# Feds warned Premera about security flaws before breach

By Originally published March 18, 2015 at 11:04 am Updated April 2, 2015 at 1:45 pm

Published: 2015-03-18 · Archived: 2026-04-02 12:33:06 UTC

In what the health insurer called a routine audit, federal officials found a handful of issues with Premera's network security — three weeks before a major breach first occurred.

By

Seattle Times staff reporter

Three weeks before hackers infiltrated Premera Blue Cross, federal auditors warned the company that its network-security procedures were inadequate.

Officials gave 10 recommendations for Premera to fix problems, saying some of the vulnerabilities could be exploited by hackers and expose sensitive information. Premera received the audit findings April 18 last year, according to federal records.

The company disclosed Tuesday that a breach occurred May 5, potentially exposing Social Security numbers, addresses, bank-account information, medical information and more for 11 million customers.

Premera didn't respond to the audit findings until June 30 and said at the time it had made some changes and planned to implement others before the end of 2014. The company, based in Mountlake Terrace, said it didn't discover the breach until January of this year and didn't disclose it until this week so it could secure its information-technology systems first.

Premera spokesman Eric Earling said the audit, conducted by the U.S. Office of Personnel Management (OPM), was routine. He said the company worked to address the issues raised and that the vulnerabilities described in the audit may not have been exploited by the hackers.

"We believe the questions OPM raised in their routine audit are separate from this sophisticated cyberattack," Earling said. He declined to discuss details of the hack, citing an ongoing FBI investigation.

In one part of the technology audit, federal officials conducted vulnerability scans and found Premera wasn't implementing critical patches and other software updates in a timely manner.

"Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached," the auditors wrote.

Premera responded to the auditors by saying it would start using procedures to properly update its software. But the company told the audit team it believed it was in compliance when it came to managing "critical security patches."

The auditors responded that the vulnerability scans indicated the company was not in compliance with that aspect. They suggested Premera provide evidence that it had implemented the recommendation, although the documents don’t say whether that occurred.

The auditors also found that several servers contained software applications so old that they were no longer supported by the vendor and had known security problems, that servers contained “insecure configurations” that could grant hackers access to sensitive information, and that Premera needed better physical controls to prevent unauthorized access to its data center.

Federal auditors examined Premera because it is one of the insurance carriers that participates in the Federal Employees Health Benefits Program. Auditors examined applications used to manage claims from federal workers, but also the company’s larger IT infrastructure.

Susan Ruge, associate counsel to the inspector general at the Office of Personnel Management, said the office is monitoring the situation at Premera, but hasn’t determined whether the data breach will lead to any unplanned audit work at the company.

Premera Blue Cross is the largest health-insurance provider in Washington state based on enrollment, and it has more than 6 million current and former customers in the state who could be affected by the breach. The company said the hackers may have gained access to customer information dating back as far as 2002.

The company has started to mail letters to the approximately 11 million affected customers in Washington and elsewhere.

---