

U.S. POSTAL SERVICE BREACH: A TIMELINE

At a Nov. 19 congressional hearing, Randy Miskanic, vice president for secure digital solutions at the United States Postal Service, provided details about its data breach and how the Postal Service responded.

Customers' names, addresses, phone

2.9 MILLION

numbers, e-mail addresses - compromised.

800,000 Employees' names, dates of birth, Social Security numbers, addresses,

beginning and end dates of employment, emergency contacts - compromised.



incident.

that the investigation should remain confidential.

configure and install technical

architecture and tools to identify

affected servers and workstations.

Inspector General notifies the

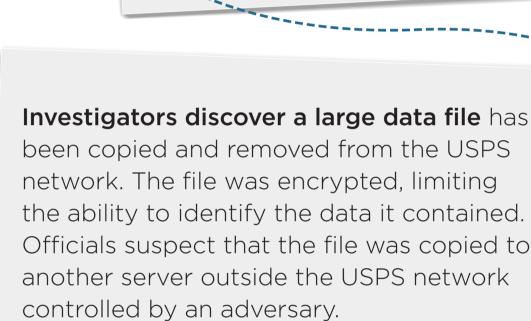
USPS about the breach. Days

later, IG advises the USPS CISO

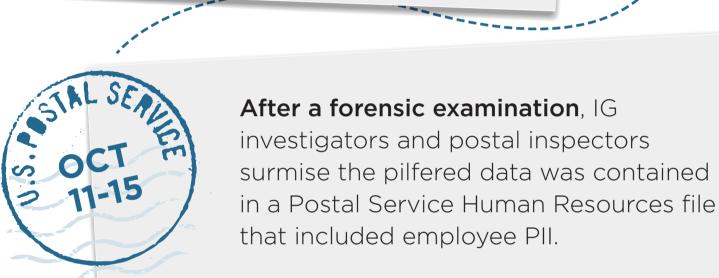
members of the CISO team meet

to develop steps to investigate











Service network.

Recovered employee PII

from the compromised server

was reconstructed and shared

with the USPS chief human

resources officer.

customer service requests.



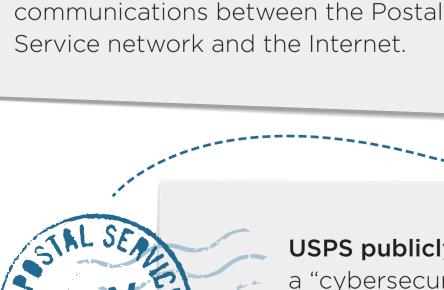
Implementing elements of the

remediation plan require a network

USPS confirms employee PII was

copied and stolen from the Postal





brownout, which limited

USPS publicly acknowledges a "cybersecurity intrusion" into some of its information systems.

The Postal Service CIO activates a

Continuing Action: USPS blocks employees' access to e-mail sites, such as Gmail and Yahoo, to reduce the likelihood of phishing and

spear-phishing attacks.

Source

View this infographic online

U.S. Postal Service

http://www.databreachtoday.com/us-postal-service-breach-timeline-a-7606