HM Government

EU Directive on Network and Information Security

SWD(2013) 31 & SWD(2013) 32

A call for views and evidence

22nd May 2013

Contents

Overview: The EU Directive on Network and Information Security

Background

The European Commission published a proposal for a Directive for Network and Information Security on 7th February. This was accompanied by a cyber security strategy (or 'Communication') which contains non legislative measures on a broad range of issues. These documents can be found on the European Commission website;

http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

The UK shares the Commission's desire to improve levels of network and information security across the EU. We want to ensure that the internal market is a safe place to do business and that Member States know who to contact in the case of a cyber incident and can effectively work together. The UK is supportive of the broad objectives the Directive is seeking to achieve, however we will need to ensure that the proposals create the right incentives for the private sector to share information, best practice and good governance.

The proposed Directive covers the following main issues:

- It obliges all Member States to produce a national cyber security strategy and establish a CERT and a competent authority for cyber security.
- It mandates information sharing between Member States, as well the creation of a pan-EU cooperation plan and coordinated early warnings for cyber incidents.
- It mandates compulsory reporting of security breaches that have a significant impact on the provision of core services to a 'national competent authority' that would enforce the Directive. Sectors that this would apply to include public administration, the finance, energy, transport and health sectors, as well as to 'enablers of internet society services' which includes app stores, cloud service providers, social networks and e-payment providers.

The UK Government is preparing an initial impact assessment on the potential effects of the Directive in the UK and is launching this Call for Evidence to gather data to inform the evidence base for this assessment.

Your knowledge and expertise of how the Directive will affect your organisation will be extremely helpful in shaping the new requirements and ensuring they are effective, realistic, and do not place unnecessary burdens on businesses or the public sector.

Key dates

This Call for Evidence opened on **Wednesday 22nd May 2013**

The final date for submitting evidence will be **Friday 21st June 2013**.

How to respond

We welcome your views and evidence, recognising that due to the varied nature of the different affected sectors, not all questions will be relevant to all respondents

As indicated above, this call will continue to Friday 21st June 2013, but we would welcome earlier input.

Contributions can be submitted as follows:

Online Response Form: https://www.surveymonkey.com/s/EUdirective

Email: cybersecurity@bis.gsi.gov.uk

Post: Cyber Security Team
BIS
1 Victoria Street
London
SW1H 0ET

We will accept anonymous submissions (and the online response form will result in an anonymous response). If you would like confirmation that we have received your submission, please include with your submission:

1. The name of your industry body or group of companies
2. Appropriate contact details should we require any further information.

If you would like further information on any aspects of this call for evidence, please use the above email address.

Call for Evidence – Parameters

The following sections sets out the parameters of this Call for Evidence.

Purpose

The UK Government has launched this call for evidence to understand how the measures contained in the proposal for an EU Directive on Information and Network Security will affect organisations in the UK. In particular it is interested in the effects associated with the introduction of mandatory reporting of incidents with a 'significant impact', and the costs and benefits to organisations of being compliant with the proposed measures.

Scope

The UK Government is interested in receiving evidence from any organisation that could be affected by the measures as set out in the Directive. Annex A sets out the range of organisations that would be affected by the Directive. Please note that this list of sectors is not final and is likely to change as a result of negotiations. We would welcome views from any organisation who believes they could be impacted by the Directive.

This Call for Evidence is concerned with incidents in regards to service outages or periods of major disruption. As the EU Directive provides no information on the reporting threshold for incidents, for the purpose of this process we have made the assumption that the reporting threshold will be at a similar level to the thresholds that have been set for the Telecoms Sector Following the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services[1].

Responses

We recommend that you read The Draft EU Directive on Network and Information Security (published 7th February 2013) before submitting evidence on this call. The following documents may also be useful as background reading for your submission;

- The Cyber Security Strategy of the European Union: An Open, safe and secure Cyberspace (published 7th February 2013)[2]
- The European Commission's draft Impact Assessment on the Proposal for a Directive of the European Parliament and Council (published 7th February 2013)[3]

[1] http://stakeholders.ofcom.org/telecoms/policy/security-resilience/implementation-eu-framework/
[2] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
[3] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

- The UK Government Response to the European Commission Consultation on Network and Information Security. (published October 2012)[4]

Annex B sets out a response template that we would prefer industry to use when responding to the Call for Evidence. The questions are structured accordingly to establish a baseline for current activity on incident response and to understand the impact of measures as proposed in the Directive.

We understand that organisations may want to provide further evidence which is not covered in the questions on the response template. Please clearly set out this evidence in **Sector 5 – Other Comments**, that has been included for this purpose.

Questions are divided into five sections. These are:

- **Section 1 - Overview**
  Provides basic information on your organisation(s) and range of operations.

- **Section 2 - Current reporting of incidents**
  The requirements and costs of existing reporting mechanisms for your organisation.

- **Section 3 - Additional compliance costs**
  The additional requirements and costs for implementing the measures as set out in the EU Directive.

- **Section 4 - Additional benefits**
  The additional benefits as a result of implementing the measures as set out in the EU Directive.

- **Section 5 - Other comments**
  To put down any other comments on the potential impact of the Directive, not covered by the other sections.

Confidentiality

The UK government understands that much of the information requested for this Call for Evidence is sensitive and commercially confidential and will treat any information provided accordingly. We will accept anonymous submissions of evidence for this call, should that be preferable.

Any evidence submitted on this Call for Evidence and held by the Department for Business, Innovation and Skills will be subject to the Freedom of Information Act 2000. If BIS receives a request for disclosure of this

[4] https://www.gov.uk/government/publications/uk-government-response-to-european-commission-consultation-on-network-and-information-security

information it is our practice to consult with the relevant third parties to provide you with an opportunity to notify us of any particular issues or considerations that you may consider relevant to the question of disclosure of this information at that time.

In the Impact Assessment, we may publish extracts from the submissions of evidence to provide qualitative evidence. Please indicate in your submission if there are specific extracts that you would prefer not be released for commercial reasons. Any quantitative data presented will be in a high level aggregate form and not be associated with any individual response. You are welcome to make anonymous contributions if you prefer.

Call for Evidence - Terminology

CERT

CERT; Computer Emergency Response Team. CERTs have expertise to assist organisations in the response to computer security incidents and provide advice to reduce the threat exposure.

As part of its Cyber Security Programme, the UK is committed to setting up a National CERT.

Competent Authority

For the purpose of this call for evidence, the national competent authority would be a new or existing body set up to monitor and enforce the measures introduced in the Directive at a national level. The national competent authority would also form part of the European Commission's European network of competent authorities.

Incident

Incident; any circumstance or event having an actual adverse effect on security.

For the purpose of this call for evidence, an incident is also defined as either causing service disruption or service outage.

Incident of 'significant impact'

The Directive states that incidents 'that have a significant impact on the security of core services they provide' will require public administrations and market operators to notify that the event has occurred. No further information is currently available on the definition of 'significant impact' in this context.

Therefore we will assume that the reporting threshold for incidents will be at an equivalent level to the reporting thresholds set for the Telecommunications Sector following the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services[5]. In the UK, the reporting thresholds for the Sector were set out by the regulator Ofcom.

For the purpose of this exercise, the following table provides an indication of the reporting thresholds that would trigger notification.

Incident	Minimum number of end customers affected	Minimum duration of service loss or major disruption
Service Disruption resulting in loss of critical / key services (i.e endangerment of life)	1,000	1 hour
Service Disruption resulting in loss of critical / key	100,000	Any Duration

[5] http://stakeholders.ofcom.org.uk/telecoms/policy/security-resilience/implementation-eu-framework/

Incident	Minimum number of end customers affected	Minimum duration of service loss or major disruption
services (i.e endangerment of life)		
Service Disruption resulting in loss of service	1,000	24 hours
Service Disruption resulting in loss of service	100,000	1 hour
Service Disruption resulting in loss of service	1,000,000	10 minutes

These guidelines are not an exhaustive list of thresholds for all potential sectors – there will be incidents that do not fall into any categories listed. Instead the intention of the table is to illustrate the scale and type of incidents which we would expect to be considered in your evidence. Three factors should be considered in deciding whether an incident would be reported;

- The scale of service disruption
- The number of end customers affected
- The duration of service loss or major disruption

Market Operator

Market Operators; organisations that would be covered by the measures in the proposed Directive.

The Directive (in Article 3, 8(a) defines a Market Operator as:

a. Provider of information society services which enable the provision of other information society services.

b. Operators of critical infrastructure that are essential for the maintenance of vital economic and societal services in the fields of energy, transport, banking, stock exchanges and health.

This definition encompasses any organisation that provides these services – even if it is not their primary business.

Annex A provides further details on the organisations that are considered to be market operators using this definition.

Annex A – Sector Scope of the Call for Evidence

This Annex sets out the range of organisations that we would like to provide evidence on the proposal for an EU Directive on Network and Information Security.

Any organisation that provides the following services would be included in the scope of the Directive; even if it is not the primary business of that organisation.

Micro Enterprises, defined as enterprises which employ fewer then 10 persons and whose annual turnover does not exceed €2 million are exempt from the measures proposed in the Directive.[6]

A. Public Administrations

All public administration bodies would be included in the scope of the Directive.

B. Market Operators

a. Provider of information society services which enable the provision of other information society services.

Although this is not an exhaustive list, the Directive indicates (in Annex II) organisations in this category would include;

1. **E-commerce platforms**
2. **Internet Payment Gateways**
3. **Social networks**
4. **Search Engines**
5. **Cloud Computing services**
6. **Application stores**

b. Operators of critical infrastructure that are essential for the maintenance of vital economic and societal services in the fields of energy, transport, banking, stock exchanges and health. Organisations in this category include;

1. **Energy**
    - Electricity and gas suppliers

[6] http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_en.htm

- Electricity and/or gas distribution system operators and retailers for final consumers
- Natural gas transmission system operators, storage operators and LNG operators
- Transmission system operators in electricity
- Oil transmission pipelines and oil storage
- Electricity and gas market operators
- Operators of oil and natural gas production, refining and treatment facilities

2. **Transport**
   - Air carriers (freight and passenger air transport)
   - Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)
   - Railways (infrastructure managers, integrated companies and railway transport operators[7]
   - Airports
   - Ports
   - Traffic management control operators
   - Auxiliary logistics services: (a) warehousing and storage, b) cargo handling and c) other transportation support activities

3. **Banking**
   - Credit Institutions

4. **Financial Market Infrastructure**
   - Stock exchanges
   - Central counterparty clearing houses

5. **Health Sector**
   - Health Care settings (including hospitals and private clinics)
   - Entities involved in health care provisions

The Directive indicates that this list is not exhaustive

C. Regulators

Existing regulators who operate in the aforementioned sectors

[7] Following initial conversations with stakeholder, we will add transmission system (telecom) operators to this category.

Annex B – Response Template

Section 1 - Overview

1. What sector(s) does your organisation(s) operate in?

☐	Enabler of an Information Society Service
☐	Energy Sector
☐	Health Sector
☐	Transport Sector
☐	Banking Sector
☐	Provider of Financial Market Infrastructure
☐	Regulatory Body
☐	Public Administration
☐	Other

If Other, please specify below;

2. How large is your organisation (by headcount)?

☐	0-9
☐	10-49
☐	50-249
☐	250-499
☐	500-999
☐	1,000-4,999
☐	5000+
☐	N/A

3. What is your organisation's current turnover per annum? (in £ thousand)

☐	0-49
☐	50-99
☐	100-249
☐	250-499
☐	500-999
☐	1,000-4,999
☐	5,000+

4. Do you operate;

    a. Only in the UK
    b. Internationally, but within the EU
    c. Internationally, including countries outside the EU

5. What is the size/composition of your customer base?

6. Does the delivery of core services in the UK depend on networks or data held outside the EU? Can you specify/provide examples?

7. What is your IT security spend as a percentage of your overall turnover?

8. Does your organisation conform to any cyber security standard? If yes, which one(s)?

Section 2 - Current reporting of incidents

9. What is the current threshold in your organisation in deciding on whether a network or information breach is classified as an 'incident'? [the definition of a cyber security incident, as used in this Call for Evidence, is provided in the Terminology section]

10. Do you operate under a regulatory requirement to report incidents externally (i.e. outside your organisation) in regards to the security and resilience of your networks? If so:
- What is the current regulatory threshold in your organisation with respect to incidents that you need to report?
- Can you provide details of the type, information required to report/ pass on and frequency of this requirement and the regulators involved?

11. Do you have a voluntary agreement / corporate policy to report incidents externally (i.e. outside your organisation) in regards to the security and resilience of your networks? If so, can you provide details of:
- the type of agreement/policy
- the information required to report on/ pass on
- the frequency and threshold of this voluntary agreement / corporate policy?

12. How many incidents did you report in the last financial year [or other suitable timeframe]? What types of incidents were these? (i.e. human error, cyber incident, accidents, etc…). What type of information did you include in these reports? (i.e. number of customers affected, length of incident, etc).

13. Did the total number of incidents your organisation experience differ from the number you reported? ('total' referring to both reported and unreported externally).

14. What types of incidents were these which went unreported and why were they not reported? (i.e. no requirement, not in public interest, etc)

15. Can you give the average cost for dealing with an incident in your organisation? This should not include the cost of reporting the incident. Examples of areas that you may wish to consider are given below;
    a. Commercially confidential/Restricted information compromised
    b. IP/material property stolen
    c. Resource required to manage incident
    d. Reputational Risk – clients and suppliers
    e. Loss of capability/service
    f. Damage to servers/infrastructure

16. When an incident was reported (if applicable), either as a requirement or as part of a voluntary agreement, what was the average administrative cost to the organisation of creating and sending that incident report? Can you provide a breakdown of the different costs associated with the incident reporting?

    [If possible please provide these in terms of number of Full-time equivalents (FTEs), time taken for the respective task and annual salary cost of the FTE or occupation[8].]

[8] Broad categories are: 1) Managers, director and senior officials, 2) Professional occupations, 3) Associate professional and technical occupations, 4) Administrative and secretarial occupations, 5) Skilled trade occupations, 6) Caring, leisure and other service occupations, 7) Sales and customer service occupations, 8) Process, plant and machine operatives, 9) Elementary occupations

17. Can you provide details on the current costs for monitoring your networks/ systems? For example, provide details on the reporting process for incidents or the level of resource retained to monitor the network.

18. When an incident is reported, is there any obligation/ voluntary agreement to make details of the incident public? Can you provide details of any thresholds when this would occur?

Section 3 - Additional Compliance Costs

For the following section, the questions are considering a scenario where the Directive is implemented in its current form, so that all incidents that have a significant impact will need to be reported to the national competent authority. In the terminology section we have defined this term and provided a similar table to that used by the telecoms sectors as an example. This however may not be relevant to your business model – and we understand that you have a better understanding of how an incident could have a significant impact both at national and EU level. The first question in this section is therefore highly significant as it provides information on the threshold where you believe an incident would have a national or international impact.

19. Given the definition as provided in the terminology section, at what point of disruption in your core service would you consider an incident to have a 'significant impact'. Please consider the following factors in your response;
    a. The scale of service disruption
    b. The number of end customers affected
    c. The duration of service loss or major disruption

20. What would be the impact to your organisation of having to report all 'incidents of significant impact' in the UK, in the following areas? [The definition of 'incident of significant impact, as used in this Call for Evidence, is provided in the Terminology section]

    a. Additional resource cost for reporting additional information (See Section 2, Question 6 as a starting point)
    b. Expected increase in security spending in relation to the new thresholds?
    c. Additional costs associated with potential security audits from the National Competent Authority

21. Will the Directive cause your organisation to report incidents that it would not have otherwise reported (using the thresholds as outlined on pp. 8-9 and in Q19)? Can you give an indication of the area/remit these would fall under?

22. Will the Directive potentially make incidents of significant impact public that your organisation would not have made public in your current activities? Can you provide details on the impact this may have on your organisation?

    [We would recommend that you reread Article 14, 4 for further information on the potential for incident disclosure]

23. [For multinational organisations] Will the Directive have any additional impacts on security and resilience procedures on your operations located outside of the EU?

24. Could implementing the Directive have any additional consequences or impact on your organisation, unintentionally or not, that you have not covered in the previous questions? If yes, please provide details.

Section 4 - Additional Benefits

25. 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? Please provide details.

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

27. 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? Please provide details.

28. 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?

Section 5 – Other Comments

29. Please use this section to raise any other issues and concerns on the Directive that have not been raised in your response so far.

Below we have set out some examples of topics you may wish to consider in your response. This is not an exhaustive list.

- Barriers to entry for new entrants
- Effects on Supply Chain
- Proportion of impact for SMEs
- Impact within/outside Europe
- Requirements for additional expertise/skills

This publication is also available on our website at www.bis.gov.uk
Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/13/880