Call for views on software resilience and security for businesses and organisations

The IET responded to the above consultation from the **Dept for Science, Innovation & Technology** and the **Dept for Digital, Culture, Media & Sport**. The text below gives the IET's responses to the questions that it answered. Unanswered (parts of) questions have been omitted.

Organisational demographic questions on those responding to the call for views:

1. Are you responding as an individual or on behalf of an organisation?

b. Organisation

3. Which of the following statements best describes your organisation?

f. A business that uses software developed or maintained by others
g. Organisation that employs, contracts or uses software and/or cyber security professionals
k. Organisation with an interest in software and/or cyber security
l. Non-cyber security specific professional body or trade organisation with an interest in software and/or cyber security: Engineering & Technology. The Institution of Engineering and Technology (IET) is a Professional Engineering Institution.

4. Including yourself, how many people work for your organisation across the UK as a whole?

e. 500-999

5. What is the name of the organisation on whose behalf you are responding?

The Institution of Engineering and Technology (IET)

6. Are you happy to be contacted to discuss your response and supporting evidence?

Yes

7. Please provide a contact name and email address below.

Andrew Rylah, arylah@theiet.org . We would be happy to discuss our answers with you in more detail at a time of your convenience.

Questions on risk areas:

We have compiled responses to the questions that relate to general impacts and risks, as opposed to ones that relate to the IET itself.

9. To what extent do you think issues in each of the software risk areas outlined above impact the security and resilience of the wider UK economy?

High impact across all the areas mentioned.

a. Software development security

- **Accidental vulnerabilities in software code**
- **Intentional compromises of software code**
- **Insecure development environments**

b. Barriers in the open source community

c. Security and resilience in the distribution of software

d. Transparency and communication of software materials, vulnerabilities and incident management

e. Procurement, supplier assurance, and supplier management

f. Maintenance, configuration and use of software by the customer

g. Please explain your answers to the above:

There are often cost / security / capability trade-offs in the design of software. The rapid increase in software complexity and our everyday reliance on it means that the impact of failure due to the exploitation of vulnerabilities is business critical. Despite having up-to-date software, robust and effective resilience, and disaster recover policies, even a relatively short disruption in access to key software could cause severe financial and reputational damage. A prolonged disruption may cause business failure, albeit this latter outcome has yet to become commonplace.

There is a concentration of power in a few major players, which can deter businesses from sourcing alternative software that may be less established. Many UK organisations are becoming over-reliant on cloud-based software, often based outside UK national borders.

10. Which, if any, of these risk areas do you see as the <u>biggest problem</u>?

a. Software development security

- Accidental vulnerabilities in software code

11. Please explain your answer to the above

We see the biggest problem to be software development security, particularly when related to accidental vulnerabilities in software code.

Vulnerabilities can disadvantage customers. However, this may not necessarily be due to direct cyber-attacks, for example, if a business is using software that is reputationally damaged due to vulnerability exploitation elsewhere. This could be due to a lack of awareness of what the code is actually doing, with impacts resulting from it.

Various causes may lead to vulnerabilities – the complexity of the software; the expected rate of software development (software may need to be pushed out very quickly for companies to remain competitive); a lack of security awareness.

Vulnerabilities could also be due to integrated systems that have been developed by different suppliers. This could happen if systems are linked together without a good understanding of the individual systems, or where systems are maintained as part of a supply chain, particularly if those involved are not cyber specialists. Cyber security needs to be (a) built into the curriculum for relevant disciplines and (b) needs to be reviewed as part of every board decision.

Code recycling is also a problem, especially if code is obtained from open sources. There's an assumption about the quality of open source code. However, copying without a good understanding of the code can lead to vulnerability issues. With traditional software development, there are issues around patching code that is obtained from a social space. The issue could get worse with the development of AI, where an understanding of the code and predictions of its impacts is more difficult to ascertain.

12. Are there other risks that are linked to software but not covered in the risk areas above?

a. Yes

13. What other risks are you referring to?

There's a challenge finding people with the required skills at competitive salary rates. It's also difficult to assess the competency of developers. Competency frameworks and lists of recognised qualifications would help provide this reassurance, though infrastructure would be needed to maintain such frameworks. Competence is less well managed outside regulated communities.

New entrants to the marketplace are valuable sources of innovation. However, innovation may also present a barrier to security. Competence may focus on self-regulation based on internal guidance that could set the bar low, given upfront costs. Such reduced costs may make firms more competitive, though it raises security risks.

The aim is for proportionate regulation to allow for innovation, whilst minimising risk levels. Risks that have a small impact would be regulated less than mission-critical ones. Regulatory sandboxes have been developed with regards to AI, where regulators & developers collaborate in developing appropriate assurance models. However, these are expensive.

Questions on future interventions:

21. In which of the risk areas do you think there is a need for greater government and/or industry intervention?

b. Barriers in the open source community

d. Transparency and communication of software materials, vulnerabilities and incident management

e. Procurement, supplier assurance, and supplier management

f. Maintenance, configuration and use of software by the customer

g. Please explain your answers to the above

Greater government and industry intervention is needed across all the above aspects. However, in particular, intervention is required in the following areas:

b. Barriers

There is a risk of organisations exposing themselves to vulnerabilities from open source code. The risk increases if there is a small user / developer base i.e. where there has been limited testing in a small number of different scenarios. This is especially the case if they don’t relate to areas that a particular company is involved in.

d. Transparency

IEC 61508 includes a desire for a safety manual to be issued with devices, a manual which lists dangerous failure modes and details tests to ensure ongoing safety. A similar type of document could accompany software, detailing the measures taken during its development to reduce the software’s vulnerabilities. However, this may not be popular with suppliers given the time, effort and cost involved, plus the amount of information that an organisation has to reveal to competitors and bad actors. Such a cyber safety manual may give away too much detail to hackers who would be able to see what hasn’t been done, and target suppliers accordingly.

e. Procurement

There’s a balance between suppliers and users around planned obsolescence and the withdrawal of support. Suppliers need to be careful about when they withdraw support, to ensure users can still access their data and fulfil statutory duties. End users need to ensure they manage the obsolescence of their data appropriately.

f. Maintenance

This is often down to the competence of customers – do they understand how their equipment is working, what the software is doing and whether they are using it correctly? End users need to ensure their software is kept up-to-date to avoid issues. In addition, disaster management plans should include contingencies to deal with cyber resilience issues.

22. Do you think further action is needed to address software risks that are not covered in the risk areas outlined above?

a. Yes

23. Please explain your answer.

With regards to software competence, senior leaders and managers need to drive cultural change organisationally from the top and hence require ‘organisational security for senior leaders / management’ training.

Software Development Kits (SDKs) can be used to flag up vulnerabilities to developers to ensure that updates are provided for users.

24. Cross-cutting interventions
a. To what extent do you think the following interventions would be effective in addressing cross-cutting or other cyber risks linked to software?

- **International coordination on guidance**

Somewhat effective

- **Accreditation of cyber security consultants specialising in digital supply chains (e.g. to support software developers in implementing secure practices and/or to support customers implement secure practices in procurement processes).**

Somewhat effective

b. Please explain your answers to the above

- **International coordination on guidance**

International standards are created to ensure resilience is built into software. Standards / guidance should be as technical as needed to be useful to particular audiences and not oversimplified such that they become diluted. Guidance may be done by sector as often sector-specific knowledge is relevant. However, there would need to be a mechanism to ensure that a consistent level of confidence is achieved, perhaps via national guidance / standards with sector level interpretations akin to IEC 61508 and ISO 26262.

The UK plays a significant role in developing standards and guidance through the BSI and IEC. It influences the work of others through example and learns from others where appropriate. The national standard bodies work towards alignment with EU regulations (eg IEC 62443 and EU Cyber Resilience Act). However, the production of internationally agreed formal guidance is too slow. The UK should ensure any guidance produced meets the intent of other international standards (as a minimum), without adopting necessarily a particular set of standards. This would allow the UK to set its own guidance at its own (faster) pace. There is some divergence from the EU ethos, which is based around using the best available technology, whereas the UK focuses on developing and recognising its own good practice based on consensus. UK industry needs its rules to be aligned with those of the EU, US and other trading partners to ensure it can trade in such markets.

- **Accreditation of cyber security consultants specialising in digital supply chains (eg. to support software developers in implementing secure practices and/or to support customers implement secure practices in procurement processes).**

The risk is that effective accreditation can easily be corrupted by bodies that are too focussed on profit. The Government should ascertain and recognise particular qualifications that practitioners needed to have, qualifications that would have to be renewed, say, every 3 / 5 yrs to keep them valid. Regulation for such qualifications would need to be overseen by a government authority to ensure standards were met, in the same way that e.g. built environment standards are now regulated.

There is also a need for organisations to be **aware** of the qualifications / accreditations that are relevant to the areas they are procuring for, eg what accreditations relate to what skills and at what levels. The UKCSC can support this through their mapping of qualifications - Cyber security careers, a route map through the 16 cyber security specialisms. A common framework of skills is needed to support employers in navigating the many qualifications available; and a common curriculum (which could be based on CyBOK) would be the basis for a consistent accreditation of qualifications.

c. What other cross-cutting government interventions do you think would be effective at addressing cyber risks linked to software?

Competitive salaries at all levels need to be paid in the civil service to ensure it can attract competent, quality staff. Through attracting competence in Government, meaningful change can then be driven into relevant business sectors.

25. Software development security

a. To what extent do you think the following government interventions would be effective in addressing risks linked to secure software development (in both open source and proprietary software contexts)?

Somewhat effective

- **Guidance on best practice (e.g. code of practice for software developers, secure software development frameworks, self-assessment tools etc.)**

- **Support development and promotion of tools that scan software packages and components for known vulnerabilities and indicators of malicious compromise.**

b. Please explain your answers to the above

We believe that the government should intervene on all the above areas with money for public and private sector interventions. Regulation and intervention need financial support to be effective.

Guidance on best practice
This can be very effective, but only if agencies have the funds to hire competent staff and produce the required Codes of Practice.

Support development and promotion of tools
The National Security Agency (NSA) in the US supplies patches to open source systems. Key IT players inform suppliers of vulnerabilities and give them a timeframe (depending on the criticality of the issue, product reach etc) for patching issues before making knowledge of such vulnerabilities public. This is so that vendors take software issues seriously. It would be very useful if GCHQ could do a similar role in the UK, together with key IT players in industry so that product safety devices are tested before they go to market.

Can the government help accelerate secure by design? Software developers would be contacted when vulnerabilities were found. However, government pressure would compete against company cost-benefit analyses related to the release of software. Companies may push out software that contains vulnerabilities, knowing that getting products to market quickly will gain them more customers than they would lose through vulnerable software issues.

Government could also encourage cloud providers to do more in this respect. Such providers are focused on ensuring that the cloud stays up, rather than looking at potentially more minor issues.

c. What other government interventions do you think would be effective at addressing these risks?

We believe it's important that key roles in cyber security have protected status (in the same way that 'medical doctor' has protected status). This could help drive up and guarantee standards. Individuals would not be able to give themselves such titles unless they were proven to be qualified and their competence was validated on a regular basis.

Certain roles and responsibilities could require delivery by those with a particular level of qualification (eg Chartered Cyber Security Professional through the UKCSC). An example would be for those responsible for signing off building control systems or control systems for key infrastructure (eg transport systems, power plants).

26. Barriers in the open source community

a. To what extent do you think the following government interventions would be effective in addressing risks specific to open source software development?

- Guidance on how to increase secure development of software in the open source community

Somewhat effective

- Work with industry to develop mapping tool to understand which open source components are most critical

Somewhat effective

b. Please explain your answers to the above

- Guidance

Contextually sensitive risk analysis should be done on each project to assess its criticality.

- Work with industry

The value gained in identifying the most critical open source components needs to be ascertained. The risk for government in doing so is that it will encourage bad actors to target it, knowing that it can have severe impacts.

c. What other government interventions do you think would be effective at addressing these risks?

It would be useful for open source code to be regulated and stamped as credible in the same way that software elements are being considered by the EU Cyber Resilience Act, and a national library of approved code developed. Software credibility could be achieved at two different levels: self-certification of code for non-critical software, and third-party certification for critical software. Details would need resolving such as how critical / non-critical criteria are determined, whether all software interaction with government systems requires third-party certification, how to control quality, and approval sector by sector. Processes would need to be put in place to ensure a streamlined, efficient system that didn't stifle development and innovation.

27. Security and resilience in the distribution of software

a. To what extent do you think the following government interventions would be effective in addressing cyber risks linked to the actions of those who sell or resell software or software licences, or those who manage software services? Somewhat effective

- **Guidance on best practice (e.g. to assure the software they sell, secure their own networks and information systems)**

- **Accreditation of software vendors, resellers or providers who follow best practice (e.g. certification or trusted vendor marketplace)**

- **Regulation requiring software vendors, resellers or providers to follow a minimum standard (e.g. attestation on security measures they implement, notifying customers of incidents etc.)**

c. What other government interventions do you think would be effective at addressing these risks?

Please see the response to Q26.

28. Transparency and communication of software materials, vulnerabilities and incident management

a. To what extent do you think the following government interventions would be effective in addressing risks linked to visibility and communication of software materials, vulnerabilities and incident management?

- **Certification of software developers and vendors who adhere to best practice in promoting transparency**

Somewhat effective

c. What other government interventions do you think would be effective at addressing these risks?

Software incidents are not necessarily due to malicious behaviour – they could equally be due to unexpected software behaviour. As such, it would be useful to establish a regulated, secure approach where failures suspected of being as a result of vulnerabilities can be freely shared without liability. This could function in the same way as the safety reporting system for aircraft faults, which allows for safe reporting of actual or potential safety issues and avoids cover ups that could have severe consequences.

In the same vein there could be a criminal offence for not disclosing a breach of software integrity.

29. Procurement, supplier assurance and supplier management

a. To what extent do you think the following interventions would be effective in addressing cyber risks linked to software procurement, supplier assurance and supplier management?

Somewhat effective

- **Tools to help businesses implement guidance on securing their own supply chains (e.g. recommended clauses to include in contracts)**
- **Training resources aimed at procurement and contract management teams**
- **Work with industry to develop and promote tools that support businesses in securing their own supply chains**

c. What other government interventions do you think would be effective at addressing these risks?

It would be useful to establish a 'blue tick' scheme that considers the software and how it is being used across the whole supply chain. It may be that there are product and organisational certifications so that consumers can be confident in the security of the products or services that are critical to their businesses. Certification could be handled by private companies (in the same way that CE marking is managed), but regulated and audited by government to ensure standards are maintained. This approach would generate necessary business in an efficient way without burdening Government with delivery issues and costs.

30. Maintenance, configuration and use of software by the customer

a. To what extent do you think the following interventions would be effective in addressing cyber risks linked to the ongoing maintenance, configuration and use of software?

Somewhat effective

- **Guidance and comms campaigns to promote minimum actions businesses should take to secure the software they use**
- **Training resources aimed at non-cyber security specialists**
- **Work with software vendors to minimise the knowledge and actions required of customers to secure software products (e.g. building in prompts to change default passwords, or ensuring that multi-factor authentication is opt-out rather than opt-in).**

c. What other government interventions do you think would be effective at addressing these risks?

Whatever interventions are adopted, it's important that risks are quantified, that measures taken are proportionate and cost effective, and that they take account of the criticality and extent of software use in approved ways, its up to date nature, business size etc.

31. What do you think are the greatest challenges in implementing the potential interventions outlined above?

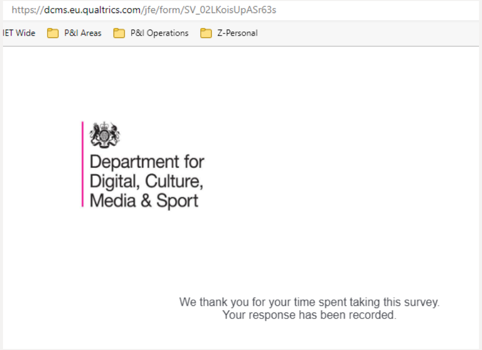
Policy in this area will not stand still. This requires a Government / industry task force, best organised by sector, to ensure UK interests are served.

The national economic security of the UK's commercial and service sectors is dependent on suppliers and systems based outside UK borders. Consequently they are outside UK Government control, and some risks comes with such remote delivery and software updates. Government intervention should focus on bringing more resilience and security back under UK control, where possible.

Currently the UK is vulnerable to crime-focused, state-sponsored or ideologically-based terrorism that could shut down UK-businesses for short or extended periods of time. The means of ensuring the ongoing development, resilience and maintenance of critical infrastructure is key.

The management of cyber risks needs to feature as a core element of the UK's national recovery plan. This requires consistent resource investment on the part of the Government to maintain technological excellence and competitiveness.

28/04/23



Department for
Digital, Culture,
Media & Sport

We thank you for your time spent taking this survey.
Your response has been recorded.