Cyber Incident Response

A PRACTICAL PLAYBOOK FOR ELECTION OFFICIALS

ELECTION SECURITY Exchange

Election offices manage sensitive systems under close public attention, where even a minor cybersecurity incident can escalate into a broader crisis if it isn't handled carefully, affecting operations, creating legal obligations, and drawing attention that can undermine public confidence.

This guide provides a practical framework for responding to a potential cyber incident. It covers how to act immediately, coordinate, and communicate clearly under pressure.

Key Takeaways for Responding to an Incident

- Act quickly to contain the issue, but preserve evidence
- Coordinate internally before communicating externally (but don't delay unnecessarily)
- Assume information will be made public and plan accordingly
- Manage the information environment alongside the technical response
- Document decisions and actions in real time
- Alert legal counsel immediately; notification obligations may be time-sensitive
- If you have cybersecurity insurance, contact them after discussing with legal counsel

DEEPER DIVE

1. Introduction: Incidents in the Election Context

Few government functions are watched as closely as elections. Even a limited incident, whether a single affected system, compromise of a small set of data, or a quickly contained incident, can rapidly escalate beyond a technical issue. Incidents may disrupt operations, raise concerns about the chain of custody, and prompt immediate scrutiny from the public, media, and elected officials. In many cases, the mere perception of what may have occurred versus what actually occurred can have just as much impact as a successful attack.

This dynamic is not hypothetical. Election systems are closely watched and remain high-value targets, and even a contained or unsuccessful incident can cause harm. Reports of cyber incidents, whether they are confirmed, suspected, or misunderstood, spread quickly and can be weaponized to cast doubt on or raise questions about the election process. An IT problem can rapidly become a crisis of public trust.

Cyber incidents in election environments can take several forms, including unauthorized system access, data exposure (whether deliberate or accidental), system disruption or degradation, and manipulation of websites or public-facing information. These incidents are not always identified internally first. Often the first sign comes from outside, from a state agency, a vendor, a trusted partner, or a reporter. Offices differ widely in what they can detect on their own, and during initial response, the full picture is rarely fully understood.

The timing of an incident also shapes the response. Incidents that occur close to Election Day may limit available options, increase operational pressure, and garner more public attention. The same issue identified well before or after an election may allow for a more measured response. Election officials often must make decisions quickly, with limited information, while balancing operational priorities and public communication to ensure elections can continue.

This guide provides a practical framework to support that response. It focuses on the actions election officials can take to contain incidents, coordinate internally and externally, and communicate clearly under pressure. Throughout, it emphasizes that technical response and public trust considerations must be managed together, not sequentially.

2. Before an Incident: Preparation & Planning

Across the nation, election offices vary widely in size, resources, technical capacity, and even in how they conduct elections, as rules and procedures differ from state to state. At the same time, these challenges are not unique to elections. Election systems face the same persistent threats as every other sector. Even the largest and best-resourced organizations, such as finance, healthcare, and government, are regularly targeted, so no amount of preparation or single control makes any office immune. Effective response depends on building layered capabilities across people, processes, and systems that increase the likelihood of detecting issues early and responding quickly when they occur.

Recognize Your Capabilities and Plan Accordingly

Understanding your current environment is the starting point for an effective response.

- Identify the systems you rely on to conduct election operations
- Understand who manages those systems (internal staff vs. vendors)
- Assess available staff capacity and expertise
- Map key external relationships (state partners, vendors, IT support)

This does not require a comprehensive technical audit, but it should provide a clear picture of what you have and where you may rely on others.

Prepare for How a Cyber Incident May Be Identified

Not all incidents are detected internally. Sometimes someone outside your office notices it first.

- Anticipate receiving reports from state agencies, vendors, federal partners, researchers, or other third parties
- Establish a clear intake process for external notifications:
  - Who receives it?
  - How is it validated?
  - What's the threshold for triggering incident response plans?
  - How should it be escalated?

Planning for external notification reduces confusion and delays when information arrives unexpectedly.

Establish Your Incident Response Team in Advance

Response is more effective when roles and responsibilities are clearly defined before an incident occurs.

- Identify core roles across IT, leadership, legal, and communications
- Designate a lead responsible for coordinating response actions
- Clarify decision-making authority, especially for time-sensitive actions
- Ensure backups are identified and accessible if key personnel are unavailable

Even in smaller offices, clearly defined roles reduce delays and conflicting actions.

Build Relationships Before You Need Them

Many response actions and resource coordination depend on external partners.

- Establish contacts with state IT or CISO offices, fusion centers, the state's chief election official, federal partners, and key vendors and infrastructure providers.
- Identify law enforcement points of contact (e.g., state police, local FBI field office)
- Engage legal counsel familiar with election operations, relevant requirements, and potential cyber insurance requirements

> **Pre-established relationships enable faster coordination and clearer, more efficient communication during an incident.**
> **The Election Security Exchange has developed a practical guide on building and sustaining an election security working group convening trusted partners across physical, cyber, and operational security.**
> **The resource emphasizes collaboration, preparedness, and strong relationships to support incident response before, during, and after elections.**
>
> Resource: IT STARTS WITH A TEAM: BUILDING YOUR ELECTION SECURITY WORKING GROUP

Plan for Timing Variability

The timing of an incident affects both response options and potential impact.

- Consider how response priorities shift:
  - Well before an active voting period
  - Within 30 days of Election Day or around the close of voter registration
  - Within 72 hours of Election Day
  - On Election Day
  - Post-election, such as canvassing or certification windows
- Identify which actions may be limited or constrained in each scenario
- Plan for how communication expectations may change as Election Day approaches

Preparing for different timing scenarios helps reduce uncertainty when decisions must be made quickly.

Document and Test Your Preparedness

Preparedness should be documented and periodically tested.

- Maintain an inventory of systems, data, and key assets
- Ensure backups are regularly tested and stored offline in an encrypted format
- Keep contact lists current and accessible
- Conduct tabletop exercises (TTX), including scenarios where incidents are reported externally

Testing plans in advance helps identify gaps and improve coordination across teams.

3. Response Framework: What to Do & When

When a cyber incident is suspected or confirmed, election officials must act quickly, often with incomplete information and under heightened scrutiny. Response actions should prioritize containing the issue, preserving critical evidence, coordinating decision-making, restoring necessary operations, and preparing for external communication.

> ***Note:** these activities do not occur sequentially; they often happen in parallel and require clear coordination.*

Immediate Actions: Contain and Stabilize

The first priority is to limit the spread of the issue while preserving evidence needed to understand what occurred. Actions taken in the first moments of an incident can significantly affect both the investigation and the ability to recover.

Avoid shutting down affected systems unless necessary, as doing so may disrupt forensic analysis. At the same time, take steps to secure accounts and prevent further unauthorized access. You may also have legal obligations early on, especially if sensitive data or cyber insurance is involved.

Key Actions:

- Isolate affected systems (e.g., disconnect from the network) without powering them down unless required
- Secure accounts and reset credentials, prioritizing administrative access
- Preserve logs, system data, and other potential evidence
- Maintain the chain of custody for affected systems and data
- Confirm backups are secure and not connected to compromised systems
- Notify legal counsel early to assess potential reporting obligations

Active Incident Response: Coordinate and Manage

Once initial containment steps are underway, shift to structured incident management. Clear leadership and coordination are critical, especially as more information becomes available and decisions become more complex.

> **Election offices can benefit from following established incident management approaches, such as those outlined in the Federal Emergency Management Agency's National Incident Management System (NIMS), which emphasizes defined roles, clear leadership, and coordinated communication. NIMS is a core set of concepts, principles, and processes supporting all-hazards preparedness for emergency management and incident response.**

Key Actions:

- Designate a lead (e.g., incident coordinator or incident commander)
- Activate core teams across IT, leadership, legal, and communications
- Establish a regular coordination rhythm (e.g., scheduled check-ins)
- Begin and maintain an incident log documenting actions and decisions
- Ensure all participants understand roles and decision authority

Assess Impact: Understand Scope and Risk

As the response progresses, officials need a clearer picture of what is affected and what the consequences could be. This assessment informs both operational decisions and communication strategies.

Impact is not limited to technical systems. Even minor incidents or the perception of one can damage public trust, especially if they affect public-facing systems or involve sensitive data.

Key Actions:

- Identify affected systems and services
- Determine what data may have been accessed, exposed, or altered
- Assess operational impact (e.g., disruption to election processes)
- Assess reputational and public trust implications
- Consider election-specific risks (e.g., impact on voting vs. perception of integrity)
- Prioritize response actions based on election timing

External Notification and Reporting

Many incidents require coordination with external partners and may trigger legal or regulatory reporting obligations. These requirements vary, but reaching out early helps you meet them and keep the response coordinated.

Election officials should not wait until they have the complete picture to begin notifications, particularly when timelines are defined by law or policy.

Key Actions:

- Notify appropriate law enforcement and federal partners (e.g., CISA, FBI) as needed
- Coordinate with state authorities (e.g., chief election official, state IT/CISO offices, fusion centers, state police)
- Assess the applicability of state incident notification laws and voter data protections
- Engage vendors or third-party providers if their systems or services are involved
- Document all notifications and communications

4. Communications & Public Trust Management

Communication runs alongside the technical response from the start, not as a separate phase. Officials should assume that information about an incident will become public quickly, whether through external reporting, stakeholder awareness, or media inquiry. Establishing a clear, consistent approach to communication early helps reduce confusion internally and limits the risk of conflicting or inaccurate information being released.

> **In election environments, how information is shared, when it is shared, and how uncertainty is handled can directly shape public understanding and confidence. Even well-managed incidents can create confusion or distrust if communication is delayed, inconsistent, opaque, or overly speculative.**

Internal Communication

Effective response depends on everyone in the office sharing the same understanding. Staff should be informed that an issue is being addressed, while also being given clear guidance on how information should be handled.

Communication should prioritize consistency and clarity. Limiting speculation is critical, particularly in fast-moving situations where details are still emerging. Staff should understand what is known, what is not yet confirmed, and where to direct questions or external inquiries. Establishing a single point of coordination for internal updates can help prevent miscommunication and ensure alignment across teams.

External Communication

Decisions about external communication should balance the need for transparency with the reality of incomplete information and sensitive details. Waiting for full clarity before communicating can create a gap that is filled by speculation or inaccurate reporting. At the same time, premature or overly detailed statements can introduce confusion or require later correction, which in turn can stoke distrust.

In many cases, issuing a brief initial statement acknowledging that an issue is under review can help establish control of the narrative. These "holding statements" should be factual, limited to confirmed information, and clear about what is still being assessed. As more information becomes available, updates should be provided in a consistent and measured way.

> **The Election Security Exchange has created a brief guide with practical strategies to help election officials respond quickly, coordinate messaging, and share clear, accurate information with the public. Election incidents are inevitable, and how you communicate in those moments is critical.**
>
> Resource: COMMUNICATING DURING AN ELECTION INCIDENT

Managing Inaccurate and False Information

Incidents affecting election systems are likely to be interpreted, shared, and sometimes misrepresented in ways that extend beyond or ignore the facts of the situation. Officials should anticipate how an incident could be framed or misunderstood and plan communication accordingly.

Providing clear, factual information early helps establish a baseline understanding before narratives take hold. Monitoring for inaccurate or misleading claims can help inform response, but engagement should be measured. Correcting false information should focus on reinforcing accurate facts, rather than amplifying or repeating incorrect claims.

> **The period between initial awareness of an incident and official communication is often when false or misleading information emerges and spreads.**

Stakeholder Coordination

Communication during an incident rarely occurs in isolation. Election offices often need to coordinate messaging with state authorities, federal partners, law enforcement, and vendors. Misalignment across these groups can create confusion and reduce credibility.

Where possible, officials should align on key messages, timing of communications, and roles in public engagement. Coordination does not require identical messaging, but it should avoid contradictions or gaps. Early communication with partners helps ensure that information shared publicly is accurate, consistent, and reflects a common understanding of the situation.

5. Recovery & Continuity

Recovery is not simply about restoring systems. It is about restoring operations in a way that is secure, reliable, and credible. Before recovery begins, you need confidence that the threat actor has been fully contained and eradicated. Moving to restore systems while an adversary still has a foothold can reintroduce the very compromise you are trying to recover from. In addition, moving too quickly to bring systems back online without validating their integrity can reintroduce risk or create additional uncertainty. At the same time, election offices may need to continue operating under time constraints, particularly when incidents occur close to key deadlines or Election Day.

The focus during this phase is to restore essential functions safely while maintaining continuity of operations. This may require a phased approach, where systems are brought back online in stages after they have been verified as secure. Where restoration is delayed or not immediately possible, contingency plans should be activated to ensure that election processes can continue.

Key Actions:

- Restore systems from clean, verified backups
- Validate system integrity before returning to normal operations
- Prioritize critical systems that support election functions
- Shift to contingency operations if needed (e.g., backup processes, manual workarounds)
- Continue coordination with state partners, vendors, and technical support as systems are restored

Communication remains important during recovery. Officials should provide clear, factual updates on what has been restored, what remains under review, and how operations are being maintained. This helps reinforce confidence and reduces uncertainty as systems return to normal.

Recovery efforts should also be documented as part of the broader incident record. This documentation supports transparency, enables post-incident review, and may be necessary for legal, regulatory, or public reporting purposes.

6. Post-Incident Review

The conclusion of an incident does not mark the end of the work. A structured post-incident review is critical to understanding what occurred, identifying gaps, and strengthening future preparedness. Without this step, the same vulnerabilities that led to the incident, whether technical or procedural, may persist.

This review should be conducted once systems are stabilized and immediate pressures have eased. It should bring together relevant participants across technical, operational, legal, and communications functions to develop a shared understanding of the incident and the response.

Key Actions:

- Conduct an after-action review with key stakeholders involved in the response
- Identify root causes, including technical vulnerabilities, human factors, and process gaps
- Assess what worked well and where coordination or decision-making broke down
- Capture lessons learned in a clear, actionable format
- Update incident response plans, protocols, and training based on findings

The goal is to improve resilience, not to assign blame. Findings should inform both immediate adjustments and longer-term investments in systems, staffing, and partnerships.

Where appropriate, insights from the incident should feed into future training and exercises so lessons learned carry into your ongoing preparedness.

Tools & Templates

- **Department of Homeland Security:** Incident Handling Overview for Election Officials
- **The Election Security Exchange:** Toolkit: Election Incident Reporting
- **CISA:** Enhancing Election Security through Public Communications
- **Belfer Center for Science and International Affairs:** Election Cyber Incident Communications Plan Template
- **The Elections Group:** Crisis Communications Intake Response Form