Response to the Security of Network and Information Systems Public Consultation
Compiled on behalf of the UK Computing Research Committee, UKCRC.

Coordinated by:

Chris Johnson

Professor and Head of Computing Science,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson, johnson@dcs.gla.ac.uk

UKCRC is an Expert Panel of the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading computing researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Questions

Q1 Are the identification thresholds set at a level that captures the most important operators in your sector based on their potential to cause a significant disruptive effect if disrupted?

YES

Q2 If not, why not? What would you change and why? Narrative response?

Q3 Do you agree with the government's proposed approach of adopting a multiple competent authority model.

NO

Q4 If not, why do you believe a single competent authority model represents a better option? Do you have an alternative outside of these two models?
Narrative answer.

A slight alteration of the proposed approach might be preferable where all incidents are reported directly to the NCSC for triage to the industry-specific competent authorities. This should support the detection of cross-sector incidents and also reduce ambiguity/doubt, while at the same time making it clear that the responsibility for responding to sector specific incidents remains in the hands of those who understand their industry the best. NCSC might also be able to reduce the need for duplicated cyber expertise by offering centralized forensic support in response to an incident.

Q5 Is the proposed competent authority for your sector a suitable choice? NO

Q6 If NO, who do you believe should be the competent authority for your sector and why?
Narrative answer.

As it stands, many competent authorities have almost no cyber expertise and very limited budgets to address this omission. More seriously, it is unclear how public finance might be deployed to retain individuals who develop competency in this area (and also the industry sector) against a highly competitive international market place. Hence the NCSC should act as a centralized clearinghouse to supplement the competent authorities, otherwise if an incident was reported direct to the competent authorities it is doubtful whether many existing employees would know what steps would be appropriate to determine if it was or was not cyber related.

Under the proposed arrangements for Digital Service Providers, OFCOM would be more appropriate than the ICO reflecting existing reporting obligations under the Telecoms Directive. Related to this is a concern about online marketplaces, online search engines and cloud computing services. These are described very closely to the definitions provided by ENISA in https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers However, how this description is applicable to the UK's national level is unclear. e.g.
* Online marketplaces: Does this refer to marketplaces that are physical hosted in UK? Or cover EU member states?
* Cloud computing services: why restrict this only to the cloud? How this will be appropriate if/when future virtualised computing models become popular, e.g., fog / mobile edge computing?
* In addition to search engines, should (smaller) ISPs and data centre providers be included, and perhaps even hosted web services for sections of industry that are otherwise not represented in the various lists? Generally, I'm not sure where the current lists were derived. Similarly with the definitions of Operators of Essential Services; the telecommunication operators (fixed and mobile) need to be included in the list, along with the largest ISPs. These may or may not be under the category of digital infrastructure.

Q7 Do you believe these high level principles cover the right aspects of network and information systems security to ensure that risks will be appropriately managed? NO

Q8 If NO, can you clarify what aspects you believe are missing and recommend how we could address these?
Narrative answer

1. There should be more consideration of the role of board level leadership and accountability for cyber security.

2. There should be more on determining and protecting an appropriate budget for cyber security.

3. There should be more on determining appropriate means of compliance, for example, when there is ambiguity or conflict between existing safety and security standards.

4. There should be more on developing a roadmap for cyber security where existing practices and standards are improved over time when some risks cannot be immediately mitigated; for instance gradual replacement of insecure systems.

5. Some consideration of operational technology (OT) and not just IT following the Ukraine attacks.

6. There needs to be considerable emphasis on establishing resilience management principles rather than simple security (which is more about defending and not enough about recovering from challenges). Resilience goes beyond security: it anticipates intrusions and builds in monitoring and remediation steps along with risk management at the outset.

Q9 Do you believe these principles would impose any additional costs on designated operators, or on the sectors in scope as a whole? YES

Q10 If YES, what do you consider would be the anticipated resource implication on designated operators, or on the industry as a whole of meeting these principles? Are you able to elaborate on the nature of these costs? Where possible please detail any specific financial costs you consider would likely result.
Narrative answer

The directive covers many diverse aspects of UK industry – we have been involved in reviews for HMG that show a significant portion have a very low level of maturity and those that do demonstrate good practice are often highly focused eg on payment protection and not operational/infrastructures. If the principles were followed in a systematic and sustained way then there would be increased costs but these should be proportionate to the perceived threats. Unfortunately, the perception of the threat is not consistent even within individual industries.

Q11 Do you have any plans to make additional security related investments as a result of this Directive? Where possible please indicate the size of investment (in £)?
YES

YES – in conjunction with planning for the GDPR (see answer to Q12).
Q12 If YES, please provide the amount and details of what investments would be required.
Narrative answer

We represent UK Universities, active in cyber related research and development hence this is not entirely applicable.

Q13 Do you consider these incident reporting proposals to be reasonable to ensure that serious incidents affecting the network and information systems of essential services are reported?

NO

Q14 If NO, why not? Can you suggest revised incident reporting proposals that ensure serious incidents are reported?
Narrative answer

As mentioned, the NCSC should act as the immediate national point of contact for serious reportable cyber incidents; to maximize finite cyber resources and provide means of correlating common attacks across common infrastructure supply chains.

Very little has been said about what will be done *with* the data at a national or European level. Members of UK CRC helped ENISA set up the reporting systems already in place under the Telecoms Directive and the response to this has been very mixed. Some companies act as ‘good citizens’ whilst it is clear that others have no intention of reporting even more serious adverse events, especially where they are deemed to involve IP or other commercial concerns. The level of competition and cooperation between UK companies varies enormously across the sectors covered by the Directive and I would expect that HMG would have to work with the NCSC and the Competent Authorities to identify and then support those sectors with a relatively low level of cyber maturity. In the US, they have developed techniques such as Sentinel Reporting systems to tackle low rates of participation together with significant financial penalties in NORS/DIRS.

Q15 Do you consider that the proposed timeframe for providing incident reports place an undue burden on designated operators of essential services?

NO

Q16 If YES, can you explain what these burdens and costs would be? Narrative answer

Q17 Are Digital Service Providers easily able to identify themselves using these criteria?

NO

Q18 If NO, Why Not? Can you provide revised criteria that would identify providers more easily?
Narrative answer

The IaaS, SaaS, PaaS taxonomy is useful but does not distinguish between internal and external cloud services. In many cases, these are very blurred distinctions – what would happen about public sector bodies hosting services, for example for neighboring NHS trusts? There are emerging technologies and architectures (Fog and mobile edge computing) that do not fit well into the IaaS, SaaS, PaaS taxonomy. Similarly, what is the UK position with respect to cross-border Cloud services? There also seems scope for the inclusion of some larger data center providers with a direct impact on National resilience.

Q19 Would using these definitions create any unfair competitive advantage or disadvantage for Digital Service Providers within scope?

NO

Q20 If you answered YES to the previous answer , please clarify nature of the advantage or disadvantage?
Narrative answer

Q21 Are these principles reasonable? NO

Q22 If NO, Why Not? Can you suggest revised principles that would enable important incidents to be reported?
Narrative answer

For DSPs there should be an additional principle of transparency for clients/customers. There should ideally be an expectation that customers are notified about an incident in a timely manner. Without this, many parts of UK industry cannot mitigate the consequential losses that they might suffer from a breach. This is a general concern with the present draft.

Q23 What would be the impact on your business in applying these principles? Narrative answer

We represent UK Universities, active in cyber related research and development hence this is not entirely applicable.

Q24 Do you have an alternative preferred approach? Narrative answer

See answer to Question 22.

Q25 Would this incident reporting timeframe place an undue burden on your business or operations?
YES/NO

NO

Q26 If YES, can you explain what these burdens and costs would be? Narrative answer

Q27 Do you wish to take part in the proposed targeted consultation exercise once the security and incident reporting thresholds have become clearer?

YES

Q28 If YES, please provide an appropriate name, and email address for future correspondence.

As mentioned, a UK CRC member helped ENISA design the security and incident reporting thresholds under Article 13b of the Telecoms Directive which is now operating across European member states:

Prof. Chris Johnson,
Head of Computing Science,
Sir Alwyn Williams Building, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson
Johnson@dcs.gla.ac.uk

Q29 Do you consider the proposed penalty regime to be proportionate to the risk of disruptions to operators of essential services?
YES

Q30 Do you believe that the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems? YES

Q31 If you answered NO to either of these two questions, please explain how the penalty regime could be amended to address your concerns.
Narrative answer

N/A