EINPRESSWIRE

ISF warns geopolitics will be the defining cybersecurity risk of 2026

LONDON, UNITED KINGDOM, January 9, 2026 /EINPresswire.com/ -- Geopolitics is set to become the dominant cybersecurity risk of 2026, the Information Security Forum warns, as nation states intensify digital espionage and pressure on critical infrastructure — and even paper back-ups regain importance as a last line of defence when systems fail

Cybersecurity risk in 2026 will be shaped less by opportunistic criminals than by geopolitics, as nation states increasingly weaponise technology, information and infrastructure, according to the Information Security Forum (ISF).

Speaking in a new broadcast interview, Steve Durbin, chief executive of the ISF, said the convergence of political tension, digital dependency and state-backed capability is pushing organisations into a far more volatile threat environment.

“If 2026 is anything like 2025, we’re going to have a bumpy year,” Durbin said. “Society has become very dependent on technology and nation states have understood that there is a lot of value in the information that is out there.”

Durbin warned that espionage has undergone a fundamental transformation. Activity that once required physical presence, risk and human networks can now be conducted remotely, at scale and with far lower cost.

“Espionage has been around for centuries but today there’s no need for spies to do things the hard way like they did in the past,” he said. “They can work from home very easily, so espionage has changed completely.”

That change, he argued, places businesses, public bodies and critical infrastructure directly in the firing line of geopolitical conflict, whether they see themselves as political actors or not.

“We have to come back to critical infrastructure,” Durbin said. “If you’re a key player in that space, you will be under significant attack at some point in time, if not already.”

The ISF believes governments have become increasingly aware that political leverage can be exercised through digital disruption as well as diplomacy.

“Some governments have woken up to the fact that politics itself can be weaponised,” Durbin said. “Others have understood they need to be playing a very strong defensive game, depending on where they happen to be in the world.”

He stressed that governments rarely operate alone, and that the security of national systems is deeply entwined with the private sector.

“Governments rarely work in isolation and work alongside large corporates,” he said. “It is this public–private partnership that we need to be focusing on in a geopolitical context.”

Durbin also raised concerns that many of the world’s largest organisations are failing to prepare for the long-term implications of quantum computing, despite the sensitivity of the data they hold.

Some sectors, he warned, will face particularly severe consequences if encrypted records become vulnerable.

“Organisations such as hospitals and NHS trusts that store huge amounts of sensitive, highly confidential health records should be concerned about quantum computing,” he said, adding that preparation timelines could stretch over several years.

Despite the rapid pace of technological change, Durbin cautioned against abandoning older safeguards altogether. In a geopolitically charged environment, resilience may depend on simplicity as much as innovation.

He said: “Today, it’s fashionable to go back to old paper-driven approaches. You can’t hack a bit of paper and we just need to store it safely. So although we’re all getting excited about technology, paper can be very useful.”

On regulation, Durbin reiterated the ISF’s long-held position that compliance alone does not deliver security, while acknowledging that voluntary action may no longer be sufficient.

“I’m not a big fan of regulation because I would like to think we could get the right balance,” he said. “Good compliance doesn’t mean good security, but good security does, in most cases, mean good compliance.”

He suggested that cybersecurity assurance is increasingly moving towards the logic of financial governance.

“I do think we’re getting to a point where companies need to consider their security systems in much the same way as a financial audit,” Durbin said. “Smart boards will be insisting on a security audit by a third party.”

While he would prefer companies to opt in voluntarily, Durbin acknowledged that regulatory intervention may become unavoidable.

At board level, the ISF is urging organisations to plan for failure as a matter of governance, rather than optimism.

“Boards need to plan for the day their defences fail,” Durbin said. “The starting point is to figure out how long you can be without your systems.”

He called for annual rehearsals of major cyber incidents and clearer identification of organisational priorities.

“It’s important to know what the crown jewels are in your organisation and know how to protect them,” he said. “Ultimately, it’s the board that remains responsible.”

Looking ahead, Durbin argued that no single organisation or sector can address geopolitically driven cyber risk alone.

“From now on, I think there is a need for us to embrace a cross-industry approach to sharing information,” he added.

Steve Durbin’s full interview with Business Matters will air on Bloomberg TV on Sunday 11 January at 9:30am (Sky 502, Virgin 609, Freesat 208), and will be available thereafter on The European’s YouTube channel.

C Nugent-Isitt
CP Media Global
email us here

in today's world. Please see our Editorial Guidelines for more information.