CYBER SAFETY
REVIEW BOARD

2023 YEAR IN REVIEW

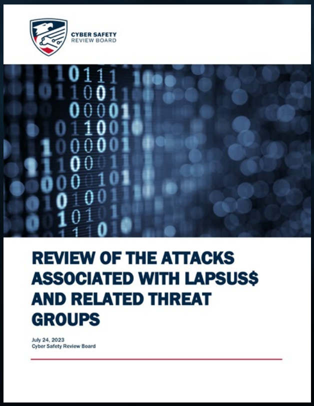
The U.S. Department of Homeland Security (DHS) established CSRB in February 2022, pursuant to Executive Order 14028, *Improving the Nation's Cybersecurity*. CSRB is an unprecedented public-private initiative that brings together government and industry leaders to identify lessons learned from significant incidents and to deliver strategic, actionable recommendations to enable advances in cybersecurity.

For more information, visit https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb

CSRB REVIEWS

August 2023: DHS publishes CSRB's second report on the hacks associated with the Lapsus$ group and related threat actors.

- Lapsus$ infiltrated victim networks and often used that access to infiltrate additional victim organizations. The groups were able to rely on relatively non-complex techniques like social engineering and bypassing weaker forms of multifactor authentication.
- CSRB's report serves as a playbook for responding to, and preventing, similar attacks through **10** actionable recommendations. The timeliness of CSRB's findings and recommendations was further reinforced by the September 2023 attacks on Caesars and MGM that leveraged similar techniques.


CYBER SAFETY
REVIEW BOARD

REVIEW OF THE ATTACKS ASSOCIATED WITH LAPSUS$ AND RELATED THREAT GROUPS

July 24, 2023
Cyber Safety Review Board

August 2023: DHS tasks the CSRB with reviewing the Microsoft Exchange Online intrusion publicized in July 2023, including the malicious access and use of cloud-based identity and authentication infrastructure. The final report is expected in early 2024.

IMPACT OF CSRB RECOMMENDATIONS

Lapsus$ Report

September 2023: The White House proposes requiring federal contractors to quickly report incidents to CISA and allow FBI access.

October 2023: CISA and NSA issue guidance addressing technology gaps limiting the adoption of secure authentication technologies.

November 2023: FCC adopts rules protecting consumers from SIM swap attacks, with Chairwoman Rosenworcel noting CSRB's recommendation that FCC "take action to support consumer privacy and cut off these scams."

Log4j Report

March 2023: The White House recommends shifting responsibility for insecure software products onto manufacturers and publishers.

September 2023: CISA releases a roadmap on secure use of open source software within the federal government.

December 2023: Cloudflare reports that Log4j remained a top target for attacks in 2023, validating CSRB's finding that the vulnerability would be endemic.

Extended Influence

March 2023: DHS submits a legislative proposal, supported by the Administration, to codify CSRB and grant it enhanced authorities. In today's evolving threat environment, CSRB's work ensures organizations can effectively protect government and private sector stakeholders.

November 2023: The Australian government announces the creation of a Cyber Incident Review Board modeled after CSRB.