Talking to the Public About Cybersecurity:

ELECTION SECURITY Exchange

PROACTIVE MESSAGES AND EFFECTIVE COMMUNICATIONS IN AN INCIDENT

Effective public communications about cybersecurity are imperative. The public reaction to any cyber incident may be amplified by existing, well-founded anxieties about cybersecurity. Proactive messaging about your protective measures can help address these concerns before they escalate. And preparing for an incident now will help you provide useful, reassuring messages if something should happen. Communication is a core election security function, not an afterthought: the goal of many attacks on election infrastructure is not to alter a result but to erode confidence in the process, and clear, trusted communication is often the most direct way to deny an adversary that objective. These are key tasks to help maintain public confidence in the integrity of elections.

Key Takeaways

- Develop your communication strategy around defined guiding principles, building templated responses for a general cyber incident and for common cyber threats, and considering who might play key roles in writing and delivering these messages.
- Highlight ongoing security measures and existing federal, state, and local partnerships as part of your proactive cybersecurity communications.
- Prepare in advance for effective, timely communications during a crisis.
- Communicate with voters about their role in cybersecurity, including seeking out trusted sources of information and reporting false or inaccurate information through proper channels.

Develop a General Communication Strategy and Templates in Advance

Consistent, transparent, and effective communication with the public during a cybersecurity incident requires advance planning. By defining core messaging, identifying common threats and vulnerabilities, and planning the timing and content of communications, you set the stage for success. Much of the damage from a cyberattack comes in the form of loss of confidence in the process. Use the tips below to develop a communications strategy that can help reduce that damage.

The work you do before an incident is what makes a fast, calm response possible during one. In the immediate aftermath of an incident, your team will be absorbed in response, and the information vacuum fills quickly. The preparation of materials and approved communication will allow you to communicate in minutes rather than hours, especially when timely communication matters.

Define a set of security principles that will structure your incident communications. These could include:

- **Containment -** that you're taking action to limit the impact of the cyber issue
- **Extent -** that you will rapidly determine what systems or how many voters are affected, and communicate that
- **Mitigation / Remediation -** that you are already taking steps to launch fallbacks or workarounds so that the public knows the services you provide will be available
- **Timing -** Be clear about what you know and what you do not know. Early in an incident, you may not have enough information to estimate how long a solution or remediation will take. Do not guess or offer speculative timelines. Instead, communicate that the team is actively working the issue and specify when the public can expect the next update. This approach maintains transparency without placing unnecessary or unrealistic pressure on the response team.
- **Accountability -** Use first person: "I apologize to voters for this happening. I am working with staff to fix it. The buck stops with me."

Create a general template, known as a holding statement, for a statement/press release on a cybersecurity incident, and individual templates for a few common cyber threats

- Use the principles outlined above.
- Consider the types of incidents you think may be most likely to occur in your jurisdiction, such as:
  - Phishing targeting your workers.
  - Website defacements or denial-of-service (DoS) attacks on voter registration or results sites.
  - Ransomware targeting election software.
  - Vulnerabilities involving network-connected hardware and software such as electronic poll books and results reporting software.
- Create a generic holding statement that can apply to any of the incidents you think might occur in your jurisdiction, recognizing that specifics to the type of incident will be inserted as appropriate at the right time.

Consider who may play key roles in writing and delivering security messages during an incident.

- Is there a communications professional in your office or from the county or city who can help hone your message during a crisis?
- Consider what messages you feel comfortable delivering and what audiences to speak to. Some messages may be best delivered through social media, a press release, or by a spokesperson.
- Some situations will be best addressed by a team:
  - » In a criminal cyber incident, speaking alongside a law enforcement partner helps underline the seriousness of your response.
  - » A vendor spokesperson may be better able to address technical aspects of a problem, and it may be appropriate for them to share the spotlight if their vulnerabilities or activity contributed to the incident.
- Consider obtaining advice from legal counsel, especially with respect to any potentially sensitive details concerning a potential incident. Legal resources may also provide valuable advice about retaining records that will be valuable post-incident, and can also assist you in working with representatives of your insurance provider if needed.
- If you have an election security working group, consider where your partners can take a lead or supporting role in message rollout, or whether they are positioned to amplify your messaging.

Develop a Communication Schedule for all phases of the election cycle.

- **Pre-election cycle -** this is your chance to educate the public on standard, ongoing security protocols such as endpoint protections, firewalls, and air gaps, as well as software penetration testing, equipment testing, and ongoing backups.
- **During the election cycle -** proactively address known threats such as phishing campaigns, doxxing, and ransomware. Showing you are aware of and responding to ongoing threats builds confidence.
- **Post-election -** describe the canvassing and post-election audit process to reassure voters about the integrity of the results.

Tactics for Proactive Cybersecurity Communications

The first steps toward effective public communication during a cyberattack or incident begin well before the incident takes place. Through proactive, ongoing outreach and education about your cybersecurity efforts, you can build confidence among voters, the media, candidates, and the general public that will pay dividends when an incident occurs. Using the tactics below, you can build a base of trust and confidence that allows you to start on solid ground when the stakes are highest.

Highlighting Ongoing Security Measures builds trust and confidence:

- Describe physical security protocols like tabulator seals, memory card storage, and chain of custody protocols that defend against cyber intrusion.
- Explain testing and certification processes for voting equipment that ensure industry-accepted safeguards against cyberattacks are in place.
- Detail cyberprotective measures managed by your team including firewalls, end-point protections, malicious domain blockers, and .gov domains.
- Describe the Logic and Accuracy testing process that verifies equipment is programmed accurately and performs without error.
- Highlight the role of non-internet-connected systems, such as vote tabulators, for critical functions.
- Highlight that the votes are cast and stored on paper (where possible)
- Emphasize the role of regular post-election audits to ensure the accuracy of results and the absence of malicious activity.

Describing Federal, State, and Local Partnerships: In the lead up to the election, communicate the ways in which you are working with any federal, state, local, or even private partners to monitor threat activity and develop plans for incident response. You can broadly describe your collaboration with federal agencies, like CISA and the FBI, state CISOs, fusion centers, cyber teams, National Guard cyber experts, and local law enforcement, without revealing potential operating gaps. This will build confidence that you have a team in place with the expertise to react quickly to a cyberattack and mitigate disruption to the election.

Review and refine any such communications with the partners involved before making them public. This will ensure you use an appropriate level of detail and that your messaging is consistent with that of those partners. Co-branded press releases or editorials can add even greater credibility to your communications.

Establish Defined Communication Channels for Regular Updates: Plan ahead how you will communicate - what methods you will use, at what times, for what purposes.
Some examples include:

- **Official election website -** maintain an ongoing informational page on your website describing cybersecurity protections you have in place, election official trainings, and any other ongoing mitigation efforts.
- **Social media platforms -** this is a perfect place to highlight how voters can play a role in cybersecurity by using trusted sources and reporting false or inaccurate information.
- **Local media -** cultivate trust and positive relationships with local media. Author an editorial on cybersecurity in elections and host a "media day" before the election to educate the press on routine processes and potential pain points.
- **Community meetings and town halls -** offer public awareness sessions to communicate directly with voters about election processes and security.

Crisis Communication and Incident Response

When a cyber incident or threat occurs, effective, transparent, and timely communication is essential. When there are gaps in information, the vacuum is filled very quickly - whether with malicious intent, innocent speculation, or false or inaccurate information. Consider the insights below to help ensure the public is kept accurately informed throughout the detection, response, and recovery phases of the incident:

Communication tactics for various stages of the incident:

- **Detection and Verification -** even as you are still gathering information and engaging in initial response and mitigation, coordinate with IT/security partners and begin communicating what you know:
  - Describe what is known and acknowledge what is not, including what steps are underway;
    - When facts are still developing, resist pressure to over-explain. A short statement keeps you credible without speculating. For example, "We take the security of this election seriously. We have identified an issue, engaged our partners, and are actively working to resolve it. We will share confirmed information and provide our next update by [time]."
  - When possible, confirm details and scope of the incident;
- **Response and Mitigation -** once mitigation is underway, begin describing the scope of impacts and any effects on the process:
  - Describe how affected systems have been isolated and that a recovery plan has been set in motion.
  - State that the incident has been contained and describe the key impacts on voters, if any, and how you are addressing those (e.g., replacement tabulators on the way, minimal wait time, potential for extended hours).

- **Recovery and Review -** when the incident has been resolved, continue communications to reassure the public and counter any false narratives surrounding impacts:
  - State that systems are restored and that post-incident review is ongoing.
  - Reassure the public of overall system integrity and assurance in results.

Other Tips/Tactics for Crisis Communications - no matter how well-prepared you are, crisis communication is always challenging. Consider the following strategies to ensure your communications are transparent, timely, and informative in the moment:

- **Create Pre-approved Holding Statements:** Boilerplate messages aid in rapid deployment of communications during an incident.
- **Weigh Transparency vs. Operational Security:** Coordinate with IT/cybersecurity teams to determine which information to share versus what to withhold to protect ongoing investigation, sensitive information, or systems. Build a review step for this analysis into your process before going public.
- **Prepare to provide information during an Incident:** Ensure rapid deployment of accurate information to counter false narratives. Consider means to assure the public that you are a trusted source by communicating only through verified channels, such as a .gov website, verified or official social media accounts, and messages carrying your office's name and seal. Reinforce these markers before an incident so voters already recognize them.

The Role of Voters in Cybersecurity

Although the primary responsibility for cybersecurity in elections lies with the election office and its IT team, voters have an important role to play. Part of an effective cybersecurity strategy includes regular communication with voters about what they can do to help protect our election systems from cyber compromise. Communicate with voters regularly throughout the election cycle about their role, including:

- **Promoting Trusted Sources:** Emphasize that voters should rely only on official sources for election information, for example:
  - The State Chief Election Official or the Election Division website
  - County, city, or other municipal government websites
  - Election websites such as voter information portals.
- **Providing Contact Information:** Provide the public with a mechanism to contact your office about false or inaccurate information.
- **Taking Care Before They Share:** Remind voters to step back and think twice before sharing rumors or allegations from unofficial sources.

- **Encouraging Secure Online Behavior:** Provide ongoing education to voters on using strong passwords and secure connections when accessing election services such as online registration updates or absentee ballot requests. Encourage voters to enable multi-factor authentication where election services offer it, and to be skeptical of unsolicited texts, emails, or calls about their registration or ballot status, which are common impersonation tactics. Remind them that your office will never ask for passwords, and they can confirm anything they receive by contacting you directly through your official channels.

Conclusion

When a cyberattack or incident occurs, how you communicate with the public can be just as important as your response and mitigation efforts. This communication starts before and continues during and after your response and recovery efforts. Implementing these strategies for cybersecurity communications above will help build public trust and confidence in the security, integrity, and accuracy of your elections.

Additional Resources

1. **Elections Cyber Incident Communications Plan Template**, Belfer Center, Defending Digital Democracy, 2018.
2. **Crisis Communications Intake Response Forms**, The Elections Group, September, 2025.
3. **Elections Infrastructure Incident Response Communications Guide**, CISA, October 2024.
4. **Enhancing Election Security Through Public Communications**, CISA, May 2024.
5. **Leading Cybersecurity Conversations with your County Team**, Partnership for Large Election Jurisdictions/Center for Tech and Civic Life/The Elections Group.
6. **Issue Guide on Post-Election Day Communications**, Partnership for Large Election Jurisdictions, November 2024.