CORVUS BY TRAVELERS

RISK PREVENTION CASE STUDY

Healthcare Provider

Company Information

Industry: Healthcare

Type: Regional provider/ facility

Employees: 2,000

Incident Type

Social engineering leading to fraudulent transfer of funds

Response time

Investigation initiated the day of discovery

Actions Taken

Forensic investigation, funds recovery (clawback), post-incident consultation on security hardening

Results

60% of funds returned to the organization; revision to policies and procedures on transfers and MFA implementation

Overview

A spear phishing campaign targeting healthcare executives led to a significant loss through the fraudulent transfer of funds. A quick response from Travelers led to the partial return of funds and improvements in prevention measures at the organization.

Challenge

A C-level executive at a regional healthcare provider was targeted in a spear phishing attack, which allowed the threat actor to take over the executive's digital corporate identity. In addition to providing access to the executive's business email account, the compromise provided the threat actor with administrative access to the organization's cloud email, storage and collaboration environment.

> **Note:** Although the use of Multifactor Authentication (MFA) was enforced for all accounts at the organization, the specific manner of MFA implementation was vulnerable to adversary-in-the-middle (AiTM) attacks, meaning the threat actor was able trick the victim into entering their unique temporary code into a spoofed login page, where it could be captured by the threat actor and used to break into the account.

Through the cloud environment, the threat actor was able to infiltrate other employee email accounts. The threat actor then sent phishing emails masquerading as various company employees, complete with fabricated forwarded email threads to create the illusion of previous exchanges that verified the information discussed. The fabricated threads included phone numbers controlled by the threat actor in order to further deceive recipients if they attempted to follow protocols for out-of-band authentication.

The most significant impact of the breach occurred when the attacker sent an email from the Chief Financial Officer's account to the finance team, instructing them to process a fraudulent invoice, resulting in a financial loss of $200,000.

Response

Once the organization discovered that the funds had been sent under deception, they filed a claim with Travelers. The Travelers Cyber Claim team assigned a dedicated claim manager to the case and initiated a wide-ranging response process, including:

- **Forensic Investigation:** A forensic team was brought in to investigate the extent of the threat actor's intrusion and piece together the timeline of events.
- **Data Mining:** An extensive data mining effort was undertaken to search for confidential and regulated data that may have been accessed or was at risk.
- **Tracing of Communications:** It was discovered that while one employee contacted the CFO regarding suspicious activity, they did not report it to the security team. Another employee proceeded with the wire transfer without having conducted out-of-band verification, highlighting a significant procedural breakdown.
- **Fund Recovery:** The Travelers Claim team initiated work with federal law enforcement to attempt to "claw back" the transferred funds.

Risk Prevention Case Study: Healthcare Provider

Company Information

Industry: Healthcare

Type: Regional provider/ facility

Employees: 2,000

Incident Type

Social engineering leading to fraudulent transfer of funds

Response time

Investigation initiated the day of discovery

Actions Taken

Forensic investigation, funds recovery (clawback), post-incident consultation on security hardening

Results

60% of funds returned to the organization; revision to policies and procedures on transfers and MFA implementation

Results

The investigation revealed the depth of the breach and its implications for the organization. While the immediate financial loss was substantial, the potential for broader legal consequences loomed large, with the risk of a class action lawsuit due to the exposure of confidential ata. In this case, the investigation did not reveal evidence of the exfiltration of data, limiting the risk of exposure.

The efforts to claw back funds were successful, with nearly two thirds of the stolen funds recovered through the efforts of federal law enforcement.

Note: From January 1, 2023, to December 31, 2024, Travelers has managed 2316 claims related to social engineering fraud. **During this same period, Travelers has recovered over $20 million in stolen funds, adding to a cumulative recovery total of nearly $110 million.**

In post-incident consultation the Travelers Cyber Risk Services team helped the organization to understand how their authentication technology could be improved to limit future AiTM attacks, and how to improve procedures to validate transfer instructions.

The incident provides a case study in how multiple layers of security controls must work in concert. Technological controls, such as the proper implementation of MFA, must be coupled with awareness of red flags and risk factors among employees, and with clear, well-understood policies and procedures for validating identities and information. With each of these components in place, risk of loss is reduced considerably.

CORVUS BY TRAVELERS

Corvus Insurance Holdings, LLC. 100 Summer Str., Suite 1175, Boston, MA 02110 www.corvusinsurance.com