AI and Cybersecurity Under the Spotlight: UK Publishes New Codes for Software Security and Warns on AI Cybersecurity Divide

Client Alert | 8 min read | 05.19.25

Earlier this month the National Cyber Security Centre ("**NCSC**") hosted CYBERUK, the UK government's flagship cybersecurity event. On 7 May the NCSC launched their report "**Impact of AI on cyber threat from now to 2027**" ("**Report**"), whilst the Department for Science, Innovation and Technology ("**DSIT**") published a new voluntary **Software Security Code of Practice**, ("**Code**"). Cybersecurity and AI are under the spotlight in the UK. Eyes are also on the recently unveiled US/UK trade agreement and the possibility of a further transatlantic tech-focused agreement to cement prior Technology and Data Partnership discussions to create a US/UK "digital bridge."

The Report

The NCSC's newly released Report warns of a "growing divide" between organisations that keep up with threat actors using AI and those that remain vulnerable to attacks. It bleakly highlights the "remote chance of universal access to AI" that would provide vital cybersecurity defence to companies. The NCSC predicts a digital divide over the next two years, raising the UK's overall risk profile to cyber threats.

The Report maintains that threat actors are "almost certainly" already using AI in their tactics to make their operations more effective, increasing their ability to exploit known vulnerabilities. It delves into how hackers use AI in various stages of their attacks, including victim reconnaissance, malware generation, social engineering, and vulnerability research, to the point that some of the more capable actors are building their own AI models. Other groups will still have access to commercial and open-source AI models—perhaps with cyber tools made available "as a service."

The NCSC particularly highlights AI-assisted vulnerability research and exploit development ("**VRED**") as the most significant development, allowing threat actors access to systems by identifying flaws in code or configurations, and shrinking the already short time between disclosure of a known vulnerability and its exploitation.

The Report also alerts organisations to their increased risk when using AI systems because of the greater available attack surface (i.e., a larger number of potential vulnerabilities and entry points in the relevant systems), particularly within critical national infrastructure. It also cautions developers who may prioritise competitive advantage in releasing updates over security—highlighting the increased relevance of the recent voluntary security-related codes. The NCSC is strongly signalling that cybersecurity strategies should be the focus for all businesses, and that keeping up will be "critical to cyber resilience."

The NCSC's **press release** for the Report references the voluntary **Code of Practice for the Cyber Security of AI** ("**AI Code**"), which was published at the end of January 2025 and adopted on 7 May as a global standard by the European Telecommunications Standards Institute, establishing baseline measures that organisations

globally should implement to ensure the security of AI systems and models. It looks to create a standard on how developers, data custodians, and deployers (such as system operators) of AI should protect and manage risks of cyber threats across the supply chain.

The AI Code sets out 13 principles covering elements of secure design, development, deployment, and end of life, alongside a separate implementation guide. Whilst voluntary, this clearly indicates the focus of UK regulators on the cybersecurity of AI, and the unique risks that apply in comparison to generic software development.

The Code

The Code is intended to improve software security and resilience. It follows hard on the heels of the voluntary AI Code (as detailed above). The NCSC, together with various academic and industry experts, was involved in creating the Code which also considers views obtained from the public obtained between May and August 2024. The Code is also co-sealed by the Canadian Centre for Cyber Security.

The Code aims to assist software vendors and their clients in minimising the chance of and the effects of software supply chain attacks. Such incidents often result from preventable vulnerabilities in software development and maintenance practices and can be made worse by bad communications between organisations and their software suppliers.

The Code comprises 14 principles that software vendors are expected to implement to ensure a minimum level of software resilience and security across the market. The principles are divided into four main themes, apply to all types of software provided to businesses and are considered to be fundamental and capable of being realised by all organisations.

The Code is likely to be relevant to: (i) software developers and distributors; (ii) software resellers (to whom only principles 3 and 4 apply); (iii) software developers only (to whom only principles 1 and 2 and potentially 3 apply); and (iv) open-source developers and maintainers (although these are not regarded as the Code's primary audience) whether on premises or 'as a service.' The Code is considered to be most relevant to the sale and distribution of proprietary software in the context of business-to-business commercial relationships. As the Government continues apace with digital transformation and AI adoption, we anticipate a greater focus on compliance for those supplying in to critical infrastructure and all levels of the public sector and customers undertaking significant digital transformation may find it useful to assess how suppliers maintain the resilience and security of their software.

The Code targets senior leaders in software vendor organisations and is supplemented by implementation guidance to assist technical teams who are tasked with applying the principles outlined in the Code. It is suggested that a "Senior Responsible Owner" should be appointed at senior leadership level to be responsible for the principles being followed by relevant organisations. The Code will also be relevant to specialist and technical teams and roles and organisations procuring software. Some of these governance requirements and principles bear similarities to Facility Security Clearance (formerly known as List X) ("**FSR**") for holding Government protectively marked information at a commercial site. For example, there are risk-based approaches for security, implementation of layered controls (whether it be code reviews with separate build environments to layered physical security controls) and accountability at senior levels of an organisation (like appointing a Cyber Security Officer).

The Government has produced a self-assessment form to sit alongside the Code which can be utilised to assist with internal compliance monitoring or provided to customers to provide software security assurance.

The Code adopts the NCSC's Principles Based Assurance approach and is divided into a set of "Assurance Principles and Claims" which derive a set of ideal-scenario claims that, if met, mean the software vendor is achieving the Code's principles. The Government is also creating a certification scheme based on this compliance process.

The Code's first theme relates to **secure design and development**, with the aim of making sure that software and services are sufficiently secure when provided. The principles set out under this theme include, among others, following an established secure development framework and understanding the composition of the software and assessing risks linked to the ingestion and maintenance of third-party components throughout the development lifecycle.

Building environment security is the focus of the second theme. The intention is that suitable measures should be implemented to reduce the risk of build environments becoming jeopardised and to protect the integrity and quality of the software. The relevant principles include protecting the build environment against unauthorised access and controlling and logging changes to the build environment.

To ensure that software remains secure throughout its lifetime and reduce the possibility of and effect of vulnerabilities, the third theme of the Code concerns **secure deployment and maintenance.** Principles espousing this theme include, for example, having processes and documentation in place for detecting, prioritising and managing vulnerabilities in software components and providing timely security updates, patches and notifications to customers.

The final theme of the Code highlights **communication with customers.** Its underlying principles aim to ensure that vendors provide adequate details to customers to facilitate effective risk and incident management. Relevant principles include, among others, specifying the level of support and maintenance provided for the software being sold and also making information available to customers about notable incidents that may cause significant impact to customer organisations.

Although the Code was created by DSIT and the NCSC, it is voluntary. Organisations that choose to comply with the Code will be able to use it to provide reassurance to their customers as to the security and resilience of their software products and also as an internal compliance monitoring tool. Complying with the Code could also prove useful to organisations as a mitigating factor to present to relevant regulators (*e.g.*, the Information Commissioner's Office) in the event of a cyber incident.

On the Horizon

As noted above, the newly agreed UK-US trade deal has been heralded as a landmark deal in Britain's national interest, focusing on car manufacturing, steel, and farming, with hopes that this will be one of many international deals for the UK. The Government has noted that it will continue to work on the remaining sectors.

The US has agreed that the UK will receive preferential treatment in any further tariffs which are put in place as part of Section 232 investigations (investigations under the US Trade Expansion Act of 1962, as amended, to determine whether imports of certain goods threaten national security). The deal could possibly facilitate a

new technology collaboration between the UK and the US with a focus on significant aspects of advanced technology, such as aerospace and space, life sciences, nuclear fusion, quantum computing, and biotech. As reported in The Guardian, the UK's ambassador to the US, Peter Mandelson, confirmed that a "technology partnership" would be negotiated "over the coming months". It's one many will keep under surveillance, with trade associations techUK and the Information Technology Industry Council ("**ITI**") noting in their 9 May **joint statement** the opportunity to "set the global tech agenda" to define the future with "trust, openness, innovation, and security".

Comment

While the UK cyber sector was described at the CYBERUK 2025 event by Chancellor of the Duchy of Lancaster Pat McFadden as a "prime target for economic growth", as highlighted by the Report, the threat posed to UK organisations by cybersecurity vulnerabilities and the UK's overall cyber risk are matters of serious concern for the Government. The Code, together with the AI Code and other relevant codes and guidance (such as the **Cyber Governance Code of Practice**), demonstrate the Government's continuing focus on and commitment to improving cybersecurity in the UK. As demonstrated by recent reports of the "Scattered Spider" cyber-attacks on UK-based retailers (including Marks & Spencer, Harrods, and Co-op), organisations should take action to strengthen their cybersecurity protections and minimize cyber risks to the extent possible. Adhering to the Code and the AI Code should assist organisations with these endeavours.

Contacts

Emma Wright
Partner
London D | +44.20.7413.1315
ewright@crowell.com

Rafi Azim-Khan
Partner
London D | +44.20.7413.1307
San Francisco D | +1.415.365.7282
rafi@crowell.com

Clare Sellars
Counsel
London D | +44.20.7413.1309
csellars@crowell.com

Grace Tang
Associate
London D | +44.20.7413.1353
gtang@crowell.com

