Threat Intelligence Report

Exposure of Personal Information Poses Increased Physical and Cybersecurity Threats to Election Officials in Lead-up to Presidential Elections

As professionals responsible for overseeing pre- and post-election administration, as well as proper and orderly voting at polling stations, U.S. election officials play a critical role in conducting and safeguarding electoral processes. However, election officials increasingly face threats and harassment, particularly surrounding major election cycles. A 2024 Brennan Center survey of 928 local election officials found that 38 percent experienced threats, harassment, or abuse in the course of their duties. This issue is significantly exacerbated by the exposure of election officials' personal information online, an alarming trend that almost certainly contributes to physical and cybersecurity threats.

THREAT ACTIVITY

Cyber-Enabled Threats to Physical Security

Numerous reports have documented instances of election officials facing physical harm or threats of violence, often enabled by online disclosure of personal information. Threat actors are known to intentionally, and without consent, publish the personal information of individuals for the purposes of harm, a phenomenon known as "doxing." Doxing, in turn, amplifies the risk of physical harm from threats like swatting, harassment, assault, and even pre-planned attacks.[1]

- In December 2023, Maine Secretary of State Shenna Bellows was doxed in a post on Doxbin, a paste site for doxing. The post provided extensive information on Bellows' family members, residence, e-mail addresses, and phone numbers. That same evening, Bellows was the victim of a swatting attack.
- In January 2024, Missouri's top election official was the victim of a swatting attack after an anonymous caller, impersonating the official, reported he was armed with an AR-15 and had just shot his wife. In August 2024, Michigan Secretary of State Jocelyn Benson said she was targeted in two swatting attacks in 48 hours. In some instances, individuals solicit swatting services on doxing sites in exchange for payment. Known as "swat-for-hire," these transactions frequently take place offline via private messages on end-to-end encrypted messaging platforms. Swatters use text-to-voice programs, some of which use artificial intelligence to mimic victim's voices, and virtual private networks (VPNs) to maintain anonymity when contacting law enforcement.
- Recent events have demonstrated that physical threats extend beyond individual instances of intimidation, harassment, and threats. Orchestrated violent attacks, involving both lone-wolf actors and organized groups, pose a threat to public officials. Perhaps the most notable example of such threats is the planned kidnapping of Michigan Governor Gretchen Whitmer. In 2020, law enforcement arrested 13 men for conspiring to kidnap the Governor from a vacation residence.

Figure 1 - Partially redacted excerpt of a now-deleted post on 'Doxbin' targeting Bellows. The post goes on to provide extensive information on Bellows' public calendar, resume, family members, and other addresses.

[1] Swatting involves falsely reporting an emergency, such as a bomb threat or hostage situation, that would initiate a large-scale police response at an individual's home.

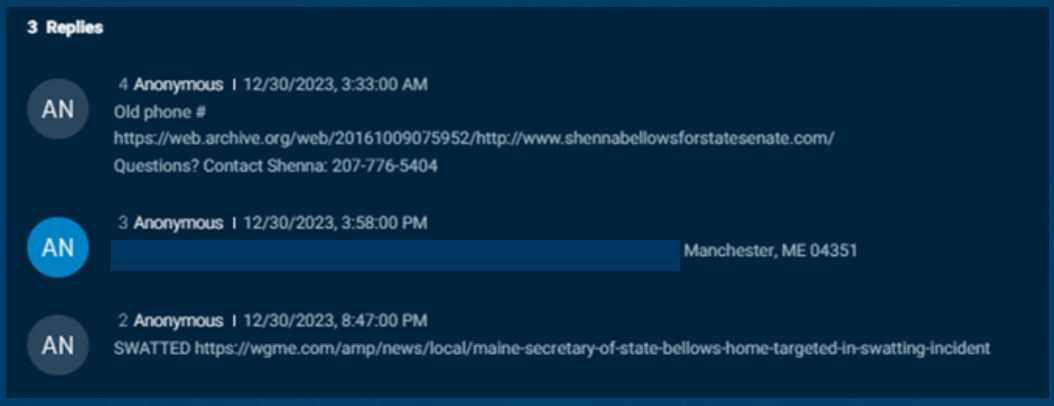

Figure 2 - Comments on the 'Doxbin' post from Figure 1 depict users contributing additional information on Bellows and sharing that she has been swatted.

Cyber Threats to Digital Security

The integrity of election administration hinges not just on the physical security of officials but also on the protection of their digital identities. The availability of personal information makes election officials prime targets for cyber attacks aimed at stealing sensitive data or compromising their accounts. Specifically, exposure of personal information increases officials' exposure to targeted cyber attacks, hack-and-leak operations, and online account takeovers, all of which can be used to discredit, undermine, or otherwise damage individuals and/or the electoral process itself.

- In a Private Industry Notification published in 2022, the Federal Bureau of Investigation (FBI) warned that cyber actors were targeting U.S. election officials with invoice-themed phishing emails designed to harvest officials' login credentials. According to the FBI, U.S. election officials in at least nine states received these emails within a short time period, suggesting a coordinated campaign.
- Hack-and-leak attacks have been prominent in election security discussions since the Democratic National Committee hack in 2016. As recently as this past summer, state-sponsored cyber actors used spearphishing emails to hack personal accounts of individuals belonging to a presidential campaign. The threat actors subsequently circulated confidential documents to members of the press, as well as opposing campaign staffers.
- In 2020, the Twitter/X accounts of several high-profile figures, including Joe Biden, Barack Obama, Elon Musk and others, were hacked as part of a cryptocurrency scam. The hackers posted tweets from these accounts promoting a Bitcoin scam. These types of attacks undermine public confidence in election officials and can be used to disseminate or perpetuate misinformation.

THREAT ASSESSMENT

FTI Cybersecurity assesses that election officials will face considerable threats and harassment leading up to and following the 2024 U.S. Presidential Election. This threat will almost certainly continue through the official certification of election results, and may persist beyond official certification if results are contested by either candidate. For this reason, election officials' personal information, including personal email addresses, phone numbers, home addresses, and the information of family members, should be considered highly sensitive data that could make election officials more vulnerable to physical threats if disclosed.

RECOMMENDED ACTIONS

- Establish robust data governance and Identity and Access Management (IAM) frameworks and solutions to safeguard sensitive personal information.
- Conduct regular deep and dark web assessments to evaluate personal information exposure online.
- Develop and stress-test an incident response plan that specifically addresses personal information exposure, doxing, and swatting scenarios to understand, plan, and practice potential responses ahead of time.
- Provide comprehensive security awareness training, including hands-on exercises and simulations, focused on social engineering, phishing, and personal cybersecurity best practices to equip stakeholders with the skills to identify, respond to, and effectively protect against cyber threats.

SOURCES

- Local Election Officials Survey — May 2024
- Criminal Compliant: United States District Court for the Western District of Michigan
- Maine elections official who removed Trump from primary ballot targeted in swatting incident, police say
- Election officials' homes 'swatted' as presidential race heats up
- Michigan Secretary of State Jocelyn Benson targeted in 'Swatting' attack
- Cyber Actors Target US Election Officials with Invoice-Themed Phishing Campaign to Harvest Credentials
- We received internal Trump documents from 'Robert.' Then the campaign confirmed it was hacked
- FBI says Iran sent hacked Trump info to Biden campaign staffers
- Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

AMERICAS

Atlanta
Boston
Chicago
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
San Francisco
São Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Düsseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com