposal
5. The development of a risk register associated with the measures.
6. Further breakdown of the impacts and benefits of the proposal on different groups, such as multinationals and SMEs.
7. Further analysis of potential barriers to entry for new entrants to these sectors, and in particular consideration of the impact for proposals might have on innovation in the sectors affected.
8. Further analysis of the various issues that need to be resolved to achieve a comparable level of national capability and preparedness, and a comparison of the advantages and disadvantages of both a voluntary and legislative approach.
9. Further detail on why a voluntary (or mixed voluntary/legislative approach) was not assessed in more detail.
10. A more detailed analysis of how voluntary activities could play a role in enhancing EU wider capability in Network and Information security.
11. Further analysis of the responses to the Commission's consultation, and publication of the responses.
12. Further breakdown of the data received in the consultation by sector, organisational size and geographical distribution of the figures cited in Annex 1 of the Impact Assessment.
13. Further information for why the energy sector's current investment is considered as a target for other sectors (as well as all company sizes within these sectors.)
14. Further clarity for why healthcare providers will need to increase ICT security spending (as % of total ICT spending) to the same level as the energy sector.
15. An update to the Impact Assessment once there are more details on where the thresholds will be set through delegated acts.

16. Further information, including a more detailed breakdown on the relevant regulations that underpin the assumption that between 40-70% of additional required ICT security spending will not be caused by the NIS Directive.
17. More detail on analysis of ongoing costs.

Annex 5 – Read across to terms used by European Commission

Definitions used by the Directive, SIC codes used and number of companies falling under this definition

Please note that SIC codes appear in some case more than once as different aspects of the descriptions are captured by the same SIC code (see ONS, 2007 for further details). In the calculations for the total figures of companies potentially affected these were only included once to avoid double counting.

Sector	Directive Description	SIC description	SIC code	Number
Energy	Electricity and gas suppliers	Electricity and gas supply	35.1 & 35.2	135
	Electricity and/ or gas distribution system operators and retailers for final consumers	Electric power generation, transmission and distribution	35.1	110
	Natural gas transmission system operators	Manufacture of gas, distribution of gaseous fuels through mains	35.2	25
	Storage operators and LNG operators	Manufacture of gas, distribution of gaseous fuels through mains	35.2	25
	Transmission system operators in electricity	Electric power generation, transmission and distribution	35.1	110
	Oil transmission pipelines and oil storage	Transport via pipeline (gases, liquids, water slurry and other commodities via pipelines	49.5	10
	Electricity and gas market operators	No specific one available but implicitly included in 35.1 & 35.2		
	Operators of oil and natural gas production, refining and treatment facilities	Extraction of crude petroleum and extraction of natural gas; Manufacture of refined petroleum products	6.1, 6.2 & 19.2	95
Transport	Air carriers (freight and passenger transport)	Air carriers (passengers and freight)	51.1 & 51.2	155
	Maritime carriers (sea and coastal passenger water transport	Maritime carriers (sea and coastal passenger and freight water	50.1 & 50.2	175

	companies and sea and coastal freight water transport companies)	transport)		
	Railways including infrastructure managers, integrated companies and railway transport operators	Passenger rail transport, interurban and freight rail transport	49.1 & 49.2	35
	Airports and ports	Support activities for transportation	52.2	1,500
	Traffic management control operators	Support activities for transportation	52.2	1,500
	Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities	Warehousing and storage	52.1 & 52.2	2,170
Finance	Banking including credit institutions and electronic money institutions	Financial service activities except insurance and pension funding and excluding activities of holding companies	64 except for 64.2	1,025
Financial market infrastructures	Stock exchanges and central counterparty clearing houses	Activities auxiliary to financial services, except insurance and pension funding	66.1	1,325
Health	Health care settings (including hospitals and private clinics) and other entities involved in health care provisions	Human health activities and residential care activities	86 & 87	16,665
Information society enablers	E-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores	Data processing, hosting and related activities, web portals	63.1	350

Public administrations	Public administrations	Public administration and defence, compulsory social security	84	795

Source: BIS, Business population estimates 2012, BIS: business population estimates 2010 to 2012 - Publications - Inside Government - GOV.UK; except for Public Administrations where UK: Business Activity, Size and Location – 2012 was used; UK Business: Activity, Size and Location, 2012

Definitions used by the Commission's Impact Assessment, SIC codes and number of companies falling under this definition

Please note that SIC codes appear in some case more than once as different aspects of the descriptions are captured by the same SIC code. In the calculations for the final figures of companies potentially affected these were only included once to avoid double counting.

Sector	Commission's IA description	SIC description	SIC code	Number
Energy (electricity and gas market)	Main electricity generating companies (i.e. those dealing with at least 5% of the country's electricity or gas)	Electric power generation, transmission and distribution	35.1	110
	Electricity retailers for final consumers	Electric power generation, transmission and distribution	35.1	110
	Entities bringing natural gas into the country	Extraction of natural gas	6.2	5
	Retailers selling natural gas to final consumers	Manufacture of gas, distribution of gaseous fuels through mains	35.2	25
Transport	Air carriers (freight and passenger air transport)	Air carriers (passengers and freight)	51.1 & 51.2	155
	Maritime carriers (sea and coastal passenger water transport companies and the number of sea and coastal freight water transport companies)	Maritime carriers (sea and coastal passenger and freight water transport)	50.1 & 50.2	175
	Railways (infrastructure managers, integrated companies and railway transport operators	Passenger rail transport, interurban and freight rail transport	49.1 & 49.2	35
	Airports (EU airports with more	Support activities	52.2	1,500

	than 150,000 passenger unit movements per year) and ports	for transportation		
	Traffic management and control operators	Support activities for transportation	52.2	1,500
	Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities	Warehousing and storage	52.1 & 52.2	2,170
Banking	Credit institutions and stock exchanges	Financial service activities except insurance and pension funding and excluding activities of holding companies	64 except for 64.2	2,350
Health	Hospitals including private clinics	Human health activities	86	10,410
Enablers of internet services	E-commerce platforms, social networks, search engines, cloud providers	Data processing, hosting and related activities, web portals	63.1	350
Public administration	Central, state, local Government and social security funds	Public administration and defence, compulsory social security	84	795

Difference between number of companies falling under the definition used by the Directive and the Commission's Impact Assessment

Energy	Transport	Banking/ Finance	Health	Information services enablers	Public administration
100	0	0	6,255	0	0

Difference between the number of companies falling under the definition used by the Directive and the numbers used in the Commission's Impact Assessment

Energy	Transport	Banking/ Finance	Health	Information services enablers	Public administration
180	507	1,954	14,805	N/A	N/A

Annex 6 – Potential benefits

Table A.3 – Potential benefits (in £ m) for small companies assuming low costs of £4,000 and 17 incidents per year (100%)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	1.7	3.4	8.5	17.0	34.0	68.0
10% cost reduction	3.4	6.8	17.0	34.0	68.0	136.0
25% cost reduction	8.5	17.0	42.5	85.0	170.0	340.0
50% cost reduction	17.0	34.0	85.0	170.0	340.0	680.0
75% cost reduction	25.5	51.0	127.5	255.0	510.0	1,020.0
100% cost reduction	34.0	68.0	170.0	340.0	680.0	1,360.0

Comparison to the High case (Potential costs of £533.7)
The table above reflects that if the associated costs of security incidents are rather low then even taking into account a reduction of 25-50% would be required for 20,000 of the small affected companies for the costs of the Directive to outweigh the benefits in this case. Another possible case is for only 10,000 affected companies to see a reduction in the costs associated with security incidents of 75-100% for the potential benefits to outweigh the potential costs associated with increased security spending.

Comparison to the Medium case (Potential costs of £266.8)
In the medium case for security spending, either around 20,000 companies would require a 10-25% reduction in costs associated with security incidents or 5,000 companies would require a 75-100% reduction to ensure that the potential benefits outweigh the costs in this case.

In both cases outlined above a rather large number of companies would require a significant reduction in the costs associated with security incidents to outweigh the potential costs, which seems overall rather unlikely to occur.

Table A.4 - Potential benefits (in £m) for small companies assuming medium costs of £27,000 and 17 incidents per year

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	11.4	22.9	57.3	114.7	229.5	459.0
10% cost reduction	22.9	45.9	114.7	229.5	459.0	918.0
25% cost reduction	57.3	114.7	286.8	573.7	1,147.5	2,295.0
50% cost reduction	114.7	229.5	573.7	1,147.5	2,295.0	4,590.0
75% cost reduction	172.1	344.2	860.6	1,721.2	3,442.5	6,885.0
100% cost reduction	229.5	459.0	1,147.5	2,295.0	4,590.0	9,180.0

Comparison to the High case (Potential costs of £533.7)
The results indicate again that there are several possibilities where the potential benefits could outweigh the costs. The spectrum of possibilities ranges from at least 20,000 companies to experience a reduction of the associated costs by 5-10 % to at least 2,500 companies to benefit from a reduction of the costs associated with security incidents by 50-75%

Comparison to the Medium case (Potential costs of £266.8)
In the Medium case for additional security spending again a range is possible with at least 10,000 companies need to experience a reduction in the costs associated with security incidents of 5-10% to 1,000 small companies experiencing a reduction of 50-75% in the costs associated with security incidents.

Again the reductions required or the number of small companies that need to realise these benefits are rather large for all incidents in one year.

Table A.5 - Potential benefits (in £m) for small companies assuming high costs of £50,000 and 17 incidents per year

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	21.2	42.5	106.2	212.5	425.0	850.0
10% cost reduction	42.5	85.0	212.5	425.0	850.0	1,700.0
25% cost reduction	106.2	212.5	531.2	1,062.5	2,125.0	4,250.0
50% cost reduction	212.5	425.0	1,062.5	2,125.0	4,250.0	8,500.0
75% cost reduction	318.7	637.5	1,593.7	3,187.5	6,375.0	12,750.0
100% cost reduction	425.0	850.0	2,125.0	4,250.0	8,500.0	17,000.0

Comparison to the High case (Potential costs of £533.7)
At least around 10,000 small companies require a decrease in incidents costs of 5-10% for all incidents for the potential benefits to outweigh the potential costs due to additional security spending.
On the other side of the spectrum around 1,000 companies would require a reduction in costs of 50-75% for all incidents.

Comparison to the Medium case (Potential costs of £266.8)
In comparison to the costs under the medium case around 5,000 companies need to experience a 5-10% cost reduction for the potential benefits to outweigh the potential costs. The smallest number of companies that would require a reduction in costs of around 50-75% is around 500 small companies.

Table A.6 – Potential benefits for large companies assuming low costs of £50,000 and 113 incidents per year (100%)

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	14.1	28.2	56.5	113.0	141.2
10% cost reduction	28.2	56.5	113.0	226.0	282.5
25% cost reduction	70.6	141.2	282.5	565.0	706.2
50% cost reduction	141.2	282.5	565.0	1,130.0	1,412.5
75% cost reduction	211.8	423.7	847.5	1,695.0	2,118.7
100% cost reduction	282.5	565.0	1,130.0	2,260.0	2,825.0

Comparison to the High case (Potential costs of £1,450.6)

If all incidents experience a reduction in costs of 50-75% for 500 companies then the potential benefits could outweigh the potential costs. On the other side of the spectrum if 400 companies experience a reduction in the costs associated with all security incidents of 50-75% then the potential benefits could outweigh the costs.

Comparison to the Medium case (Potential costs of £725.3)
For the additional costs in the medium case to be outweighed by the potential benefits either around 500 companies will need to experience a reduction in incidents costs of 25-50% or around 200 companies will need to experience a reduction of 50-75%.

Table A.7 - Potential benefits (in £ m) for large companies assuming medium costs of £350,000 and 113 incidents per year

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	98.8	197.7	395.5	791.0	988.7
10% cost reduction	197.7	395.5	791.0	1,582.0	1,977.5
25% cost reduction	494.3	988.7	1,977.5	3,955.0	4,943.7
50% cost reduction	988.7	1,977.2	3,955.0	7,910.0	9,887.5
75% cost reduction	1,483.1	2,966.2	5,932.5	11,865.0	14,831.2
100% cost reduction	1,977.5	3,955.0	7,910.0	15,820.0	19,775.0

Comparison to the High case (Potential costs of £1,450.6)
At least around 500 companies will need to experience a reduction in the incident costs of 5-10% for all incidents in that year for the potential benefits to outweigh the costs or 50 companies will need to experience a reduction of 50-75% for all incidents to achieve this.

Comparison to the Medium case (Potential costs of £725.3)
At the most 200 companies will need to achieve a reduction in the costs associated with security incidents of 5-10% or at the least 50 of the affected large companies will need to see a reduction of 25-50% for the potential benefits to outweigh the potential costs.

Table A.8 - Potential benefits (in £ m) for large companies assuming high costs of £650,000 and 113 incidents per year

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	183.6	367.2	734.5	1,469.0	1,836.2
10% cost reduction	367.2	734.5	1,469.5	2,938.0	3,672.5
25% cost reduction	918.1	1,836.2	3,672.5	7,345.0	9,181.0
50% cost reduction	1,836.2	3,672.5	7,345.0	14,609.0	18,362.5
75% cost reduction	2,754.3	5,508.7	11,017.5	22,035.0	27,543.7
100% cost reduction	3,672.5	7,345.0	14,690.0	29,380.0	36,725.0

Comparison to the High case (Potential costs of £1,450.6)

In this case around 200 large companies will need to see a reduction of security incident costs of 5-10% or around 50 will need to see a reduction of 25-50% for the potential benefits to outweigh the potential costs.

Comparison to the Medium case (Potential costs of £725.3)
For the potential benefits to outweigh the potential costs in this case either 100 companies will need to experience a reduction of 5-10% with respect to the costs associated with security incidents or 50 large companies require a reduction of 10-25%.

Table A.9 – Potential benefits in (£ m) for small companies assuming low costs of £4,000 and 9 incidents per year (50% of incidents)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	0.85	1.7	4.2	8.5	17.0	34.0
10% cost reduction	1.7	3.4	8.5	17.0	34.0	68.0
25% cost reduction	4.2	8.5	21.2	42.5	85.0	170.0
50% cost reduction	8.5	17.0	42.5	85.0	170.0	340.0
75% cost reduction	12.7	25.5	63.7	127.5	255.0	510.0
100% cost reduction	17.0	34.0	85.0	170.0	340.0	680.0

Comparison to High case (Potential costs of £533.7)
As outlined in Table 15 above either around 20,000 companies would need to see a reduction of 75-100% in half of the incidents they experience for the potential benefits to outweigh the potential costs of additional security spending.

Comparison to the Medium case (Potential costs of £266.8)
Here either 20,000 of the small affected companies would need to see a fall in security incident costs of 25-50% or at least 10,000 companies a reduction of 75-100% for the potential benefits to outweigh the potential costs.

Table A.10 – Potential benefits in (£ m) for small companies assuming medium costs of £27,000 and 9 incidents per year (50% of incidents)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	5.7	11.4	28.6	57.3	114.7	229.5
10% cost reduction	11.4	22.9	57.3	114.7	229.5	459.0
25% cost reduction	28.6	57.3	143.4	286.8	573.7	1,147.5
50% cost reduction	57.3	114.7	286.8	573.7	1,147.5	2,295.0
75% cost reduction	86.1	172.1	430.3	860.6	1,721.2	3,442.5
100% cost reduction	114.7	229.5	573.7	1,147.5	2,295.0	4,590.0

Comparison to High case (Potential costs of £533.7)

Either around 20,000 small companies will need to see a fall in security incident costs for half of those that they experience in a year of 10-25% or at least 2,500 companies will need to experience one of 75-100% for the potential benefits to outweigh the costs, where the latter seems potentially less likely.

Comparison to the Medium case (Potential costs of £266.8)
At least 2,500 companies will need to see a reduction in security incident costs of 25-50% for half of the incidents that they experience or 20,000 small companies will need to see a fall in costs of 5-10% for the potential benefits to outweigh the potential costs.

Table A.11 – Potential benefits in (£ m) for small companies assuming high costs of £50,000 and 9 incidents per year (50% of incidents)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	10.6	21.2	53.1	106.2	212.5	425.0
10% cost reduction	21.2	42.5	106.2	212.5	425.0	850.0
25% cost reduction	53.1	106.2	265.6	531.2	1,062.5	2,125.0
50% cost reduction	106.2	212.5	531.2	1,062.5	2,125.0	4,250.0
75% cost reduction	159.3	318.7	796.8	1,593.7	3,187.5	6,375.0
100% cost reduction	212.5	425.0	1,062.5	2,125.0	4,250.0	8,500.0

Comparison to High case (Potential costs of £533.7)
For half of all incidents that small companies experience, costs would need to fall by 5-10% for 20,000 companies or by 50-75% for 2,500 companies for the potential benefits to outweigh the potential additional costs from security spending.

Comparison to the Medium case (Potential costs of £266.8)
At least 10,000 small companies would need to see a reduction in security incident costs for half of the incidents that occur of 5-10% or 1,000 companies would need to experience at least a reduction of 50-75% for these for the potential benefits to outweigh the potential costs.

Table A.12 - Potential benefits (in £ m) for large companies assuming low costs of £50,000 and 57 incidents per year (50%)

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	7.1	14.1	28.2	56.5	70.6
10% cost reduction	14.1	28.2	56.5	113.0	141.2
25% cost reduction	35.3	70.6	1141.2	282.5	353.1
50% cost reduction	70.6	141.2	282.5	565.0	706.2
75% cost reduction	105.9	211.8	423.7	847.5	1,059.3
100% cost reduction	141.2	282.5	565.0	1,130.0	1,412.5

Comparison to High case (Potential costs of £1,450.6)

For the potential benefits to outweigh the potential costs more than 500 large companies would need to experience a 100% reduction in security incident costs for half of all incidents that they experience. This seems rather unlikely.

Comparison to the Medium case (Potential costs of £725.3)
Around 500 large companies would need to experience a reduction in incident costs of 50-75% for half of all incidents or 400 companies would need to see a reduction of 50-75% for the potential benefits to outweigh the potential costs or around 400 companies would need to see the same fall at the least.

Table A.13 - Potential benefits (in £ m) for large companies assuming medium costs of £350,000 and 57 incidents per year

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	49.4	98.8	197.7	395.5	494.3
10% cost reduction	98.8	197.7	395.5	791.0	988.7
25% cost reduction	247.1	494.3	988.7	1,977.5	2,471.8
50% cost reduction	494.3	988.7	1,977.5	3,955.0	4,943.7
75% cost reduction	741.5	1,483.1	2,966.2	5,932.5	7,415.6
100% cost reduction	988.7	1,977.5	3,955.0	7,910.0	9,887.5

Comparison to High case (Potential costs of £1,450.6)
To cover the potential additional costs related to security spending either around 500 companies would need to see a reduction for half of the security incidents of 10-25% or around 100 companies would need to see a reduction 50-75%.

Comparison to the Medium case (Potential costs of £725.3)
Around 500 companies would need to see a reduction of 5-10% related to half of all incidents or 50 companies would need to experience a reduction of 50-75% for the potential benefits to outweigh the potential costs associated with additional security spending.

Table A.14 - Potential benefits (in £ m) for large companies assuming high costs of £650,000 and 57 incidents per year

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	91.8	183.6	367.2	734.5	918.1
10% cost reduction	183.6	367.2	734.5	1,469.0	1,836.2
25% cost reduction	459.1	918.1	1,836.2	3,672.5	4,590.6
50% cost reduction	918.1	1,836.2	3,672.5	7,345.0	9,181.2
75% cost reduction	1,377.1	2,754.3	5,508.7	11,017.5	13,771.8
100% cost reduction	1,836.2	3,672.5	7,345.0	14,690.0	18,362.5

Comparison to High case (Potential costs of £1,450.6)
For the potential benefits to cover the potential addition security spending required in this case under the Directive, would mean that around 500 large companies would need to see a reduction of 5-10% in the costs associated with half of their incidents. On the other hand only around 50 large companies would

need to experience a reduction of 75-100% for the potential benefits to outweigh the potential additional costs under the Directive.

Comparison to the Medium case (Potential costs of £725.3)
At least 50 large companies would need to see a reduction of around 25-50% for half of their incidents or around 200 companies would need to experience a reduction of 5-10% for the potential benefits to outweigh the potential costs.

Table A.15 – Potential benefits in (£ m) for small companies assuming low costs of £4,000 and 4 incidents per year (25% of incidents)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	0.42	0.85	2.1	4.2	8.5	17.0
10% cost reduction	0.85	1.7	4.2	8.5	17.0	34.0
25% cost reduction	2.1	4.2	10.6	21.2	42.5	85.0
50% cost reduction	4.2	8.5	21.2	42.5	85.0	170.0
75% cost reduction	6.3	12.7	31.8	63.7	127.5	255.0
100% cost reduction	8.5	17.0	42.5	85.0	170.0	340.0

Comparison to High case (Potential costs of £533.7)
In this case more than 20,000 small companies would need to see a reduction of 100% for a quarter of the security incidents that occur for the potential benefits to outweigh the potential costs, which seems rather unlikely.

Comparison to the Medium case (Potential costs of £266.8)
For the potential benefits to outweigh the potential costs around 20,000 small companies would need to experience a reduction of 75-100% for a quarter of all incidents that they experience in one year for the potential benefits to outweigh the potential additional costs under the Directive. Again this seems rather unlikely.

Table A.16 - Potential benefits in (£ m) for small companies assuming medium costs of £27,000 and 4 incidents per year (25% of incidents)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	2.8	5.7	14.3	28.6	57.3	114.7
10% cost reduction	5.7	11.4	28.6	57.3	114.7	229.5
25% cost reduction	14.3	28.6	71.7	143.4	286.8	573.7
50% cost reduction	28.6	57.3	143.4	286.8	573.7	1,147.5
75% cost reduction	43.0	86.1	215.1	430.3	860.6	1,721.2
100% cost reduction	57.3	114.7	286.8	573.7	1,147.5	2,295.0

Comparison to High case (Potential costs of £533.7)

Around 20,000 companies that are affected by the Directive would need to see a reduction in the costs associated with security incidents for a quarter of these of 10-25% or around 5,000 small companies would need to see a fall in these costs of around 75-100% for the potential benefits to outweigh the potential costs.

Comparison to the Medium case (Potential costs of £266.8)
At least around 2,500 companies will need to experience a reduction in incident costs of around 75-100% for a quarter of all incidents in one year or around 20,000 companies will need to see a fall of these by 10-25% for the potential benefits to outweigh the potential costs.

Table A.17 - Potential benefits in (£ m) for small companies assuming high costs of £50,000 and 4 incidents per year (25% of incidents)

	500 companies	1,000 companies	2,500 companies	5,000 companies	10,000 companies	20,000 companies
5% cost reduction	5.3	10.6	26.5	53.1	106.2	212.5
10% cost reduction	10.6	21.2	53.1	106.2	212.5	425.0
25% cost reduction	26.5	53.1	132.8	265.6	531.2	1,062.5
50% cost reduction	53.1	106.2	265.6	531.2	1,062.5	2,125.0
75% cost reduction	79.6	159.3	398.4	796.8	1,593.7	3,187.5
100% cost reduction	106.2	212.5	531.2	1,062.5	2,125.0	4,250.0

Comparison to High case (Potential costs of £533.7)
At the most around 20,000 companies will need to receive a benefit from reduced incident costs of 10-25% or at least 5,000 companies will need to experience a fall of the costs of 50-75% for the potential benefits to outweigh the potential costs.

Comparison to the Medium case (Potential costs of £266.8)
For the potential benefits to outweigh the potential costs there is a range of possibilities with respect to the number of companies that would need to see a reduction in security incident costs. Either around 20,000 companies need to see a fall of 5-10% or around 2,500 companies will require a reduction of 50-75%.

Table A.18 - Potential benefits (in £ m) for large companies assuming low costs of £50,000 and 28 incidents per year (25% of incidents)

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	3.5	7.1	14.1	28.2	35.3
10% cost reduction	7.1	14.1	28.2	56.5	70.6
25% cost reduction	17.6	35.3	70.6	141.2	176.5
50% cost reduction	35.3	70.6	141.2	282.5	353.1
75% cost reduction	52.9	105.9	211.8	423.7	529.6
100% cost reduction	70.6	141.2	282.5	565.0	706.2

Comparison to High case (Potential costs of £1,450.6)

In this case more than 500 large companies that are affected by the Directive would need to experience a reduction of 100% in the costs associated with security incidents for a quarter of these for the potential benefits to outweigh the potential costs.

Comparison to the Medium case (Potential costs of £725.3)
Similarly to the High case more than 500 companies would need to see a reduction of incident costs of 100% for a quarter of these for the potential benefits to outweigh the potential costs.
In both cases this seems rather unlikely to occur.

Table A.19 - Potential benefits (in £ m) for large companies assuming medium costs of £350,000 and 28 incidents per year (25% of incidents)

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	24.7	49.4	98.8	197.7	247.1
10% cost reduction	49.4	98.8	197.7	395.5	494.3
25% cost reduction	123.5	247.1	494.3	988.7	1,235.9
50% cost reduction	247.1	494.3	988.7	1,977.5	2,471.8
75% cost reduction	370.7	741.5	1,483.1	2,966.2	3,707.8
100% cost reduction	494.3	988.7	1,977.5	3,955.0	4,943.7

Comparison to High case (Potential costs of £1,450.6)
Around 500 companies would require a reduction of incident costs of 25-50% for a quarter of all incidents that they experience in one year or around 200 companies would require a higher reduction of 50-75% for the potential benefits to outweigh the potential costs.

Comparison to the Medium case (Potential costs of £725.3)
A reduction of 10-25% in the costs associated with security incidents for around 500 large companies would be required for a quarter of incidents or a reduction of 50-75% for at least 100 large companies is needed for the potential benefits to outweigh the potential costs.

Table A.20 - Potential benefits (in £ m) for large companies assuming high costs of £650,000 and 28 incidents per year (25% of incidents)

	50 companies	100 companies	200 companies	400 companies	500 companies
5% cost reduction	45.9	91.8	183.6	367.2	459.1
10% cost reduction	91.8	183.6	367.2	734.5	918.1
25% cost reduction	229.5	459.1	918.1	1,836.2	2,295.3
50% cost reduction	459.1	918.1	1,836.2	3,672.5	4,590.6
75% cost reduction	688.5	1,377.1	2,754.3	5,508.7	6,885.9
100% cost reduction	918.1	1,836.2	3,672.5	7,345.0	9,181.2

Comparison to High case (Potential costs of £1,450.6)

Either at least 100 companies need to see a fall of 75-100% of the costs associated with security incidents for a quarter of these or around 500 companies will need to experience a reduction of 10-25% for these for the potential benefits to outweigh the potential costs.

Comparison to the Medium case (Potential costs of £725.3)
For the potential benefits to outweigh the potential costs around 500 companies need to see a reduction of 5-10% for incident costs for a quarter of these or around 50 companies need to see a much larger fall in these of 75-100%.

Annex 7 – Post-Implementation Review

Basis of the Review
The Directive already requires a review no later than three years after the date of transposition, which is requiring Member States to adopt and publish by one year and a half after adoption at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. This review is likely to be accompanied by an EU Impact Assessment and may result in legislative changes being proposed. If changes are proposed then it would be appropriate for the PIR to be carried out at the same time.

Review objective
The objective would be to consider the progress towards the Directive's goals, specifically to improve and support a minimum level of network and information security across all Member States.

Review approach and rationale
The review will take into account the work undertaken at the EU level as well as considering stakeholder views through representative organisations. How the review will be undertaken though is likely to depend on the final shape of the Directive and its implementation.

Baseline
As this Impact Assessment has shown establishing a baseline in this area can be rather difficult. Further information and research might need to be undertaken in advance of the implementation of the Directive to establish a more robust baseline.

Success criteria
The EU review is likely to outline the success criteria and might propose changes to the approach through the EU Impact Assessment, which will intend to validate the current policy position. Core indicators of progress were already defined in the Commission's Impact Assessment.

Monitoring information arrangements
Affected institutions and the national competent authority will need to work closely together to provide the required information under the reporting mechanisms in the Directive. This could also be supported through regular stakeholder liaison through emailing lists and discussions through BIS organised stakeholder engagement meetings for example.

Annex 8 - References

Cabinet Office, 2013, Understanding the Security Policy Framework, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200552/HMG_Security_Policy_Framework_v10_0_Apr-2013.pdf

Campbell, Richard, 2012, Weather-related power outages and electric system resiliency, For the Congressional Research Service, http://www.fas.org/sgp/crs/misc/R42696.pdf

Computer Weekly, 2013, UK cloud computing providers directory, UK cloud computing providers directory

Department for Business, Innovation and Skills (BIS1), 2012, UK Government response to European Commission consultation on Network and Information Security, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43267/12-1222-uk-response-ec-consultation-network-information-security.pdf

Department for Business Innovation and Skills (BIS2), Business population estimates 2012 BIS: business population estimates 2010 to 2012 - Publications - Inside Government - GOV.UK

Department of Health, 2013, Information Governance Toolkit, Information Governance Toolkit

European Commission (EC1), 2001, Communication from the Commission to the Council, The European Parliament, The Euroopean Economic and Social Committee and the Committee of the Regions; Network and Information Security: Proposal for a European Policy Approach; http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf

European Commission (EC2), 2006, Communication from the Commission to the Council, The European Parliament, the European Economic and Social Committee and the Committee of the Regions; A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”; http://ec.europa.eu/information_society/doc/com2006251.pdf

European Commission (EC3), 2009, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection; “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

European Commission (EC4), 2013, Consultation on Network and Information Security – Publication of individual responses; Digital Agenda for Europe - European Commission

European Commission (EC5), 2013, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF

European Commission (EC6), 2013, Impact Assessment accompanying the document ‘Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union, COM(2013), 32 final; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2013:0032:FIN:EN:PDF

European Commission (EC7), 2013, Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

European Network and Information Security Agency (ENISA 1), 2013, Technical Guideline on Incident Reporting, Technical guidance on the incident reporting in Article 13a, Version 2; https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

European Network and Information Security Agency (ENISA 2), 2013, Technical Guideline on Security Measures, Technical guidance on the security measures in Article 13a, Version 1.93; https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-on-security-measures-v1.9

European Parliament, 2009, Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisations of electronic communications networks and services; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

Evening Standard, 2011, MPs to probe cable theft crisis on the railways, MPs to probe cable theft crisis on the railways - News - London Evening Standard

Detica, 2011, Impact of the Security and Integrity provisions of the EU Electronic Communications Framework, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77642/CVCA1181D001Impact_of_Security_and_Integrity_Provisions_of_ECF_v1-2.pdf

Electronic Payments, 2013, Compare online payment providers | Electronic Payments | Edinburgh UK

Elexon Ltd., 2011, The Balancing and Settlement Code, http://www.elexon.co.uk/wp-content/uploads/2013/07/gb_bsc.pdf

Energy Networks Association, 2013, The Distribution Code and The Guide to the Distribution Code of Licensed Distribution Network Operators of Great Britain, http://www.dcode.org.uk/assets/files/dcode-pdfs/Distribution%20Code%20v%2020.pdf

Federation of Small Businesses (FSB), 2012, Cyber security and fraud: The impact on small businesses; http://www.fsb.org.uk/frontpage/assets/fsb_cyber_security_and%20_fraud_paper_2013.pdf

Financial Conduct Authority, 2013, Financial Conduct Authority Handbook, http://www.fshandbook.info/favicon.ico

Gartner, 2013, IT Metrics: IT spending and staffing report, 2013

HMG, 2002, The Electricity Safety, Quality and Continuity Regulations 2002, http://www.legislation.gov.uk/uksi/2002/2665/pdfs/uksi_20022665_en.pdf

HMG, 2010, A strong Britain in an age of uncertainty: The National Security Strategy, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

HMG, 2011, The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Information Commissioner's Office (ICO), 2012, Notification of data security breaches to the Information Commissioner's Office, Data Protection Act, http://www.ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/BREACH_REPORTING.ashx

National Grid, 2006, The Connection & Use of System Code, http://www.nationalgrid.com/NR/rdonlyres/BC4FA6D1-F3C6-4ECE-8FF6-73297C302A71/60801/CompleteCUSC_01_June13_CMP208.pdf

National Grid, 2013, The Grid Code, Issue 5, Revision 4, http://www.nationalgrid.com/NR/rdonlyres/67374C36-1635-42E8-A2B8-B7B8B9AF2408/62011/00_GRID_CODE_FULL_I5R4.pdf

Ofgem 1, 2013, Electricity Act 1989, Standard conditions of electricity supply licence, https://epr.ofgem.gov.uk/Content/Documents/Electricity_supply_standard_licence_conditions_consolidated%20-_Current%20Version.pdf

Ofgem 2, 2013, Gas Act 1986, Standard conditions of gas supply licence, https://epr.ofgem.gov.uk/Content/Documents/Gas%20supply%20standard%20licence%20conditions%20consolidated%20-%20Current%20Version.pdf

Ofgem 3, 2013, Transmission Licence Standard Conditions, https://epr.ofgem.gov.uk/Content/Documents/Electricity%20transmission%20full%20set%20of%20consolidated%20standard%20licence%20conditions%20-%20Current%20Version.pdf

ONS, 2007, UK Standard Industrial Classification of Economic Activities 2007 (SIC 2007); http://www.ons.gov.uk/ons/guide-method/classifications/current-standard-classifications/standard-industrial-classification/sic2007---explanatory-notes.pdf

ONS, 2010, Industries' intermediate consumption in 2010, The 'Combined Use' matrix

ONS, 2012, ICT Activity of UK Businesses, 2011, http://www.ons.gov.uk/ons/dcp171778_289328.pdf

ONS, 2012, UK Business: Activity, Size and Location; UK Business: Activity, Size and Location, 2012

Ponemon Institute, 2013, Cost of Data Breach Study: United Kingdom; commissioned by Symantec; http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-uk-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach

PWC, 2013, Information Security Breaches Survey, Technical report; http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf

Quocirca, 2013, The trouble heading for your business, Targeted attacks and how to defend against them, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_quocirca-analyst-targeted-attacks.pdf

SunGard Availability Services, 2012, Power and Communication Failures continue to disrupt UK workplaces, SunGard Availability Services UK / Blog » Feed

Symantec, 2013, Internet Security Threat Report 2013, Vol. 18; http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

The Telegraph, 2007, Gales cause transport disruptions, Gales cause transport disruption - Telegraph

Verizon, 2013, 2013 Data Breach Investigations Report, Download: 2013 Data Breach Investigations Report - Verizon Enterprise Solutions

Zhu, Shanjiang & Levinson, David, 2011, Disruptions to Transportation Networks: A http://nexus.umn.edu/Papers/DisruptionReview.pdf