BCS, The Chartered Institute for IT

Submission:

Department for Science Innovation and Technology Code of Practice for Software Vendors: call for views

August 2024

Compiled by BCS Senior Policy and Public Affairs Manager, Claire Penketh

BCS, The Chartered Institute for Information Technology
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY

Executive Summary

This is the BCS response to the call for views from the Department for Science, Innovation and Technology on a voluntary Code of Practice for Software Vendors which sets out the security and resilience measures which should be expected of organisations which develop or sell software.

Whilst overall our experts believe the principles are an important step to ensuring software resilience, they do have some additional recommendations:

- The Code of Practice should be mandatory, not voluntary, to ensure effective take-up and a level playing field for all firms.
- There must be an accountable person for software quality on a company's board (or at senior management level) who is a competent, ethical, registered technical professional, preferably with chartered status.
- Standards should be adopted or developed that set out clear, consistent terminology for best practice
- The government should create a central point for collating incident software failure reports, including near misses, and that data should be published.
- The Code of Practice needs to be accessible, understandable and relevant for SMEs who may need extra support to implement it.
- Artificial Intelligence should be included in the scope of the Code of Practice, as it is also subject to code errors in a similar way to any other software system.
- Companies need to be encouraged to service resilience and to focus on their business continuity and disaster recovery plans to deal with the consequences of an outage.
- There should be standardised contractual clauses, including Service Level Agreements that have penalties built in and are quantifiable by metrics.

BCS has over 50 specialist interest member groups. For this consultation we asked for contributions from our Software Testing Specialist Group, the Information Security Specialist Group, and the IT Leaders Forum.

Several of our recommendations are also drawn from our experts' reactions to the CrowdStrike outages, and our responses to the previous government's calls for views on software resilience and security for businesses and organisations, the cyber security code of practice, and the cyber resilience of the UK's critical national infrastructure.

Who we are

BCS, The Chartered Institute for IT is the professional body for technology, with over 70,000 members. Our purpose, as defined by a Royal Charter, is to promote and advance the education and practice of computing for the benefit of the public., BCS brings together academics, practitioners, industry and government to share knowledge, promote new thinking, inform the design of new curricula, and shape policy.

Questions relating to Chapter 1: Introduction

Q8: Do you agree with any of the following statements? [checkboxes]

- The market is currently operating with appropriate levels of secure by design principles.
- The government should produce guidance that will show software vendors what "good" cyber security looks like. ✔
- There should be an assurance / certification scheme for software. ✔
- There should be mandated security regulations for all software. ✔

Q9: Are there any types of organisations for which this Code of Practice would not be suitable?

Q10: Do you agree that senior leaders in software vendor organisations should be the target audience of this Code of Practice?

- Yes ✔

Questions relating to Chapter 3: How organisations procuring software should use this Code of Practice

Q11: If one was available, how likely would your organisation be to use to a voluntary Code of Practice for software vendors to inform

a) Procurement?

- Very likely
- Likely
- Neutral ✔
- Not likely
- Definitely won't use
- Don't know

b) Supplier management processes?

- Very likely
- Likely
- Neutral ✔
- Not likely
- Definitely won't use
- Don't know

Questions on Chapter 4: Voluntary Code of Practice for Software Vendors

The next questions are going to ask you specifically about the Code of Practice that has been designed and proposed by DSIT. The questions will be focused on individual actions asked by the Code.

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure the organisation follows an established secure development framework.

Q12: Do you agree with this provision?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

Q13: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure the organisation has a clear process for testing software before distribution.

Q14: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure that the organisation follows secure by default principles throughout the development lifecycle of the product.

Q15: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔

- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations should do the following:

- Ensure secure by design principles are followed throughout the development process.

Q16: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations should do the following:

- Encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure.

Q17: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

We have asked you questions on the following provisions of principle 1:

Principle 1: Secure design and development

This principle ensures that the product or service is appropriately secure when provided.

The Senior Responsible Officer in vendor organisations shall do the following:

1.1 Ensure the organisation follows an established secure development framework.

1.2 Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

1.3 Ensure the organisation has a clear process for testing software before distribution.

1.4 Ensure that the organisation follows secure by default principles throughout the development lifecycle of the product.

The Senior Responsible Officer in vendor organisations should do the following:

1.5 Ensure secure by design principles are followed throughout the development process.

1.6 Encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure.

Q18: Do you think there is anything missing from this Principle? If so, what? [free text]

The principles are good. Our experts do, however, have concerns about whether they tackle the right problems. Development is a start not an endpoint.

Q19: Do you have any other comments or feedback relating to this Principle? [free text]

The challenge comes when this principle is tested against something like the CrowdStrike outage - should Microsoft be held responsible for the code error at CrowdStrike, or should they have assumed it could happen and ensured break points in their software to prevent errors migrating?

Regarding 1.3, distribution is not a once-a-year function, it is ongoing and so the updating process needs testing and validation against errors on the updates. Software is continuously updated and downloaded as part of contracted services eg Microsoft licence.

The wording in 1.4 reflects an inappropriate model of the digital service delivery landscape.

The wording in 1.6 we believe should be 'ensure' not 'encourage'. free text

Principle 2: Build environment security

Senior Responsible Officers in vendor organisations shall do the following:

- Ensure the build environment is protected against unauthorised access.

Q20: Do you agree with this action?

- Yes – I think this action should be included as a "shall" ✔
- Yes – I think this action should be included as a "should"
- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 2: Build environment security

Senior Responsible Officers in vendor organisations should do the following:

- Ensure changes to the environment are controlled and logged.

Q21: Do you agree with this action?

- Yes – I think this action should be included as a "shall" ✔
- Yes – I think this action should be included as a "should"
- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 2: Build environment security

Senior Responsible Officers in vendor organisations should do the following:

- Ensure you are using a build pipeline you trust.

Q22: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 2: Build environment security

This principle ensures that the appropriate steps are taken to minimise the risk of build environments becoming compromised and protect the integrity and quality of the software.

Senior Responsible Officers in vendor organisations shall do the following:

2.1 Ensure the build environment is protected against unauthorised access.

Senior Responsible Officers in vendor organisations should do the following:

2.2 Ensure changes to the environment are controlled and logged.

2.3 Ensure you are using a build pipeline you trust.

Q23: Do you think there is anything missing from this Principle? If so, what? [free text]

Q24: Do you have any other comments or feedback relating to this Principle? [free text]

This principle neglects sources of error other than unauthorised access, e.g. errors by authorised users, or new versions of components causing erroneous errors elsewhere. The point here is that software is a complex tightly coupled system and the principles seem to apply to simple linear systems.

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure that software is distributed securely to customers.

Q25: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.

Q26: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure the organisation implements and publishes an effective vulnerability disclosure process.

Q27: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure the organisation provides timely security updates, patches and notifications to its customers.

Q28 Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations shall do the following:

- Ensure that vulnerabilities are appropriately reported to the relevant parties.

Q29: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”

- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 3: Secure deployment and maintenance

Senior leaders in vendor organisations should do the following:

- Make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.

Q30: Do you agree with this action?

- Yes – I think this action should be included as a "shall" ✔
- Yes – I think this action should be included as a "should"
- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 3: Secure deployment and maintenance

This principle ensures [gr14] that the product or service remains secure throughout its lifetime, to minimise the likelihood and impact of vulnerabilities.

The Senior Responsible Officer in vendor organisations shall do the following:

3.1 Ensure that software is distributed securely to customers.

3.2 Ensure the organisation implements and publishes an effective vulnerability disclosure process.

3.3 Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.

3.4 Ensure that vulnerabilities are appropriately reported to the relevant parties.

3.5 Ensure the organisation provides timely security updates, patches and notifications to its customers.

Senior leaders in vendor organisations should do the following:

3.6 Make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.

Q31: Do you think there is anything missing from this Principle? If so, what? [free text]

BCS believes there should be the monitoring and reporting of data software outages and near misses and that the data should be published. It is of great value to users and can lead to overall improvements in resilience.

Q32: Do you have any other comments or feedback relating to this Principle? [free text] We reiterate that software is a tightly coupled complex system so user organisations struggle to keep up to date with a multiplicity of security updates, patches and notifications. Further, updates from different

vendors may be incompatible. Hence the disclosure as in 3.6 of incidents and near misses is important.

Principle 4: Communication with customers

Senior Responsible Officers in software vendor organisations shall do the following:

- Ensure the organisation provides information to the customer, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.

Q33: Do you agree with this action?

- Yes – I think this action should be included as a "shall" ✔
- Yes – I think this action should be included as a "should"
- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 4: Communication with customers

Senior Responsible Officers in software vendor organisations shall do the following:

- Ensure the organisation provides at least 1 year's notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.

Q34: Do you agree with this action?

- Yes – I think this action should be included as a "shall" ✔
- Yes – I think this action should be included as a "should"
- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 4: Communication with customers

The aim of this principle is to ensure that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

Senior Responsible Officers in software vendor organisations shall do the following:

- Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.

Q35: Do you agree with this action?

- Yes – I think this action should be included as a "shall" ✔
- Yes – I think this action should be included as a "should"
- No – I think this action should not be included in this Code of Practice
- I don't know

Principle 4: Communication with customers

The aim of this principle is to ensure that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

Senior Responsible Officers in vendor organisations should do the following:

- Ensure that high level information about the security and resilience standards, frameworks, organisational commitments and procedures followed by the organisation is made available to customers.

Q36: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 4: Communication with customers

Senior Responsible Officers in vendor organisations should do the following:

- Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident. How this would be done should be documented and agreed in contracts with the customer.

Q37: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 4: Communication with customers

Senior Responsible Officers in vendor organisations should do the following:

- Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

Q38: Do you agree with this action?

- Yes – I think this action should be included as a “shall” ✔
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 4: Communication with customers

This principle ensures that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

Senior Responsible Officers in software vendor organisations shall do the following:

4.1 Ensure the organisation provides information to the customer, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.

4.2 Ensure the organisation provides at least 1 year's notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.

4.3 Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.

Senior Responsible Officers in vendor organisations should do the following:

4.4 Ensure that high level information about the security and resilience standards, frameworks, organisational commitments and procedures followed by the organisation is made available to customers.

4.5 Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident. How this would be done should be documented and agreed in contracts with the customer.

4.6 Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

Q39: Do you think there is anything missing from this Principle? If so, what ? {free text]

Q40: Do you have any other comments or feedback relating to this Principle? [free text]

The information needs to be accessible, understandable and relevant for SMEs who may need additional support from the government. A one stop shop for such organisations would be a good strategy, as opposed to having information available in several locations.

Also we would query if vendors are happy for purchasers to have internal data on organisation's procedures (4.4)

(Q41 - 45 not relevant to BCS as they concern an Organisation/Business that is involved in the sale or development of software")

Questions on Chapter 5: Supporting materials

Q46: Are the proposed technical controls suitable for measuring compliance with the Code of Practice for software vendors?

- Yes
- No ✔
- Don't know

Q46b [if Q44="no"]: Why is it not suitable? [Typically, organisations may operate systems with software from hundreds of vendors. For most user organisations, this level of inventory and checking is only feasible for the relatively few components delivering Important Business Services (as in Bank of England regulations for Financial Sector.) [CP21]

Q49: Do you have any other comments about the technical controls outlined above and the implementation guidance example (attached in B)? [

1. Software services are now mostly delivered through tightly coupled complex systems. One characteristic of such systems is that they must be expected to fail. This places new demands on IT, procurement and risk professionals. It also means that Boards need to become accountable for service breaches and demand the tools to understand their exposure.

2.Software is embedded in sensors, controllers, devices, with a module often sold by hundreds of companies. This software may have vulnerabilities not understood by the companies selling the devices, or their customers. Even if the supplier of the software module produces a new version without the vulnerabilities, it is not often an environment in which the updated version can be realistically retro-fitted.

3.Services supplied by software rather than persons (e.g. face-to-face or by phone call) are pervasive. This means that many citizens and customers are likely to be wrestling with interfaces unfamiliar to them.

4. According to TechUK's 2022 Digital Economy Monitor, 57% of UK IT firms find the present talent shortage and access to skills among the biggest barriers for their companies.

Q50 - [if Q3 = "An organisation that procures software"]: As a customer procuring software, what other supporting materials would be helpful to enable you to request adherence to this Code of Practice from your suppliers? [check boxes]

- Standardised contractual clauses
- Guidance on how to assess suppliers' adherence to the Code
- Standardised templates for supplier attestation of compliance with the Code
- Training for non-cyber specialists
- An assurance scheme or certification
- Product security testing labs
- N/A - my organisation does not procure software
- Other [Although BCS is not responding as an organisation that procures software, all the above points would be of benefit] ✔

Q51 not relevant to BCS as we're not an Organisation/Business that is involved in the sale or development of software".

Survey close

Q52: Do you have any other feedback on our Code of Practice ?

The Four Principles

We broadly agree with the Four Principles outlined in the Code of Practice as they are an important step toward enhancing our national software resilience. The CrowdStrike outage shows the huge impact that a software failure can have on our interconnected systems which now run everything we rely on. However, these principles alone are not enough.

Increasingly, software is part of a complex supply chain. A software component is embedded in devices or vehicles or telecom systems etc. This means that software vendors are not able to anticipate what other software may be integrated with their product to implement a system. Typically, organisations may operate systems with software from hundreds of vendors – the vendors cannot ensure, for instance, the information in section 4 (communication with customers) is relayed to the end user. Vendors supplying components integral to supply chains should be able to supply development metrics but cannot commit to communication or maintenance metrics.

We have taken a broader look at what other measures could be taken to improve our national software resilience:

Mandatory Code of Practice

A mandatory Code of Practice with annual reporting would be more effective than a voluntary code, hence why the response to question Q11. We also recommend that boards of organisations that provide UK Critical National Infrastructure (CNI) services should have an accountable company board member for cyber and software resilience. Improved trust should be established to enable more effective sharing with private sector organisations that provide or support UK CNI services.

Standards

Adopt and develop standards in this area that set the framework for good practice. Inspiration could be taken from international technical standards such as ISO/IEC – such as the 'accountability and governance', ability to absorb, adapt and effectively respond to change, and risk management principles. The technical and operational standards provide management systems, processes and measurement methods to support implementation of the principles. In Europe, for instance, with the EU AI Act we now have standards that have a legal basis.

Centralised, Regulatory Framework for Incident Reporting

In terms of procurement, supplier assurance, and supplier management (information sharing on failures and known causes) studies by the BCS IT Leaders Forum (itlf-software-risk-resilience.pdf (bcs.org) and The Elephant in the Room) found that information asymmetry between purchasers and suppliers was extreme.

The government should create a central point responsible for collating incident reports, similar to the Mandatory Occurrence Reporting system operated by the UK Civil Aviation Authority since 1976. Government departments could take the lead in publishing failure data on their own services, using a framework based on the RDSPs proposed by the NIS. This framework could cover aspects like availability, integrity, authenticity, confidentiality, risk, and material damage to users.

Government support of an industry collaboration to publish information on failures and known causes would allow Boards to make more informed decisions about service resilience. This measure would also provide a firmer basis for follow-on actions, and could position the UK as an economy supported by resilient digital services

Detection and sharing of information are often limited to government organisations. Incident management systems should also pay attention to "near misses," as seen in aviation and nuclear industries (Risk Analysis, Vol. 33, No. 3, 2013, DOI: Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems, by J. Park, T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkov). Introducing such incident reporting systems for software failures could position the UK as an economy supported by resilient digital services.

Balancing Deterrence and Learning

Care must be taken to balance the deterrent effect of fines for software failure with the benefits of using the reporting process for learning purposes. This approach would not be about assigning blame but about enhancing industry-wide practices in cybersecurity and software resilience. Again, returning to the CrowdStrike incident, this appeared to be a simple update, which had catastrophic consequences. Whilst investigations into its cause are ongoing, it highlights the importance of learning from whatever mistakes happened, so they are not repeated.

Support for SMEs

The principles will work well for large organisations with IT expertise and simple supply chains. Even if adopted by all software vendors though, SMEs would struggle to make sense of the multiplicity of data provided. Software vendors often supply software embedded in devices shipped by third parties, who may not be diligent in - or unable to - install updated versions.

The government should work with organisations representing small and medium-sized enterprises (SMEs) to better understand their needs. SMEs software vendors might need specific support to navigate a complex reporting system. The language and terminology in the Code of Practice should be explicitly "low context" to avoid requiring significant prior tacit domain knowledge.

The government should create a 'one-stop shop' for advice on cyber security and software resilience, which caters for organisations in different sectors and of different sizes.

It would be helpful if the Code of Practice could link to established information, cybersecurity frameworks, and standards. This would enable organisations to 'map' their current arrangements to well-defined, well-understood and well-established frameworks.

Require company to include board members and/or senior C Suite members (CPO, or CISO) or someone responsible for quality, who will be held accountable for the firm’s cybersecurity throughout its life cycle. This person must be a skilled, competent, ethical and highly skilled tech professional.

AI should be included

AI is outside the scope of the Code of Practice and we would recommend it should be part of it. AI is implemented in software. The concerns over the introduction of AI often focus on the historic data used to train the system. However, AI is also subject to code errors in a similar way to any other software system. This can produce erroneous results that are not identified as a service breach, so humans do not know that an error has occurred and make wrong decisions. And humans make wrong decisions more frequently when augmented with AI assistants (automation bias). Communication of known software vulnerabilities in open source (FOSS) or commercial off the shelf software (COTS) is not systematically available.

An additional set of risks arises from the partial or wholesale exit of key developers from a particular community. This may create problems like those of ‘legacy code’ where the knowledge necessary to maintain and further develop code will be absent.

Incident Management

Since software is a complex, tightly coupled system, appropriate incident management (handling of service breaches) is crucial for increasing resilience. Companies need to be encouraged to focus on their business continuity and disaster recovery plans, on how to deal with the consequences of an outage.

Developing regulations that require software developers and vendors to meet minimum transparency standards (e.g., providing customers with a right to audit and request information, creating a legal requirement to notify customers of incidents affecting them) is likely to be effective. This approach incentivizes doing it right and being shown to be doing it right, potentially instilling a sense of pride in achieving certification as part of a larger package of certification elements.

Essential Security Measures

From a software testing perspective, integrating security from the outset of the development lifecycle and employing rigorous testing protocols are essential. This includes continuous monitoring, regular, safe updates, and thorough threat modelling to ensure vulnerabilities are identified and mitigated before software reaches the end user.

Increasingly, software is delivered as a service and there is a need for a Service Level Agreement contract for users. The user agrees to accept a defined level of service from the vendor. This provides a relevant measure to set expectations for the user. It is also measurable, and the agreement can be enforced. However, SLAs alone are not the answer because things move on quickly and performance targets need to be constantly reviewed. SLAs can also be 'gamed', e.g. can be shown to have been met even where actual service levels have deteriorated.

Education and Training

Education and training are vital. There are elements of cybersecurity and software resilience that are not obvious or straightforward. Training staff at all levels on risks and countermeasures is an effective means of reducing organisational problems. Government departments could lead by example, holding business continuity exercises to alert senior management to vulnerabilities and sharing the results with the wider software community.

Publicising Best Practices

Best practices should already incorporate cybersecurity, but publicising these practices would be beneficial. Setting the most secure defaults from the start is essential. Government departments could share information on recommended default settings.

1. 98% of respondents to the government's call for views on software resilience and security thought there was a need for greater government and/or industry intervention to address risks relating to software development security, with 65% believing that both would be needed to ensure the security and resilience in the distribution of software. ↩
2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation, EU, 2022. ↩
3. The UK Product Security and Telecommunications Infrastructure (Product Security) regime, Department for Science, Innovation & Technology, 2023. ↩

4. Code of practice for app store operators and app developers (updated), Department for Science, Innovation & Technology, 2023 . ↩
5. Capability Hardware Enhanced RISC Instructions (CHERI), University of Cambridge, Department of Computer Science and Technology. ↩
6. Technology that is Secure by Default has the best security it can without you ever knowing it's there, or having to turn it on. Further detail on secure by default principles can be found here: https://www.ncsc.gov.uk/information/secure-default ↩

"Secure by design" means that software products and services are built in a way that reasonably protects against malicious cyber actors successfully gaining access. This includes identifying the key risks and building protections into product design

---

Acknowledgments:

Thanks to the contributions to this report from:

Gill Ringland, member of the BCS IT Leaders Forum and Service Resilience and Software Risk expert.

Nicola Martin, Chair of the Software Testing specialist group Committee and BCS Council member

Adam Leon Smith DEng FBCS Chair of the BCS Fellow Technical Advisory Group

Dr David Miller FBCS CITP FIET FCIM, past chair of the BCS IT Leaders Forum