Threat Intelligence Report

Cybersecurity Risks Throughout the Election Lifecycle

An estimated 40% of the world's population will participate in a national election this year. Ahead of the UK General Election in July and the U.S. Presidential Election in November, federal organizations, the private and public sectors, and citizens alike should be aware of the specific cybersecurity risks surrounding every phase of the election lifecycle. Election-linked cyber attacks are not without precedent. In the 2016 U.S. Presidential Election, for example, nation-state actors exploited known vulnerabilities in voter registration systems – and during the 2019 UK General Election, multiple Distributed Denial of Service (DDoS) attacks were attempted against the Labour Party. Similarly, 2024 global elections have already been subject to malicious cyber activity. Mitigating election security risks and minimizing potential impacts to election results requires understanding how and where risks can be introduced across all stages of election campaigns.

PRE-ELECTION CYBER RISKS

- **Phishing and Social Engineering:** Targeting political parties, candidates, and election officials to gain access to sensitive information.
- **Disinformation Campaigns:** Spreading false information to undermine trust in the election process.
- **Voter Registration System Attacks:** Tampering with voter registration databases to disenfranchise voters or collect voters' personal identifiable information (PII).
- **Database Breaches:** Unauthorized access to nomination databases to manipulate candidate information.
- **Ransomware Attacks:** Disrupting the nomination process by locking essential systems.

CAMPAIGN PERIOD CYBER RISKS

- **Website Defacements:** Attacks on candidate or party websites to spread false information or disrupt communications.
- **DDoS Attacks:** Overloading campaign websites or communication channels to disrupt campaign activities.
- **Social Media Manipulation:** Hijacking social media accounts to spread disinformation or malicious content.
- **Hack-and-Leak Campaigns:** Accessing and leaking embarrassing or otherwise damaging communications from a particular candidate or party.

ELECTION DAY CYBER RISKS

- **Electronic Voting Machine Hacks:** Manipulating the machines to alter vote counts (if applicable).
- **Network Attacks:** Targeting the communication networks used for transmitting election data (if applicable).
- **Ransomware Attacks:** Disrupting government systems on critical election days to sow distrust in the integrity of the voting process.

POST-ELECTION CYBER RISKS

- **Data Integrity Attacks:** Tampering with vote tallying systems to alter results.
- **DDoS Attacks:** Disrupting the systems used for reporting results to delay or manipulate the outcome.
- **False Result Announcements:** Compromising official communication channels to announce false results.
- **Transition Attacks:** Targeting the transition team with phishing or cyber attacks to gain access to sensitive information or disrupt the process.

RECOMMENDED ACTIONS

Individuals

- Be vigilant of election-themed phishing campaigns: do not click on links or download attachments from unknown senders.
- Verify the legitimacy of political party and voter registration solicitations before sharing personal information.

Public & Private Sector Organizations

- Conduct a cybersecurity gap assessment to understand system vulnerabilities and how to mitigate them.
- Continuously monitor networks and manage logs for unauthorized access and suspicious user behavior.
- Implement network segmentation and access management to ensure users only have access to necessary systems and data.
- Assess the security of third-party vendors who have access to organizational networks.
- Have a robust incident response plan in place that includes the defined roles and expectations of involved parties, including external vendors.

SOURCES

Sources include open-source information from public and private industry reporting.

- UK Parliament: Cyber Security of Elections
- CISA: Election Security Rumor vs. Reality
- NCSC Case Study: Defending our Democracy in a New Digital Age - At the Ballot Box and Beyond
- FBI: Russian Interference in 2016 U.S. Elections
- General Election 2019: Labour Party Hit by Second Cyber-Attack
- CISA: #Protect2024
- Securing Democracy: The Criticality of Physical and Digital Security

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	Los Angeles	San Francisco
Boston	Mexico City	Sao Paulo
Chicago	Miami	Seattle
Dallas	New York	Toronto
Houston	Philadelphia	Washington, DC
Irvine	Roseland	Wayne

EMEA

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

APAC

Brisbane	Perth	Sydney
Hong Kong	Shanghai	Tokyo
Melbourne	Singapore	

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI CONSULTING