New York State Election Incident Response Cyber Tabletop Exercise (TTX)

July 21, 23, & 24, 2020

Exercise Purpose:

Evaluate the incident response capabilities, processes, procedures, and coordinated communication flow of the 62 County Board of Elections in the State of New York.

Objectives:

1. Assess the State of New York's 62 County Board of Elections' cyber incident response and continuity of operations plans and identify areas needing improvement.
2. Discuss plans, policies, and procedures that guide incident response actions.
3. Increase awareness of organizational roles and responsibilities when coordinating incident response.
4. Assess the preparedness of state and local election officials to respond to and manage cybersecurity incidents.
5. Test preparedness and response of local election officials to weather-related incidents.

Contact

For questions or to learn more about the DHS Cybersecurity and Infrastructure Security Agency (CISA) Exercises, please contact:
CEP@hq.dhs.gov

Module 1

September 8, 2020
Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) release an alert regarding an increase in observed compromises to tablet operating systems (OS) for State, Local, Tribal, and Territorial entities with a new malware variant disguised as an OS update. The new variant spreads via phishing emails that updates users on a new critical OS update for their devices. The malware also bypasses signature-based security measures making it difficult for most anti-virus programs to detect.

September 14, 2020
The Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) releases an alert concerning an observed increase in attempts to affect the absentee ballot process and social media disinformation regarding absentee ballots. In addition, there is also misinformation about the worldwide COVID-19 Pandemic and how the virus will impact the general election in several states.

September 18, 2020
Many members of the New York State Election Commissioners Association (NYSECA) receive a series of emails with attachments from a colleague. The emails state that the attachments contain updated guidance regarding new procedures for teleworking during the COVID-19 quarantine. Wanting to learn more about the new guidance, some members open the attachment.

September 25, 2020
A hashtag begins trending on social media encouraging people to hold "parties" at various locations throughout the State on Election Day. The goal, according to social media, is to encourage voters to cast their ballot for the party's candidate Harvey Dent. Partygoers are instructed to display the Reformation logo prominently to "Show Reformation Strength." The hashtag #MakeTheVoteCount begins trending and is promoted on social media.

October 1, 2020
Although only a small number of elections officials are teleworking, many of these teleworkers are experiencing computer issues and are unable to complete tasks effectively. Some elections officials cannot log on to their computers. IT representatives are unable to resolve many of the issues remotely.

In addition, the Statewide Voter Registration database experiences significant lag during the day as updates made from the counties are being put into long queues. County and State elections offices experience difficulty accessing registration data and in some cases are unable to login into the State-Wide Voter Registration database.

October 3, 2020
Voters begin noticing significant changes on the State election websites. One election website claims that New York State will no longer allow in-person registration, and that the deadline for absentee registrations is October 27, 2020. Many voters call their County Board offices to ask why the State sanctioned this change. Election staff assure those who call that there has been no change to the process.

A county's election website is created with a .org domain from an unknown actor and being highlighted and advertised on popular search engines. The .org site directs voters to an invalid registration form request page. Although they appear to be legitimate, the State and County does not receive the data from those online registration forms.

October 20, 2020
A County Board of Election website crashes unexpectedly due to an increase in web traffic. This incident is receiving local and national media attention including "chirps" on social media from national news networks.

October 20, 2020
A County IT Department check of the database logs shows abnormal activity outside normal business hours that is inconsistent with routine data updates. The IT department is able to restore functionality of the websites within 2 hours but informs your leadership that should the site receive that amount of traffic again, the problem is likely to reoccur.

Discussion Questions

1. Would you receive the information presented in this scenario?
   - ★ a. Through what channels would this information be received and disseminated?
   - b. Are there established mechanisms to facilitate rapid information dissemination?
   - c. Is the information disseminated to the county level?
   - d. What actions do you take based on this information?
2. ★ What other sources of cybersecurity threat intelligence does your organization receive?
   - a. What cyber threat information is the most useful?
   - b. Is the information you receive timely and actionable?
   - c. Who is responsible for collecting and sharing information across your organization?
3. Does your department or agency provide basic cybersecurity and/or IT security awareness training to all users (including senior elections officials)?
4. Does your organization have cybersecurity awareness training program?
   - a. Do all users receive training (including senior elections officials?)
   - b. What does your training cover?
   - c. Is training required to obtain network access?
   - d. Are vendors required to complete cybersecurity awareness training?
   - e. How often is training required to be completed?
     - i. What happens if someone does not complete the training?
5. ★ How would your employees report suspected phishing attempts?
   - a. What actions do you take when suspicious emails are reported?
   - b. Are there formal plans or policies that would be followed?
   - c. Do you conduct phishing self-assessments?
6. Does your organization utilize multi-factor authentication to mitigate the potential effects of account compromise (e.g., something you know, something you have, something you are)?
7. Are there alternate methods of communicating to voters if the website information cannot be trusted?
8. How would your organization handle this invalid website?
9. ★ If your County discovered indicators of compromise or unusual activity such as that on October 20, what information, if any, would you be sharing?

Module 2:

October 25, 2020
On the second day of early voting, it becomes apparent that a large number of voters are not appearing in the e-pollbooks as expected. The early voting locations are now having to rely on compressed format pollbooks. This is causing long lines and is greatly increasing wait times.

October 30, 2020
Voters across the State complain to their respective counties that they have not yet received their absentee ballot, even though the election is 4 days away. Other voters, who received their ballots and mailed them in, now begin to wonder if their ballot was received and if it will be counted. Major newspaper outlets contact the New York State Board of Elections (NYSBoE) requesting a response.

Voters begin posting on social media questioning their confidence in the elections process. Media outlets are calling the County Board of Election offices in several counties asking for comment.

October 31, 2020
Several county election websites in New York have been defaced with an image of the hashtag #Rigged2020. IT staff are initially unable to access the sites to remove the defacement.

The affected County Managers are overwhelmed with media inquiries about the defacement and question the integrity of the elections.

November 2, 2020 10:35 a.m.
The National Weather Service releases a warning of a late season thunderstorm which could impact areas of New York.

November 2, 2020 2:45 p.m.
Local news stations have announced an update to the warning, citing this could be a dangerous storm producing straight line winds and is encouraging residents to seek shelter until the storm passes.

November 2, 2020 11:20 p.m.
After the storm passes, it is determined there is widespread power outages and road blockages across the State due to fallen trees. The high winds and fallen trees have also caused disruption to cell towers across certain areas of New York, causing an overload to the towers that are still functioning.

November 3, 2020
Reformation partygoers begin to surround several polling locations across the State. These parties of several citizens appear to be peaceful protests, with partygoers encouraging votes for the Reformation candidate. Some posts on social media begin to claim that members of the group are harassing citizens before they cast their votes and are disregarding social distancing guidelines. These posts are amplified by social media and start causing concern among voters.

A highly contested U.S. House of Representatives race in a rural district is being closely watched as the result may be determined by absentee ballots. State Board Elections officials notice the county's Election Night Reporting (ENR) website is displaying vote totals over 90% of the registered voters in their counties and alert the proper authorities.

State ENR website IT staff are able to identify unpatched vulnerabilities that may have been exploited to cause the issues.

November 16, 2020
When all absentee ballots have been counted, the NYSBoE Office notes that the total number is well below average and well below what was expected for a general election. State and local news stations and state-wide political groups begin to speculate as to the cause of the low numbers on their respective social media accounts.

Discussion Questions

1. How would your office handle the issues on October 25?
   a. What is the back-up procedure when e-pollbooks are not accurate?
   ★ b. How often are back up procedures or records updated/tested?
   c. How would you handle the accumulating line of voters due to the delay during this COVID-19 environment?
2. What processes do you have in place for replacing a ballot when a number of citizens report not receiving them?
   a. How many ballots does your office have the ability to replace without relying on outside assistance?
   ★ b. How would you respond to the media regarding the potential loss of mail in ballots a week prior to the election?
   c. What efforts are being made to restore voter confidence following the events on October 30?
3. Does your organization have tools or procedures in place for monitoring social media?
   a. How would your organization respond to the emerging news and social media issues?
   b. Who is responsible for responding to social media inquiries?
   c. Do you have pre-approved messages for immediate release as part of a larger communications plan?
   d. How long/how often is social media monitored?
4. How would your office handle the defacement of your elections websites?
   ★ a. If you were unable to restore the functionality of your websites, how would you ensure that voters are getting the correct information?
5. Does your office have personnel designated to address inquiries from the media?
   a. If yes, are other staff trained to refer media inquiries to the designated point of contact?
6. Does your office have existing procedures to run an election without power? How else would the storm and the damage it caused impact your election procedures?
7. How would your office respond to reports of voter intimidation by this Reformation party? Have you exercised response procedures with relevant local partners (e.g., law enforcement, etc.)?
8. Is there a process for handling issues that arise during ENR, such as those on November 3?
9. How would you determine whether unauthorized manipulation of mail-in ballots has occurred?
   a. What are the procedures for certifying an election in the State of New York?
   b. What would the State Board of Elections' reaction be to the low turnout?
   c. How would you address the speculation by the state-wide political groups in social media?
   ★ 10. What capabilities are needed to respond to this series of incidents?
   a. Are your internal resources sufficient to respond to this series of incidents?
   b. If not, what resources are available within the State or locally? How do you request those resources?
   c. How would you address the speculation by the state-wide political groups in social media?

Notes

Notes