Elections Cybersecurity White Paper:
Incident Lifecycle and Incident Response Management Planning

Rahul K. Patel, PhD
Elections Information Security Officer
Office of the Cook County Clerk and Chicago Board of Election Commissioners
Chicago, IL USA

Tonya Rice, J.D.
Director of Elections
Office of the Cook County Clerk
Chicago, IL USA

ABSTRACT

In the past few years, the volume, types, and quality of cybersecurity-related attacks in elections have become more damaging and disruptive, and new types of security-related incidents have emerged. This white paper describes the best-known method for analyzing the stages of cybersecurity incidents and identifies actions that can be taken to avoid or minimize impacts at each incident lifecycle stage. We discuss the overarching workflow for elections security incident response and management and describe the Point and Line analysis approach, which considers factors such as attack vectors, motives, probability, and impact to develop a set of Incident Response Templates in this paper. In addition, we include reusable templates for analyzing cybersecurity Incident Lifecyle and Incident Response Management, which can be customized for specific needs of any election jurisdiction in this paper.

THE PROBLEM

Incident response management has become a critical part of elections security. A cyber incident can span a wide spectrum of malicious cyber activity, and for the elections system, it could range from theft of voter registration data to disruption or manipulation of the vote tally (Gorman, Cortez, & Belfer Center, 2018). The volume, types, and quality of cybersecurity-related attacks have become more damaging and disruptive (Cichonski, Millar, Grance, Kent, & NIST, 2013). New types of security-related incidents emerge frequently. As a result, election officials and information security professionals must find effective ways to decrease response times and recovery times, and limit costs. Effective incident management can prevent incidents by accurately identifying potential attack vectors from the perspective of a hacker, and efficiently detecting vulnerabilities in the systems before incidents occur. Rapid incident response can minimize the potential damage and destruction to election infrastructure and voter confidence. It can also help mitigate weaknesses and help officials restore normal operations more quickly.

This white paper provides the best-known method (BKM) for incident management planning, handling, and analysis of incident stages, and determining the appropriate response to each incident. The Office of the Cook County Clerk and the Chicago Board of Election Commissioners successfully developed and implemented these tools to strengthen their cybersecurity protocols. However, the BKM can be further customized or localized autonomously for specific environments or boundaries in elections, or other government agencies.

THE APPROACH

Incident Stage Analysis and Swift Response

To implement swift incident response processes, it is first necessary to analyze the progressive stages of a cybersecurity incident, and design and implement measures in each stage effectively. When an incident occurs, it takes time to pass thru each stage of the lifecycle. The expanded stages of the incident lifecycle explore these factors, as detailed in the following five analytical categories (Figure 1):

(1) Detect: reporting of the incident;

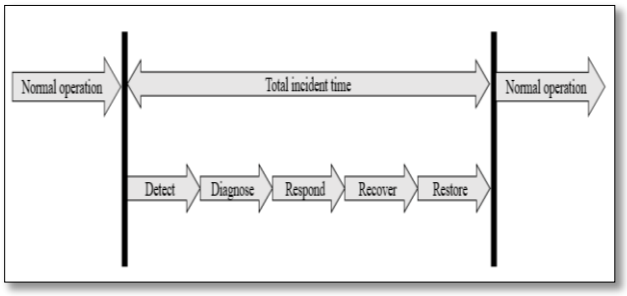
(2) Diagnose: identifying the cause and effects of the incident;

(3) Respond: planning for and implementing the measures in advance and in real time;

(4) Recover: planning appropriate steps and time to recuperate from a security incident by successfully deployed response; and

(5) Restore: fully re-establish the normal working operations of the services that experienced the cybersecurity incident.

Figure 1: Stages of a Cybersecurity Incident



Detection: Detection of an incident occurs when the incident is reported to security operations by various means (Nieles, Dempsey, Pillitteri, & NIST, 2017). This detection can be through monitoring tools, event management systems, or through a user. Ideally, every incident would be detected automatically. In this stage, the time spent by the response team or tools are only to detect the incident and the response process has not been started. Hence, detection needs to be very fast and accurate. In several cases where there is high confidence level detection, an automated response may be possible for the incident.

Diagnose: Effectively determining the cause and effect of an incident takes time. Knowledge generated at this stage must be reused to reduce diagnose time in the future for similar causes and/or effects. The time spent on this stage of the incident can be reduced with readily available scripts and tools to assist with the diagnoses and incident management process. While diagnostic activities may take a great deal of time, resilience and redundant systems and connectivity can ensure that the service is still operational even though some part of it may have failed.

Response: Responding to an incident involves many different activities that can only be partially defined prior to an incident occurring. For anticipated causes, attack vectors, and effects, responses can be designed and drafted in advance so that they can be performed as quickly as possible. This includes designing response techniques into a service and incident response processes. Preventive measures such as fail-over and fault-tolerance capabilities can be implemented in advance to eliminate or reduce the severity of the incident.

Recover: Recover involves bringing the service back to an operational state (Nieles et al., 2017). However, it may not be at a usable state yet. This may involve ensuring that all components of the service are free of incident effects, operating as expected, and that the cybersecurity incident has been truly resolved but data may not have been restored fully yet and utilization level of the service that experienced the security incident may not be at the pre-incident stage yet.

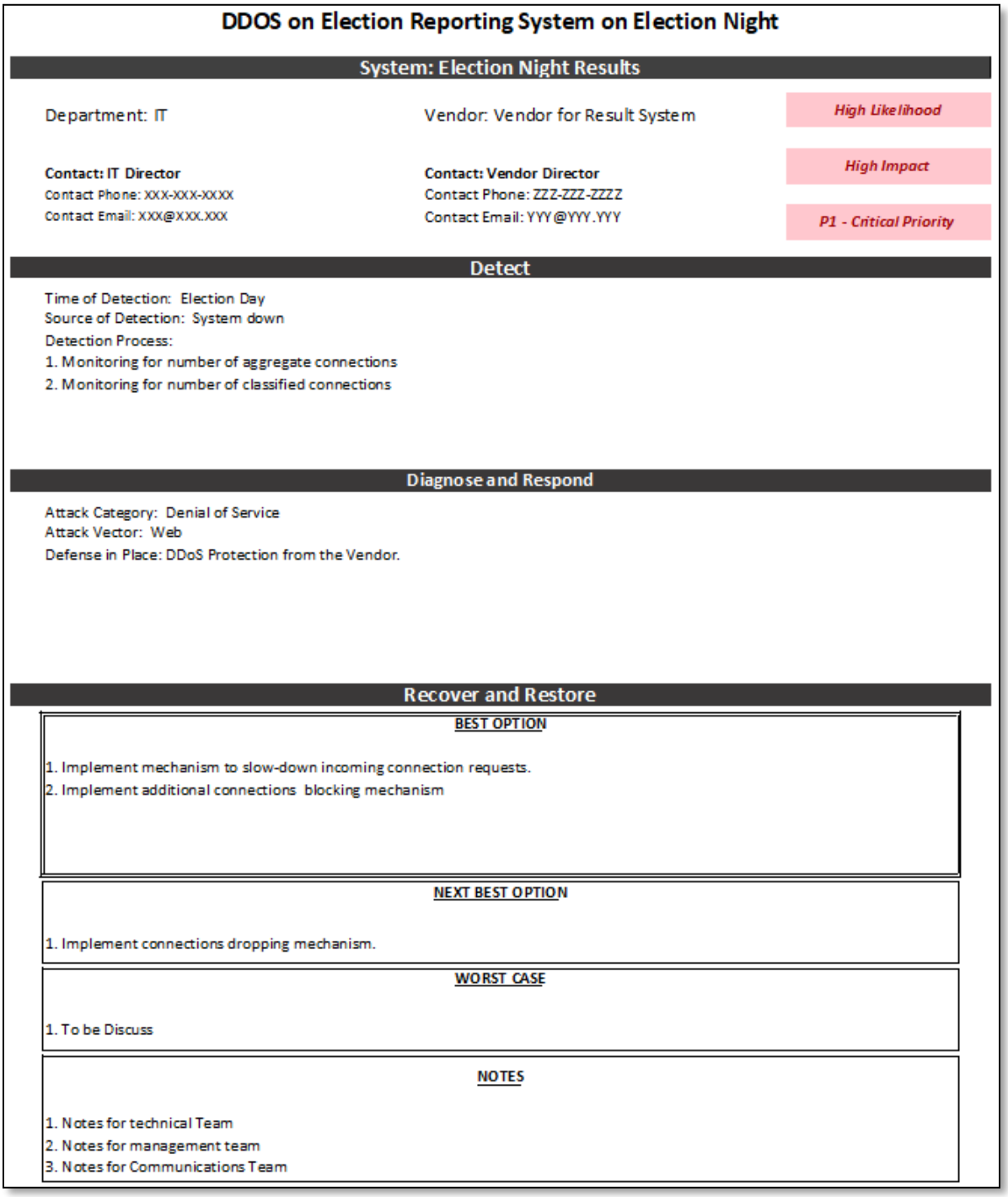
Restore: Restoration involves bringing a service back to its fully usable state (Nieles et al., 2017). After recovery, there are times when data may need to be restored to ensure that users can continue to use the service as they did prior to the incident occurring. At this stage, even though the system may have been fully restored, it may still take time for all users and processes to return gradually to the pre-incident level.

THE SOLUTION

Incident Response Scenarios &Templates

Effectively performing incident response is a complex undertaking for any election organization. Establishing a successful incident response capability requires substantial planning and the optimized use of available resources. Establishing clear procedures for prioritizing the handling of security incidents is critical to overall elections operations. It is also essential to build relationships and establish suitable means of communication with other internal groups (e.g., communications team, human resources, legal) and with external groups (e.g., Vendors, the public, customers, and other incident response teams, law enforcement) (Gorman et al., 2018). Having, pre-built workflows in the form of response templates makes incident handling fast, consistent, and effective. The following template (Figure 2) was developed considering many factors including systems and connectivity with their classification, attack vectors, attack channels, incident effects, priority, defense in place, detection mechanism in place, recover and restore steps.

Figure 2: Cybersecurity Incident Response Scenario Template



DDOS on Election Reporting System on Election Night

System: Election Night Results

Department: IT

Vendor: Vendor for Result System

High Likelihood

High Impact

P1 - Critical Priority

Contact: IT Director
Contact Phone: XXX-XXX-XXXX
Contact Email: XXX@XXX.XXX

Contact: Vendor Director
Contact Phone: ZZZ-ZZZ-ZZZZ
Contact Email: YYY@YYY.YYY

Detect

Time of Detection: Election Day
Source of Detection: System down
Detection Process:
1. Monitoring for number of aggregate connections
2. Monitoring for number of classified connections

Diagnose and Respond

Attack Category: Denial of Service
Attack Vector: Web
Defense in Place: DDoS Protection from the Vendor.

Recover and Restore

BEST OPTION

1. Implement mechanism to slow-down incoming connection requests.
2. Implement additional connections blocking mechanism

NEXT BEST OPTION

1. Implement connections dropping mechanism.

WORST CASE

1. To be Discuss

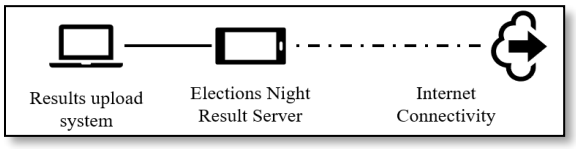
NOTES

1. Notes for technical Team
2. Notes for management team
3. Notes for Communications Team

Point and Line Analysis: Response templates need to be developed for all known possible combinations of security incidents with the help of security experts, technical support groups, system owners, users, communication experts, vendors, management, and various stakeholders. A Point and Line analysis technique can be used to determine the number of possible incident scenarios. For example, in a sample Election Night Reporting system shown in figure 3, there are two systems (points) with two connectivity

type (line) under organizational control, resulting overall 4 possible attack surfaces. In addition, there could be 7 possible attack vectors; external / removable media or system, attrition / brute force, web, email, improper usage, loss or theft of equipment, and any other attack vector (Cichonski at el., 2013). Furthermore, effect could be breach of confidentiality, integrity, or availability (Nieles et al., 2017). Considering only these factors, the number of scenarios can be determined as follows:

Figure 3: Election Night Reporting



Number of Incident scenarios templates = Total systems (4) X Attack Vectors (7) X Effects (3) = 84

After analyzing all scenarios, it might be possible that some of the scenarios would have similar or the same response steps. In such cases templates can be collapsed/combined to create smaller operational set of templates. It is likely that the operational set of procedures would be very large in number and hence the format for the template should have keywords, filters, sort, and search capabilities. Most modern knowledge management systems have such capabilities. It can be a very time-consuming task at first and hence efforts at developing incident scenario response templates should be divided among system owners, support personals, information security experts.

Incident Response and Management Plan

For consistent communication and incident management, an overarching Incident Response and Communication Plan must be developed and implemented (Gorman, Cortez, & Belfer Center for Science and International Affairs, 2018). At a minimum, such Plan should have the following components.

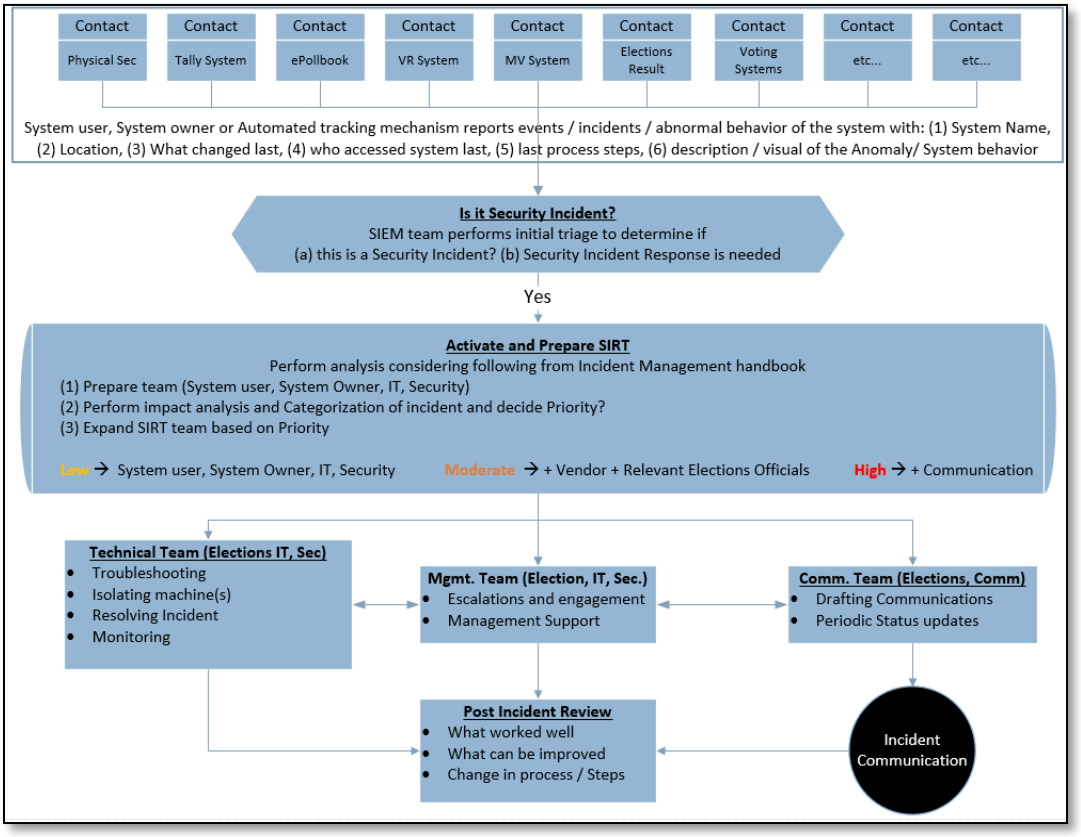
1. *Incident detection mechanism:* A coherent system for establishing reliable facts and ways to stay informed must be developed (EI-ISAC, 2019). Security incidents could be reported manually by a system user or system owner, or it could be automated by monitoring signatures, abnormal system events or abnormal behavior of the system. Basic information regarding the incident including system name, location, recent changes, recent users, recent activities and description / visual of the anomaly/ system behavior must be captured for analysis.
2. *Initial triage:* Based on available information related to the incident, the security incident and response management team must perform the initial triage to determine (a) whether this is a Security Incident, and (b) whether a Security Incident Response is needed.
3. *Impact Analysis:* The Incident Scenario Templates can be aggregated into a local handbook, which is kept ready for a team to perform the analysis for any given incident. At regular stages, the team, including the system user, system owner, IT, and security experts, prepare for incidents by reviewing best practices in the handbook. The team then performs impact analysis and categorization of any incident and decides priority. As needed, expand the Security Incident and Response Team (SIRT) based on priority. At escalated priority levels, specific subject matter experts (SMEs), Vendors, Management, Legal, and Communication teams should be engaged.

During an incident, typically three types of teams work in coordinated fashion to address different aspects of the incident. The Technical Team (Elections, IT and Security) handles technical aspects of the incident response including troubleshooting, localizing the incident by isolating machine(s), and implementing the identified solution to resolve, recover and post incident monitoring. The Technical Team also provides expertise and capacity in responding to incidents. The Technical Team's efforts are focused on finding the root cause of an incident by searching for tactics, techniques, and procedures, along with behaviors and associated artifacts (DHS, 2019).

The Management Team (Elections Administration, IT, and Security) handles executive decisions, escalations, consultations with vendors or stakeholders, and any other additional administrative support and resources required during the incident. Finally, the Communications Team handles the coordination of public information and related activities including message development, drafting, press releases, coordinating with media, and periodic status updates to internal and external stakeholders (EI-ISAC, 2019).

In addition, after completion of the recovery efforts, all teams should collectively perform a Post Incident Review to discuss what worked well, what can be improved, and whether any changes are needed in the process. Any additional need for tuning the processes or tools for preventing or more effectively detecting such incidents are also discussed in the Post Incident Reviews. The overall goal should be to avoid incidents with preventive measures and fine tune the incident management processes to minimize damage and increase effectiveness.

Figure 4: Cybersecurity Incident Response Process Template



SUMMARY

The Cook County Clerk's Office and Chicago Board of Elections Commissioners have implemented an internally developed Incident Response and Management process based on NIST, EI-ISAC, and Harvard Belfer Center's recommendations. This multi-faced approach benefits election jurisdictions by providing consistent and systematic processes for identifying and prioritizing incident response with pre-designed scenario templates to avoid ambiguity in security incident response efforts. It also helps generate awareness among the entire elections staff and all system owners, and it can practically act as a tabletop exercise while identifying and developing incident scenario templates. The process provides a clear picture of preventive and detective measures and possible gaps so it can be addressed proactively. The process also provides an effective means of consistent and timely communication regarding cybersecurity incidents. In addition to providing improved internal protocols, the public may gain external confidence through the knowledge that elections officials and information security professionals are utilizing well-developed cybersecurity incident response plans.

REFERENCES

1. Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). (2019). Elections Resources. https://www.cisecurity.org/wp-content/uploads/2018/05/EI-ISAC-Checklist-Final.pdf
2. The Department of Homeland Security (2019). Incident Handling Overview for Election Officials. https://www.dhs.gov/publication/election-security-resource-library
3. Gorman, S., Cortez S., & Belfer Center for Science and International Affairs (2018). *Election Cyber Incident Communications Plan Template for State and Local Officials.* https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template
4. Nieles, M., Dempsey, K., Pillitteri, V. Y., & Information Technology Laboratory (National Institute of Standards and Technology). (2017). *An introduction to information security.* doi: 10.6028/NIST.SP.800-12r1
5. Cichonski, P., Millar, T., Grance, T., Kent, K., & National Institute of Standards and Technology (U.S.). (2013). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology.* doi: 10.6028/NIST.SP.800-61r2

AUTHORS

Rahul K. Patel
Elections Information Security Officer, Cook County and Chicago Board of Elections Commissioners, Illinois.

Rahul Patel is a seasoned Cyber / Information Security professional with over 25 years of experience defending the Availability, Confidentiality, and Integrity of information assets. He is leading Elections information security and risk management efforts at the office of the Cook County Clerk and Chicago Board of Elections Commissioners as an Elections Information Security Officer. Patel holds a PhD from the Northcentral University, M.B.A. from the DePaul University, and M.S. from the Illinois Institute of Technology.

Tonya Rice
Director of Elections, Cook County, Illinois.

Tonya Rice was appointed Director of Elections by Cook County Clerk Karen A. Yarbrough in 2019. Rice leads operations for one of the largest election jurisdictions in the country and currently serves on the Bipartisan Policy Center's national Elections Task Force. Rice was a National Science Foundation Graduate Research Fellow at the University of Michigan. She is a Certified Elections Registration Administrator (CERA). Rice holds a J.D. from Northwestern University School of Law, and B.A. from Northwestern University.