Phil Pasquini/Shutterstock

Trump has fired a major cyber security investigations body. It's a risky move

Published: January 23, 2025 6:45pm EST

Toby Murray, *The University of Melbourne*

Before the end of its first full day of operations, the new Trump administration gutted all advisory panels for the Department of Homeland Security. Among these was the well-respected Cyber Safety Review Board, or CSRB.

While this change hasn't received as much notice as Trump's massive announcement about AI, it has potentially significant implications for cyber security. The CSRB is an important source of information for governments and businesses trying to protect themselves from cyber threats.

This change also throws into doubt the board's current activities. These include an ongoing investigation into the Salt Typhoon cyber attacks which began as early as 2022 and are still keeping cyber defenders busy, attributed to hackers in China.

Salt Typhoon has been described as the "worst telecommunications hack" in US history. Among other activities, the hackers obtained call records data made by high-profile individuals and even the contents of phone calls and text messages. The phones of then presidential nominee Donald Trump were reportedly among those targeted.

What does the Cyber Safety Review Board do?

The board was established three years ago by the Biden administration. Roughly speaking, its job is the cyberspace equivalent of government air traffic investigation bodies such as the US National Transportation Safety Board, or the Australian Transport Safety Bureau.

The CSRB investigates major cyber security incidents. Its job is to determine their causes and recommend ways government and businesses can better protect themselves, including on how to prevent similar incidents in future.

Its members include global cyber security luminaries from industry, such as cyber executives from Google and Microsoft, and US government leaders from several departments and agencies concerned with security.

The US CSRB has previously published three major reports. Its first covered the infamous 2021 Log4j vulnerability, described at the time as the "single biggest, most critical vulnerability ever". (A vulnerability is a weakness in a computer system that cyber criminals can exploit.)

The board's most recent published investigation involved a very sophisticated hacking campaign that targeted Microsoft's cloud email services in 2023. As a result, hackers even gained access to the emails of various US government agencies.

Cyber security experts widely consider the CSRB as a positive thing. Late last year, Australia even committed to establish its own version, the Cyber Incident Review Board.

At the time of writing, it's unclear whether the CSRB will continue – perhaps with different membership –

or whether its activities will cease entirely.

Either way, the decision to fire the board's members has significant security implications. It comes at a moment in history when cyber threats have never been more severe.

What is Salt Typhoon?

The CSRB has been investigating the Salt Typhoon hacking campaign. Salt Typhoon is the name Microsoft assigned to a sophisticated group of hackers believed to be operated by China's Ministry of State Security. The ministry is somewhat like a combination of an intelligence agency and a secret police service.

Salt Typhoon is best known for hacking into several US telecommunication companies, first reported in August 2024. In December, it came to light Salt Typhoon's telco hacks may also have impacted countries beyond the US. American, Australian, Canadian and New Zealand authorities also jointly issued public guidance to organisations to help defend against Salt Typhoon.

Salt Typhoon reportedly targeted prominent figures, including political leaders. The hackers' goal appears to have been to collect intelligence, rather than cause damage.

For example, it has been reported Salt Typhoon collected a list of all phone calls made near Washington DC, which could help them determine who was talking to whom in the US capital.

Salt Typhoon also reportedly obtained a list of phone numbers wiretapped by the US Justice Department. This confirmed the fears of many people opposed to the government's powers to lawfully wiretap citizens' phones.

It is unclear why the hackers obtained that information. Some have speculated it would identify which of their own operatives were being monitored by US law enforcement.

To say the Salt Typhoon revelations created waves in government and cyber security circles is putting it mildly. Telecommunications are critical infrastructure, as well as highly valuable targets for intelligence collection.

The idea that foreign spies could burrow so deeply into the communication fabric of the US was unprecedented and disturbing.

In October 2024 the CSRB was tasked with investigating Salt Typhoon's activities.

Verizon was one of the telcos affected by Salt Typhoon attacks. Tada Images/Shutterstock

An uncertain future

With the board now fired, the future of the Salt Typhoon investigation remains unclear.

A thorough and impartial investigation of the Salt Typhoon hacks, had it been allowed to run, was likely to have delivered highly valuable cyber security lessons. Those lessons are important for both US companies and those in Australia, which have also been the targets of Chinese intelligence collection.

The future of the CSRB itself is now also in question. The board and its overseas equivalents serve a vital role in promoting cyber information-sharing that helps to improve best practices.

It is imperative these bodies are staffed with a diverse collection of impartial experts, able to carry out their work free from government and corporate interference.

It remains to be seen whether dissolving the current CSRB will be a gift to Chinese hackers (as some have claimed), or simply a speed bump in the evolution of the board.

- Cybersecurity
- Hackers
- Cyber safety
- Trump administration
- Cyberattacks
- Cyber crimes