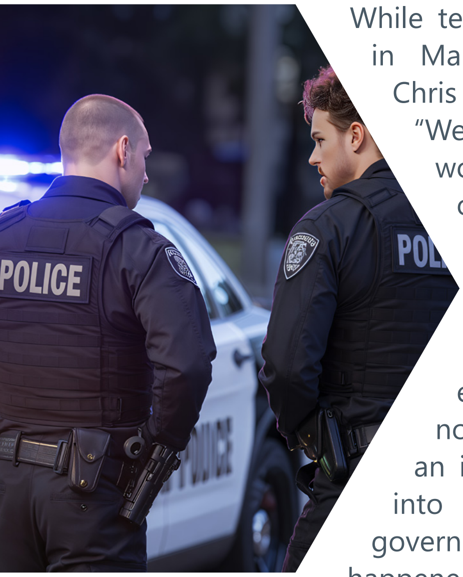
CNA

Protecting Critical Government Services from Cyber Disruptions

On September 8, 2022, the government of Suffolk County, New York was the victim of a ransomware attack. The breach caused significant data loss and prolonged disruptions to government services. For example, police incident reporting systems went offline, requiring officers to manually phone in reports over the radio. Most alarmingly, 911 dispatch computers were not functional for several weeks. The events in Suffolk County are not unique; they are part of a larger trend of rapid growth in cyber crime and attacks (such as the City of Saint Paul, MN and the state of Nevada). The potential human cost of these trends is particularly pronounced for state and local governments that rely on networked technologies to operate critical public safety and social services.



While testifying before Congress in March 2021, FBI Director Chris Wray remarked that, "We have long passed the world where it's a question of if an organization is going to be the victim of a cyberattack, we are in the world of when." While stopping every cyber intrusion is not realistic, preventing an intrusion from cascading into a disruption of critical government operations, as happened in Suffolk County, may be achievable. For example, state and local governments can take steps to fully isolate critical services from broader government networks and build cyber resilience by planning for operational continuity.

For many in local government, cyber resilience is a new concept, and one that has not been sufficiently studied in the state and local government context. CNA sees an opportunity here to fill a critical need. By investigating the details of recent government cyber intrusions and/or conducting workshops with government network defenders and consequence management professionals, we can build a knowledge base that state and local governments can leverage to enhance resilience and maintain continuity of operations in the face of an increasingly hostile cyber environment.

CNA takes a two-pronged approach to fully understanding cyber risk in this space, learn from recent events, and build preparedness and resiliency going forward.

Approach 1: Critical Incident Analysis

CNA conducts in-depth analyses of recent cyber incidents that have led to operational discontinuities. This research can focus on technology (e.g., the exploited vulnerability that catalyzed the attack or the structural failures that left critical government services vulnerable), or on the consequence management of the impacts of the outages on public safety and government continuity. Either way, our analyses include both a reconstruction of what happened and a path forward for remediation.

CNA employs our **ADEPT™** approach to critical incident analyses and after-action reviews—Adaptable, Data-Driven, Expert, Process-Oriented, and Transformational. This approach is custom designed to ensure agencies and organizations can extract optimal learning value from our analyses and continuously improve their operations, using a five-step Scope, Collect, Analyze, Share, Act process.

Approach 2: Workshops

In addition to critical incident analysis, CNA hosts workshops to proactively enhance state and local government cyber resilience. In each workshop, CNA conducts an analysis of the locality's cybersecurity posture and assists it in the framing of a governance strategy and incident response playbook.

To help government operators better understand their environment and effectively manage the risk of operational discontinuity caused by cyber incidents, the workshops focus on these key goals:

- **Identify critical systems and services** that must maintain operational continuity during cyber incidents.
- Assess the **network configuration and interconnections** between government systems and third-party software providers, looking for access points that put critical systems at risk.
- Assess the stakeholder's understanding of the **interdependencies between cyber, critical infrastructure, and emergency response** during a significant cyber incident.
- Assess the stakeholder's existing **continuity planning capabilities** and test these plans through a cyber incident exercise.
- Test the capabilities of the jurisdiction **to share intelligence and information** relevant to an incident in a timely manner.
- Foster discussion of how the jurisdiction will work to deliver coordinated, prompt, reliable, and actionable **public information** at the local and state levels.
- Examine the **incident-escalation process** in terms of information sharing and emergency management activities.
- Assist the jurisdiction in its efforts to share information, unify coordination, and integrate private-sector stakeholders in support of **recovery efforts**.

Why CNA?

CNA has designed, executed, and evaluated over 350 homeland security exercises since 1999, which have included participants ranging from local first responders to the president of the United States, and scenarios ranging from cybersecurity to hurricanes to disease outbreaks. Our cybersecurity staff draw from vast experience supporting exercises, planning, and policy for clients within the Department of Homeland Security, the Federal Aviation Administration, the World Economic Forum, UC Berkeley's Center for Long-Term Cybersecurity, and jurisdictions such as the State of Alaska, the Michigan State Police, the Cities of Fort Lauderdale and Sarasota, FL.

About CNA

CNA is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform the decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

CNA's Institute for Public Research (IPR) provides research and analysis to a diverse array of federal, state, and local government agencies. Please contact Dawn Thomas (thomasdh@cna.org) if you would like more information.

CNA