JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED EIGHTEENTH CONGRESS

JAMIE RASKIN, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
https://oversight.house.gov

Ranking Member Gerald E. Connolly
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
Joint Hearing on "Data Breach at the DC Health Exchange"
April 19, 2023

In 2022, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center received 800,944 phishing, personal data breach, and other complaints representing estimated losses of more than $10.2 billion, an increase of more than $3.3 billion from the previous year. As I stated during our last Subcommittee hearing, data breaches— including government data breaches—are no longer novel incidents.

In 2015, an OPM data breach exposed the private information of nearly 22 million individuals, including my own personal information. In 2019, the Russian Foreign Intelligence Service compromised SolarWinds software, which is widely used across the federal government. And in 2021, Microsoft reported that China's Ministry of State Security exploited vulnerabilities in their Exchange Servers.

Today, we are here to talk about the recent DC Health Link data breach which affected 56,415 individuals, including 17 Members of Congress and 43 of their family members, as well as 585 House staff and 231 of their family members. Despite DC Health Link's robust cybersecurity practices—including the use of leading commercial cybersecurity solutions, next generation firewall protections, and increased stress testing efforts—the organization remained vulnerable to attack.

According to the investigative findings to date, an undetected human error caused this breach. It was not underlying IT issues, legacy IT systems, or understaffing. A human error left the database vulnerable to unauthorized access. The breach demonstrates that even organizations with sophisticated cybersecurity practices must remain vigilant to potential risks, because one small oversight is the only window an opportunistic hacker needs to break in.

The breach also demonstrates that bad actors may not only hide in the dark web. Instead, in recent high-profile cases, stolen data has landed on easily-accessible public websites where the bad actor published the information to gain notoriety. Our cybersecurity posture must adapt to this new ecosystem.

Fortunately, law enforcement has been working aggressively to dismantle key players in the cybercrime ecosystem, including those associated with this breach. On March 15, the FBI took down the website BreachForums, the online hub of illicit activity used to expose the DC Health Link data and arrested its alleged founder.

While I acknowledge the DC Health Benefit Exchange Authority's commitment to protecting the data of their customers from another breach the fact of the matter is that the information of more than 56,000 people has been compromised already, putting their physical safety and financial security at risk. These individuals join hundreds of millions of Americans who have had their data stolen in the past year alone, and data breaches are only growing in scope. We need to move swiftly to implement the National Cyber Strategy examined in this subcommittee last month, which will drive important changes to better protect Americans' sensitive private data.

Throughout my career in the private sector and local and federal government, I have championed a trifecta cybersecurity strategy that encompasses modernizing IT systems, building a skilled federal cybersecurity workforce, and perhaps most importantly, fostering a security-centric culture at all levels of government.

One of the primary ways Congress can enforce this trifecta cybersecurity strategy is through consistent and sustained oversight of agency compliance with the Federal Information Technology Acquisition Reform Act, or FITARA, and our biannual FITARA Scorecard hearings. Through the Scorecard, we have promoted effective IT modernization by empowering agency Chief Information Officers (CIOs) and ensuring they have a seat and a voice at the decision-making table.

I am proud the Scorecard has secured big victories for the IT community by elevating CIOs within their agencies to ensure they are key players in fundamental conversations about agency mission execution. This focused oversight has raised the percentage of CIOs with a direct or partial reporting relationship to the agency head from just 50% to more than 90%. To build on this success, for the next Scorecard, we plan to ask agencies to self-report their CIO's control over IT spending and acquisition, in addition to the status of codifying their CIO reporting relationship.

We have evolved the Scorecard to include a robust cybersecurity metric to help protect against data breaches and other attacks. This change includes Inspector General assessments of agency cyber postures as well as agency implementation of government-wide cyber priorities and best practices. We are also exploring the possibility of a category that assesses agencies' IT workforce challenges, workforce gaps, and their ability to recruit, develop, and retain IT staff. Cybersecurity and IT modernization must be a priority for all federal employees, top to bottom. I look forward to our hearing later this summer to continue, along with Chairwoman Mace, this longstanding bipartisan commitment to federal IT oversight.

In today's hearing, we need to hear a strategy from the DC Health Benefit Exchange Authority to improve oversight and internal governance procedures. They must continue to act urgently to address remaining cybersecurity concerns, provide resources to breach victims, and instill the safeguards needed to prevent future breaches. I am also interested to hear how the Biden Administration's recent National Cyber Strategy might assist the Authority as it develops a resiliency plan. Lastly, this breach underscores the need for our Senate colleagues to confirm a National Cyber Director to lead the whole-of-government and whole-of-nation effort to the secure our digital infrastructure, protect the integrity and confidentiality of our data, and preserve trust in public institutions. I look forward to working with the Administration, Congressional colleagues, and other stakeholders to achieve these shared priorities.

###

Contact: Nelly Decker, Communications Director, (202) 226-5181