U.S. Capitol Security Issues – January 6, 2021

Our AI & Cybersecurity Newsletter typically covers topics such as ransomware attacks, exploits, security issues facing major companies such as Zoom, and security breaches such as the Solarwinds attacks on Nuclear Labs, the U.S. Treasury, and Pentagon. The common thread in all of these attacks is that they occur in the dark, so to speak. The malicious actors are identified after the fact, and often remain unknown. The hackers take data, disrupt services, and exploits, such as ransomware attacks on hospitals, cause us to ponder the very real risk of loss of life in the event of an attack on power grids or computer management systems integral to infrastructure.

The January 6 riot was the first time the U.S. Capitol was overrun by a hostile force since 1814 when the British set the White House and Capitol building on fire. In this case of the January 6 breach of U.S. Capitol security, all events occurred in the open, with many actors self-identified via social media posts and livestreams. Five people died as a consequence of the several hour takeover of the building, including a Capitol Police officer, Brian Sicknick, who was struck by a rioter in the head with a fire extinguisher. At least 56 officers were injured defending the Capitol.

Congress was in session at the time of the security breach. Legislators and staff were evacuated to secure locations. A group of rioters chanted "Hang Mike Pence" as they walked through the Capital. Others ransacked Speaker Nancy Pelosi's office and accessed her emails on a desktop computer. Senator Jeff Merkley reported his laptop was stolen. The Chief Administrative Officer's Office of Cybersecurity reportedly took actions to secure and protect sensitive information during the siege.

It is unclear what documents were removed from offices. Michael Sherwin, the acting U.S. attorney for Washington, D.C., said it will likely take "several days to flesh out exactly what happened, what was stolen, what wasn't," noting that "items, electronic items were stolen from senators' offices, documents and materials were stolen, and we have to identify what was done to mitigate that [damage]."

Some of the security issues related to the events of January 6 include:

Access to the Building – Rioters gained access to the building by force directly through entrances, using scaffolding to hoist themselves up a floor or two in order to break windows, scaling the building by turning metal barriers on their side and climbing them like ladders, and climbing walls without assistance.

Lack of Firewalls inside the Building; Secure Access Points – Rioters gained access all over the Capitol building including the Chambers and Member offices, created an opportunity to plant listening devices, bombs, damage sensitive documents, read/access sensitive documents

Ability to Bring Anything Inside – Items brought into the building included guns, weapons, tools, backpacks, cellphones, video cameras, zip ties, cigarettes and lighters. There was an opportunity to bring in anything inside, creating enhanced security risks including risk of fire. Social media posts referenced the desire to take hostages.

Ability to Take Anything Outside – Rioters stole a laptop and podium. They made recordings while in the building which may include sensitive information. They had the ability to take photos of all items in Member offices. Rioters has the opportunity to take documents, laptops, access computers in offices including email.

Communications – Throughout the siege, rioters had the ability to communicate with anyone, including each other, inside or outside the building, via cellphones and livestreams. They were able to access the internal telephone system. They accessed emails in Speaker Nancy Pelosi's office and could have sent harmful mass email communications. Rioters could have coordinated and mobilized other violence and riots at the U.S. Capitol and anywhere in the world.

Area around the Capitol was Not Secure- Presence of pipe bombs, napalm, molotav cocktails

Damaging Items – Ransacked offices, threw media equipment into a pile outside and tried to light it on fire

Capitol Police- There were photos and videos of Capitol Police moving barriers out of the way, motioning rioters to enter the building, and taking selfies with rioters. There are other photos and videos showing Capitol Police pushing back and punching rioters trying to move past barriers. Capitol Police Officer Brian Sicknick later died from injuries after a rioter hit him in the head with a fire extinguisher. Clearly, there were many officers fighting to protect the Capitol. There are questions regarding some members of the force and any effort to assist rioters.

Identifying Rioters Using Social Media (and Admissions)

The ability to identify people is hampered, at least to some degree, with people wearing masks out in public to avoid contracting COVID-19. However, most of the people who stormed the US Capital on Wednesday were not wearing masks. And, in fact, many of the rioters posted selfies during the hours they occupied the Capital. Some made phone calls to friends to announce they had successfully gained access and others livestreamed the attack, providing a play by play of their actions. Some spoke to the press, providing their names and home cities. Many posted their intent to go to the Capital on social media prior to January 6 and followed up with photos taken during the rally, inside the capital, and throughout the maylay. Many posted their intent to kill, including killing police officers.

Media equipment was destroyed, all while filmed by other rioters. A rioter urinated on the floor inside the Capitol and others smeared excrement. One person was easily identified by his work badge hanging around his neck and was promptly terminated by his employer for cause. Fortunately, staffers had the presence of mind to secure the electoral votes. One protestor was identified, via social media, by his proud father, announcing "THAT'S MY SON", followed up with a post stating that the FBI had contacted him, then the account went offline.

Items were stolen, such as a podium, which was promptly listed for sale on ebay, providing a second means of identifying the criminal.

Facial recognition software is often used by law enforcement to attempt to identify participants in criminal activity, but those efforts may be hampered by limited surveillance, limited photo vantages, clothing intentionally obscuring the person's identity, and inaccuracies in the software itself – in some cases, as we have written about previously, misidentifying the intended target. However, when the persons of interest self identify via social media platforms, tracking them, even across several state lines, becomes rather elementary.

Karen Heumann, G2M Communications, a re-grate-it brand