PSA demands public sector cybersecurity overhaul after Stats SA breach

Siphesihle Buthelezi Published 17 hours ago

2min

The PSA has urged an urgent overhaul of government digital infrastructure after a significant cybersecurity breach at Statistics South Africa.

Image: Supplied

The Public Servants Association (PSA) has issued a scathing call for a complete overhaul of government digital infrastructure following a confirmed cybersecurity breach at Statistics South Africa (Stats SA).

The breach targeted an HR database used for online job applications and reportedly exposed the personal information of thousands of job seekers. A cybercrime group has claimed responsibility for the attack, alleging they have siphoned 154GB of data, including over 450,000 files and are demanding a ransom of $100,000 (approximately R1.7 million).

The PSA expressed deep concern over the vulnerability of government systems, noting that this incident is part of a "growing pattern" of attacks on public institutions.

"The citizens are placed at risk of identity theft, fraud, and misuse of personal information," the PSA said in a statement.

"The growing incidence of targeted attacks against public-sector digital infrastructure demonstrates the urgent need for a comprehensive cybersecurity overhaul across all government departments."

The union has urged the government to move away from "outdated systems" and "inadequate patching," calling for a coordinated national cybersecurity strategy and the establishment of a dedicated response unit.

Despite the R1.7 million ransom demand, Stats SA has held a firm line, stating that it will not negotiate with the hackers. The agency stated it is adhering to legal protocols outlined by the Information Regulator and the Public Finance Management Act (PFMA).

In a brief media statement, Stats SA clarified that the breach was localised: "The system that was breached is exclusively the HR system available for job seekers to apply online."

Cybersecurity experts have backed the decision to ignore the ransom demand.

Richard Ford, Group CTO at Integrity360, warned that paying hackers is a "flawed recovery strategy."

"Beyond the ethical dilemma, the restoration process using an attacker’s decryption key is often significantly slower and less reliable than a well-orchestrated backup recovery," Ford explained. He further noted that paying a ransom can inadvertently paint a target on an organization’s back. "Paying can inadvertently signal to the larger threat actor ecosystem that the paying organisation is a 'good' target for future exploitation."

The PSA is now pushing for more than just technical fixes. They are calling for:

- Urgent investment in cyber hygiene training for public-sector employees.
- Full enforcement of consequence management measures.
- Modernization of digital monitoring and detection capabilities.

As the Information Regulator prepares to weigh in, the breach serves as a stark reminder of the fragile state of South Africa’s public-sector data security in an increasingly digital world.