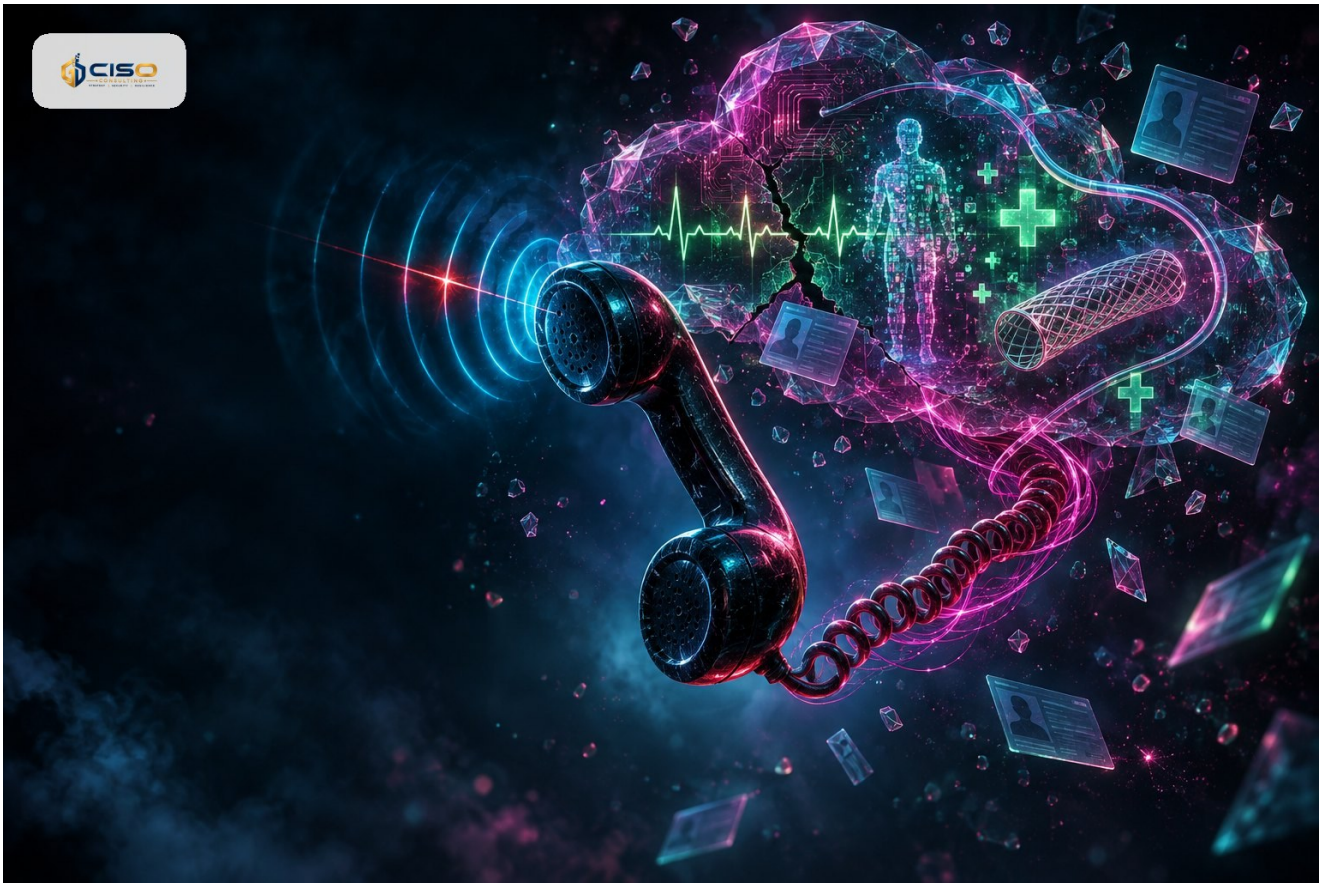
Boston Scientific confirms vishing-led cloud breach exposing personal and medical data



Boston Scientific is notifying people affected by a cloud breach that began with a voice phishing attack. Texas reports 117,789 affected individuals; the company says it is unrelated to its August 2026 incident.

- Attackers used social engineering through voice phishing (vishing) to reach the company's cloud infrastructure.
- The Texas Attorney General portal lists 117,789 affected people, with names, addresses, SSNs, government ID numbers, medical and health insurance information and dates of birth exposed.
- Patient medical records and data from remote monitoring, connected devices and clinical workflow applications were not exposed, according to the notice.
- The company reports no disruption to manufacturing, distribution, service or product safety.

> - A spokesperson said the incident is unrelated to the August 2026 intrusion, which began at an internet-facing network device.

Boston Scientific, a US medical device manufacturer, has begun sending breach notices after a cyberattack on its cloud environment. According to a notification sample filed with US authorities, the attacker used voice phishing to gain access to cloud infrastructure, exposing cloud-based applications and cloud-hosted data.

What was exposed

The company became aware of unauthorized access on May 12 and concluded that a data breach had occurred on November 5. Texas breach reporting lists 117,789 affected people. Exposed data included names, physical addresses, Social Security Numbers, government ID numbers, medical information, health insurance information and dates of birth.

The notice states that patient medical records and data from remote monitoring systems, connected medical devices and clinical case management applications were not exposed. The company reports no disruption to manufacturing, ordering, distribution or patient service, and no effect on product safety.

Context

This is the second incident the company has reported in 2026. The August incident caused outages and global operational disruption; CrowdStrike found that the attacker entered through an internet-facing network device and found no evidence of cloud application compromise. A spokesperson confirmed the two incidents are unrelated and declined to give further details.

Why it matters for Saudi institutions

The case shows that a phone call to staff can be enough to reach cloud environments. Institutions that rely on medical technology suppliers or hold health and identity data should check how identity verification works for help-desk and support calls, and how a supplier incident would be notified to them.

What to do now

1. Require strong identity verification, beyond personal details, for help-desk, password-reset and MFA-reset requests made by phone.
2. Train staff, including support and administrative teams, to recognise vishing and to report suspicious calls.
3. Review privileged access to cloud applications and data stores, and enforce phishing-resistant MFA where feasible.
4. Check contracts with medical technology and cloud suppliers for incident notification timelines and data-protection obligations.
5. Confirm your PDPL breach-notification process covers supplier-originated incidents involving health and

identity data.