Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Cybersecurity Concerns Related to the Recent Breach of U.S. Capitol Security

January 12, 2021

On January 6, 2021, individuals breached the U.S. Capitol security while a joint session of Congress met to certify the 2020 presidential election electoral votes. Upon illegally entering the Capitol, they entered and searched offices throughout the building. In the wake of this incident, experts in the cybersecurity community have been discussing issues related to how the event unfolded and what risks it raises to cybersecurity in its aftermath. Among those issues are:

- the role of social media platforms in enabling violent groups to organize and carry out their objectives, and the role of government in monitoring that speech;
- the use of public communications networks for alerting congressional building occupants; and
- the risk to information and technology from unauthorized and unscreened persons' access to the U.S. Capitol.

This Insight discusses these issues and summarizes concerns raised among the cybersecurity community. It does not discuss related issues, such as internet regulation, violent extremism, law enforcement responsibilities, or U.S. Capitol security.

The Role of the Internet

Cybersecurity experts have studied and warned of the use of social media to bolster the recruiting, indoctrination, training, and organization of extremist groups. The constitutionally protected right of free speech remains a significant aspect of the debate as policymakers seek to combat online extremism.

News media reports that the individuals who breached the U.S. Capitol security used websites and social media to organize that effort. In 2020 some private sector research firms were tracking this specific behavior online and reported on it.

While some cybersecurity experts cite advantages in leveraging social media for situational awareness and law enforcement purposes, others assert that social media facilitated the incident. Senator Mark

Congressional Research Service
https://crsreports.congress.gov
IN11572

CRS INSIGHT
Prepared for Members and
Committees of Congress

Warner has asked social media companies to preserve data posted during the event, raising competing issues of free speech and national security.

The incident on January 6 highlights some, but not all, of the issues surrounding this debate.

- What responsibilities do social media companies and web hosting providers have, or ought to have, to monitor their platforms for violent and/or extremist content and take action (e.g., remove that content or report the behavior to authorities)? The federal government previously debated limits on what may be posted and shared online and established the requirement for internet companies to report on child exploitation.
- What is the appropriateness and adequacy of federal agencies' open source intelligence collection and reporting coordination? Agencies have sought capabilities to monitor and collect information from social media platforms and websites. In doing so, some experts scrutinized the activity and wondered what systems or safeguards would be employed to prevent abuse.

Communications Systems

During emergencies, authorities rely on a variety of communications systems to alert people working in the U.S. Capitol complex. The U.S. Capitol Police used such a system on January 6, 2021. The distribution of these alerts rely on both internet-based (e.g., email and Wi-Fi networks) and cellular-based (e.g., SMS communications) systems to deliver messages. Concurrently, both occupants and individuals who breached Capitol security used social media to communicate their presence and status at the Capitol.

While the volume of communications indicate that systems worked as intended, lessons from January 6 could be used to inform future decisions on both the shared use and resiliency of these systems. Some issues concerning the use of communications systems include, but are not limited to, the following.

- What are the common communications plans for occupants and visitors to the U.S. Capitol complex and what fault tolerance (e.g., resiliency, redundancy, and graceful degradation) is in place to ensure information and communications systems are operable in an emergency?
- What capabilities do information technology (IT) security officials possess to filter or limit communications in an emergency and what are the protocols for employing such capabilities?

Physical Security of IT

One of the most widely discussed concerns are the risks introduced by the loss of physical security during the incident. News media report that offices were "ransacked" and laptops stolen. Cybersecurity experts warn that the loss of physical security increases the possible risk of lost data; corrupted devices; the introduction of unauthorized devices or applications; and compromised networks.

In response, the House Office of the Chief Administrative Officer issued a letter assuring users that the Office of Cybersecurity took steps to protect IT and that as of January 7, 2021, there is no evidence of a compromise. However, they also encouraged users to account for all IT devices and change passwords for potentially exposed equipment and accounts.

Cybersecurity experts identify physical security as foundational elements of cybersecurity. In the aftermath of the incident, and following incident response guidelines, IT teams will likely be conducting inventories, sweeps, and forensic analyses in an effort to identify and mitigate potential compromises. Policymakers may seek additional information about this response.

- How will IT teams ensure the security of devices or information already or potentially compromised?
- Do IT response teams have a plan to execute in this situation? If not, what lessons are being tracked and implemented if a similar response is needed in the future? Are IT teams resourced to implement these plans and any lessons learned?
- Do IT response teams have adequate resources to investigate and, if necessary, reconstitute IT systems and networks?
- If additional assistance is necessary from executive branch agencies, what protocols will be in place to protect the separated relationship between the executive and the legislative branches?
- Are IT administrators empowered to make changes, or are there barriers which require further debate?

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.