UK exposed by cyber omission in Spring Statement as threats intensify, ISF chief warns

LONDON, UNITED KINGDOM, March 20, 2026 /EINPresswire.com/ -- Ministers are being urged to divert funding to strengthen cyber resilience after the Spring Statement made no reference to the threat, as tensions in the Middle East and risks linked to Iran prompt fresh warnings to UK organisations

The government's failure to mention cyber security in the Spring Statement risks leaving parts of the public sector exposed as tensions in the Middle East heighten the risk of cyber spillover, one of Britain's leading cyber security experts has warned.

Steve Durbin, chief executive of the Information Security Forum, said ministers should be prepared to divert funding from other digital projects to strengthen national resilience, particularly as Iranian-linked cyber activity increasingly targets critical infrastructure and could extend to British systems.

Departments should prioritise keeping essential services running during an attack by identifying their most critical functions, planning for disruption and investing in systems that can continue operating under pressure, he said.

Failure to plan for disruption and build resilient systems risks leaving organisations unprepared when an attack succeeds, with disruption to essential services and wider economic impact likely.

Speaking to The European's Juliette Foster, Durbin said organisations should assume breaches are inevitable and focus on how they respond when systems are compromised.

He said: "So, should government be spending more time looking into this? They should. Should they be diverting funds away from other projects that they've got, that they're thinking about in the digital sphere to bolstering cyber resilience? I think they should. Are they? Well, time will

tell."

"At some point in time, you will probably have some kind of incident, whether it be a full-blown breach, whether it be something much less serious than that. And so you have to be ready for that. You have to be prepared as to how you're going to respond to that."

Durbin's warning comes after the National Cyber Security Centre urged UK organisations to review their cyber security posture following the conflict in the Middle East, warning of a heightened indirect threat for entities with operations or supply chains in the region.

The NCSC said organisations should prepare for possible collateral impacts in Britain from Iran-linked hacktivists, review their external attack surface, increase monitoring where appropriate and consider signing up to its Early Warning service.

Critical national infrastructure operators were also urged to review guidance on preparing for severe cyber threat.

But the Spring Statement made no reference to cyber security, leaving government, public bodies and businesses exposed to what Durbin described as "very real concerns" over the security of major programmes.

"If you look at what's going on in the region, then the Iranian regime seems to be targeting critical infrastructure," he said.

"So if we bring that across into the UK, I would say absolutely critical infrastructure is in the spotlight."

Private-sector organisations face heightened risk through complex global supply chains and pressure on budgets, which could see cyber investment cut, while the public sector is exposed by the scale of its digital programmes and legacy systems, he added.

Cyber security must be built in from the outset, particularly across major initiatives including the NHS and digital identity, moving "in lockstep" with modernisation plans.

"If you're looking at it from the public sector perspective, then I have very real concerns around how secure some of the cyber programmes might be that we're thinking about rolling out," he said, warning that governments rushing "headlong into a digital environment" could pay more later if security was not funded properly at the start.

"There are no shortcuts that you can take. If you don't invest right at the beginning, it will cost you more in the long run."

Looking ahead, he said the core challenges facing UK organisations were unlikely to disappear in

the few years ahead.

Supply-chain exposure would remain, AI would continue to evolve on both sides of the contest, and the role of people inside organisations would stay central.

He added: “My hope would be that by the time we get to 2028, we will have done more to realise that the absolutely fundamental and critical role that people play in not just preventing some of these attacks happening, but in responding to them as well.”

Steve Durbin’s full interview with Business Matters will air on Bloomberg TV on Sunday 22 March at 9:30am (Sky 502, Sky Glass 505, Virgin 609, Freesat 208), and will be available thereafter on The European’s YouTube channel.

C Nugent-Isitt
CP Media Global
email us here