DRAFT County Cyber Security Response Briefing

SEPTEMBER 2021
Executive Summary

If it hasn’t happened yet, it could happen at any time.

The county’s IT systems have been hacked and infiltrated, and now your information systems have been compromised and/or data that you are responsibility for keeping safe is being held ransom. What do you do now?

This Primer is designed as a high-level roadmap, from the 40,000 foot perspective, that can be used to help build our your county’s executive response plan or to evaluate and update your existing plan. Also provided is a model incident response plan, tracking & report template and flowchart. These are not designed to replace any plan created by your IT department, or your county board of elections, but to supplement either or both of them.

Once you develop your plan, test the plan using realistic simulations, where roles and responsibilities are assigned to the people who manage cyber incident responses. This ensures that your plan is effective and that you have the appropriate people involved in the plan. Use your incident response plan, along with your disaster recovery and business continuity plans, to minimize impacts to your operations and efficiently recover critical systems.

The Primer is broken down into five components: safeguarding your systems, activating your response team, securing your information systems, deploying your continuity of operations plan, and implementing your crisis communication strategy. Many of the tasks under each of these components of your response can and should happen simultaneously to keep the county running as smoothly as possible during a cyber security emergency.

Part I

Proactively Safeguarding Your County and Systems

Before a cyber attack happens, there are actions that your county can take to proactively safeguard your information systems and plan for the increasingly inevitable attempts at infiltrating your IT assets. This checklist can serve as a starting point for your management, policy and IT teams to lay the groundwork for protecting your county’s IT infrastructure.

☑ Inventory your agency’s databases and identify the high priority information (see County Datasets)

☑ Assess the risk and potential consequences of having this information compromised

☑ Review who has access to this information and whether the information is classified properly

☑ Regularly update system authorizations and control the use of administrative privileges

☑ Deploy multi factor authorization for access to email and all other critical systems, particularly when that access is remote

☑ Remind all staff “When you see something, say something.” Report any anomalies to the county’s cyber security response team on an ongoing basis

☑ Identify who should be on your County’s cyber incident response team (see County Cyber Response Team and attached IR plan template)

☑ Collect contact information of key stakeholders and members of your incident response team

☑ Conduct a table-top simulation exercise with your county’s cyber security response team
Part II

Activating Your Cyber Security Emergency Response Team

When a cyber incident occurs, issue notification as quickly as possible to minimize the impact on all individuals and organizations that may be affected, including law enforcement.

While this team should have been created or considered beforehand, now is the time to bring together your team that will help the county react and respond to this breach to your IT system(s). Your response team should include all of the individuals who have a direct stake in responding to and recovering from any cyber incident. Including but not limited to the chief county elected leader, the IT director, the county attorney, and your public information officer, among others.

The incident response team is responsible for determining the content of the notification to affected individuals and organizations and how that gets communicated. Some of the questions that should be considered include:

- Who are the affected parties?
- What support and remedies are being offered?
- What steps are being taken to minimize the impact?
- How should these messages be delivered?
- How will questions from affected individuals and organizations be addressed?

Contact all proper authorities and support:

- Law Enforcement Officials
- County Attorney’s Office
- Division of Homeland Security and Emergency Services
- Third Party Vendors
- Other additional appropriate authorities

County Datasets

Your IT department can work closely with your policy and management team to survey and assess the datasets hosted by your various county departments.

These datasets include, but are not limited to, employee records, financial records, bank accounts, voter registrations, court records, social service case files and records, probation case files, public defender cases, DA case files, nursing home records, as well as others.

These data assets should be documented and updated periodically with key contacts so that your incident response team can quickly identify and access appropriate personnel and supports in the event of a data breach or other cyber security incident.

County Cyber Response Team

- County Chief Elected Officer Executive’s Office
- IT Director
- Counsel
- Public Information Officer
- Sheriff
- Subject Matter Experts (ie department head of the impacted system(s), such at the election commissioners or social service commissioner, etc.)
- Emergency management director
Part III
Securing your Information Systems

Now that your response team has been put into place, it’s time to make decisions and take action that will limit the county’s exposure to risk and liability and help keep your county operational. The following steps—detect, contain, eradicate, and recover—are broken out in more detail below, but these should be taken up quickly to survey the damage and secure as many of your systems as possible.

Detection and Identification

This involves the ability of anyone in your county organization, including but not limited to your IT department, to recognize and report suspicious behavior, anomalies, precursors and indicators of a potential compromise. All personnel must be trained and tested on their ability to appropriately recognize and report incidents.

While not every anomaly or suspicious behavior will be a breach or compromise, they should be explored by a member of your cyber security team to categorize the incident and escalate as necessary. Examples of suspicious or anomalies include the detection of malware, evidence of tampering, inappropriate access to sensitive data, misuse of information or data, seeing an unauthorized person in a secured area, software validation failure, system failure, among others. Your cybersecurity response team should develop an incident classification categories or matrix to prioritize incidents and determine appropriate responses.

Some questions that need to be answered quickly:

- What happened?
- What systems were impacted?
- What programs are run by that system or software?
- What data has been infiltrated or compromised?
- Does this data include personal private information?
- Has the data been shared on the Internet or the Dark Web? See types of data below.

Containment

Your next immediate step is to contain the incident to as few locations or systems as possible. It’s time to isolate the network segment of infected workstations or taking down production servers that were impacted, to rerouting traffic to unaffected infrastructure. Test systems to ensure they are operational and configured securely after the incident is resolved. Communicate the damage done and the improvements applied to recovery planning and action to build trust and a culture of growth and resilience.

Eradication

If it is possible to eradicate the infected areas of your system, this should be done by your internal or external team as quickly as possible.

Recovery

Having consistent and ongoing backups of your systems and data is critically important for recovering your impacted IT systems. Identify the last full backup of your data and systems.
Part IV

Implementing Your County’s Continuing of Operations Plan

The county should have and be prepared to deploy a continuity of operations plan in the event that any of the county’s information systems are out of service, for any reason at all. This plan should include all operational processes for working with the public, including but not limited to social services, DMV and other county clerk operations, elections, mental health services. It should also include all internal processes for keeping the county operational, including payroll, banking, procurement, and other ongoing programs and services provided to residents, employees, and service recipients.

Part V

Activating Your County’s Crisis Management and Communication Program

A key component of your response plan is to provide the public with timely and accurate information.

The County Public Information Officer must be kept abreast of any developments that may impact the need for communication to internal or external stakeholders.

Maintaining trust in government operations is most effectively accomplished when the county speaks with one voice and has a plan to prevent the spread of inaccurate information across media outlets and social media. It is critical, through this or any other crisis, that the county communicates in ways that reduce speculation and limits the spread of inaccurate information.

The county may also want to consider contracting for crisis communication expertise.

Resources

INCIDENT RESPONSE PLANNING GUIDELINE
Berkely Information Security Office
security.berkeley.edu/incident-response-planning-guideline

IBM
6 Critical Stages of Incident Response

NATIONAL SECURITY RESPONSE PLAN
us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

NEW YORK STATE INFORMATION TECHNOLOGY SERVICES
Cyber Incident Response Guide for Agency Leadership
Cyber Security Primer for Principals
its.ny.gov/ciso/local-government

UNITED STATES CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
Cyber Essentials Toolkits | CISA
www.cisa.gov/publication/cyber-essentials-toolkits