Dr. Evil's Revenge: CyberSizzle

Coconino County Health and Human Services, Arizona

National Association of City and County Health Officials Preparedness Summit

May 1, 2025

Table of Contents

Handling Instructions

TLP:CLEAR

The title of this document is Dr. Evil's Climate Caper Situation Manual. This document is unclassified and designated as "*Traffic Light Protocol (TLP):CLEAR*": Recipients can spread this to the world; there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and Coconino County Health and Human Services guidelines.

For questions about this event or recommendations for improvement contact: Blake Scott, Senior Public Health Emergency Preparedness Planner at 928-679-7228 or bscott@coconino.az.gov of Coconino County Health and Human Services. Or Scott Fraser at Scott@codelinenetworks.com Chief Executive Officer of Code Line Networks.

Exercise Overview

Exercise Name	**Dr. Evil's Climate Caper: A Disaster and Cyber-Attack Game**	
Exercise Date, Time, and Location	May 1, 2025 8:00 AM – 11:30 AM Preparedness Summit, Texas	
Exercise Activities	Time	Activity
	30 Minutes	Introduction, Threat Briefing and Opening Remarks
	60 Minutes	Exercise Play
	30 Minutes	Break
	60 Minutes	Exercise Play
	30 Minutes	Hotwash
Purpose	Experience a Complex Climate Change Event (Heat) and Cyber event	
National Institute of Standards and Technology Cybersecurity Framework Functions	Identify, Protect, Detect, Respond, Recover	
Objectives	1. Test participants ability to problem solve 2. Test information sharing processes 3. Identify 3 resources for planning, responding, recovery 4. Identify 2 areas of best practices for recovery 5. Identify 2 opportunities to engage national stakeholders on federal guidance and policy impacting local preparedness	
Threat or Hazard	Climate Change Event (Heat) and Cyber Attack	
Scenario	Dr. Evil is taking his revenge upon the Preparedness Summit! Back by popular demand! This exercise is a new story with a larger seat count! Dr. Evil is cyber-attacking the county and hospital during an emergency! We are ready for his revenge plans; we can stop him and save the world! Join us for a fun and informative tabletop/game combining extreme weather impacts, public health, and cybersecurity into a complex coordinated disaster event. You will love this interactive experience to laugh, learn, and network. The bad guy is fake, but the decisions are real. This exercise is Homeland Security Exercise and Evaluation Program (HSEEP) compliant and based on recommendations from the U.S. Department of Health and Human Services (HHS), National Institute of Standards and Technology (NIST), and Cybersecurity and Infrastructure Security Agency (CISA).	
Sponsor	Coconino County Health and Human Services	

Participating Organizations	Attendees	
Points of Contact	**Coconino County Health and Human Services** Blake Scott bscott@coconino.az.gov	**Code Line Networks** Scott Fraser scott@codelinenetworks.com

General Information

Using this Situation Manual

The situation manual contains the scenario summary and assistive tools. The appendices provide the following information to tailor the exercise discussion:

- Appendix B: Reference section for acronyms used within this situation manual
- Appendix C: Case studies that provide real-world examples of the threats presented in this scenario
- Appendix D: An explanation of the threats presented in this scenario
- Appendix E: Additional cybersecurity preparedness and response resources
- Appendix: Highlighted cyber response guides

Participant Roles and Responsibilities

Controllers/Evaluators (C/E) provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Controllers plan and manage exercise play, set up and operate the exercise site, and act in the roles of organizations or individuals that are not playing in the exercise. Controllers direct the pace of the exercise, provide key data to players, and may prompt or initiate certain player actions to ensure exercise continuity. In addition, they issue exercise material to players as required, monitor the exercise timeline, and supervise the safety of all exercise participants.

Players have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario. Suggested players include representatives from the Emergency Management, Public Health, IT, communications, human resources (HR), and legal departments, and any personnel with real-world cyber incident response roles.

Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise. Observers may include representatives from the IT, communications, HR, and legal departments as well as leadership who do not have assigned real-world cyber incident response roles but may be involved in response efforts or have a need-to-know.

Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise is intended to be a facilitated exercise. Players will participate in the following:

- Climate and Cyber threat briefing (if desired)

- Exercise Play
- Hotwash

Exercise Guidelines

- This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
- Decisions are not precedent-setting and may not reflect your local government's final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
- In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

Exercise Hotwash and Evaluation

The Controllers/Evaluators will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

Exercise Play

Late Spring (May 01, 2025), the NWS announces an extreme heat event this coming weekend.

Temperatures are warm, skies are beautiful and normal weather conditions for your area's spring are 10 degrees warmer than 50 years ago. The county fair is planned to start this Friday into the weekend with higher-than-average attendance expected.

General Summary of events:

Day	Events
Thursday May 1, 2025 (Module 1)	Extreme Heat Watch for Saturday Dr. Evil released
Friday May 2, 2025 (Module 1)	Extreme Heat Warning County Fair starts
Saturday May 3, 2025 (Module 2)	Extreme Heat begins (very hot) Levine Hospital evacuates Heat injury patients start to arrive at hospitals EOC opens Fair continues
Sunday May 4, 2025 (Module 3)	Extreme Heat continues Cyber Event continues PH dept receives hospital ER data Medical Examiner's Office decedent flow increases
Monday May 5, 2025 (Module 3)	Heat & cyber events continue Heat injury patients and heat fatalities continue
Time Jump	20 days after onset of heat & cyber events

Day	Events
(Module 3)	

Appendix B: Acronyms

Acronym	Definition
BYOD	Bring Your Own Device
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cybersecurity Performance Goals
CSF	Cybersecurity Framework
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
HTTP	Hyper Text Transfer Protocol
HR	Human Resources
IP	Internet Protocol
IT	Information Technology
NCEP	National Cyber Exercise Program
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
TLP	Traffic Light Protocol
VoIP	Voice over Internet Protocol
ZTA	Zero Trust Architecture

Appendix C: Case Studies

Royal Ransomware Attack

The Royal ransomware group launched a ransomware attack against a large U.S. city in May 2023. The computer systems used by the police, fire department, courts, and libraries were compromised. The IT team immediately disconnected systems, services, and devices from the network to prevent the spread of the ransomware.[1] The ransomware note sent to the city's printers stated the group downloaded sensitive data from the city's servers and promised to restore network access and keep the attack confidential if they paid the ransom. The investigation showed the ransomware group accessed the servers for three weeks prior to the ransomware attack and downloaded the personal information of over 27,000 people. The city sent letters to current employees, retirees, and their relatives notifying them that their names, Social Security numbers, dates of birth, and medical records were exposed. The City Council approved over $8 million to cover hardware, software updates, and incident response.[2]

Ransomware Attack and Secondary Data Leak

A large U.S. city declared a state of emergency in February 2023 after a ransomware attack resulted in network outages for the city's systems. The city took its network offline to prevent the spread of the ransomware. Internal city government impacts included internet outages at City Hall and no access to payroll systems. Constituent facing processes normally handled electronically reverted to paper processes, slowing services such as filing police reports. Most services were restored within days of the attack, however some services such as city employee email and voicemail remained unavailable for three months following the initial attack. Two months after the initial attack, the ransomware group that claimed responsibility for the initial attack leaked additional PII and personal financial information of employees and residents on the Dark Web. The city never paid the ransom.[3] City employees filed a class-action lawsuit against the city after the second data leak, claiming the city did not adequately protect their information.[4]

Actors inside of US Critical Infrastructure

Chinese hackers hit critical U.S. infrastructure, intelligence agencies warn

https://www.axios.com/2023/05/25/chinese-hackers-critical-infrastructure-us-guam

A Chinese state-sponsored group has hacked into critical American infrastructure, including in the U.S. territory of Guam, Microsoft and the "Five Eyes" intelligence alliance warn.

Why it matters: Guam is home to three American military bases. The western Pacific island would play an important strategic role should the U.S. need to respond to any potential Chinese military attack on or blockade of Taiwan.

[1] Alanna Quillen, Larry Collins and Lili Zheng, "Dallas releases technology accountability report following ransomware attack," *NBC DFW,* June 9, 2023, https://www.nbcdfw.com/news/local/dallas-to-release-technology-accountability-report-following-ransomware-attack/3274570/.

[2] Ken Kalthoff, "Dallas pays millions for ransomware expenses after May attack," *NBC DFW*, June 9, 2023, https://www.nbcdfw.com/news/local/dallas-pays-millions-for-ransomware-expenses-after-may-attack/3313643/.

[3] Stephanie Sierra, "Did Oakland have right cyber insurance before the ransomware hack? Here's what experts say," *ABC7 San Francisco,* May 12, 2023, https://abc7news.com/oakland-ransomware-attack-hacked-cyber-insurance-san-bernardino-county/13240537/#:~:text=Four%20months%20after%20the%20%22Play,Team%20no%20payment%20was%20made.

[4] Shomik Mukherjee,"Oakland hit with class-action lawsuit by city employees over ransomware attack," *Easy Bay Times,* May 31, 2023, https://www.eastbaytimes.com/2023/05/31/oakland-hit-with-class-action-lawsuit-over-ransomware-attack/.

The likely aim of the operation is to "disrupt critical communications infrastructure between the United States and Asia region during future crises," per a blog post Wednesday by Microsoft, which detected the hacking.

Driving the news: The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory with its "Five Eyes" partner agencies in the U.K., Canada, Australia and New Zealand warning that the "Volt Typhoon" hackers posed a threat to all five allied countries following a "recently discovered cluster of activity."

Microsoft said in its blog post that the "state-sponsored actor based in China ... typically focuses on espionage and information gathering."

Detecting "and mitigating this attack could be challenging," Microsoft said.

State of play: "Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States," per Microsoft.

"In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Observed behavior suggests that the threat actor intends to perform espionage and maintain access without being detected for as long as possible."

The Australian Signals Directorate's Australian Cyber Security Centre noted that a key strategy of Volt Typhoon, known as "living off the land," used "built-in network administration tools to perform their objectives," allowing the group "to evade detection by blending in with normal Windows system and network activities."

The big picture: The Chinese Communist Party has been linked to previous hack attacks targeting the U.S. government, businesses and American infrastructure, but it has always denied being involved in such cyber espionage.

What they're saying: "Today's advisory highlights China's continued use of sophisticated means to target our nation's critical infrastructure, and it gives network defenders important insights into how to detect and mitigate this malicious activity," CISA director Jen Easterly said in a statement.

Cyber Attacks and Typhoon Mawar prompt Guam Cyber Conference - https://www.dvidshub.net/news/449832/cyber-attacks-and-typhoon-mawar-prompt-guam-cyber-conference

GUAM

07.24.2023

Story by Mark Scott

Guam National Guard

TUMON, Guam (July 18, 2023) – Outside the hotel conference room in the U.S. Territory of Guam, it looks like a normal tropical day. It does not appear that less than two months ago, Typhoon Mawar ravaged the island with 140-mph sustained winds.

Thanks to the whole-of-community approach between local and federal governments and community partners, the visible scars to critical infrastructure appear to have healed. Power and water have been restored to nearly 100 percent, and roadways are clear. But not all the scars are immediately visible.

On the day of Typhoon Mawar's landfall, a multi-national advisory and Microsoft announced a malicious computer code was discovered in telecommunications systems in Guam and elsewhere in the United States. The attacks were attributed to Volt Typhoon, a state-sponsored hacking group that carries out espionage and information gathering for the Chinese government.

Inside the hotel conference room, Guam Governor Lou Leon Guerrero gave opening remarks to an audience of over 100 cyber stakeholders, at a gathering hosted by the Guam National Guard. Representatives from the U.S. Indo-Pacific Command, U.S. Cyber Command, Fleet Cyber Command, Cyber Infrastructure and Security Agency, FBI, FEMA, Guam Homeland Security and Office of Technology, and others, were present.

"Cybersecurity is one of the things that keeps me up at night," said Gov. Leon Guerrero. "Our communications went down during Typhoon Mawar, and it was frustrating trying to connect with frontline workers to find out what was going on. But this gives me relief in knowing we will have a comprehensive and unified cyber plan. As a whole-of-community, we need each other to make this happen to protect our island and nation."

[Content was shortened by Coconino County, see link for full article]

Communications Status Report for Areas Impacted by Super Typhoon Mawar June 8, 2023 – FCC REPORT - https://docs.fcc.gov/public/attachments/DOC-394155A1.pdf [Content was shortened by Coconino County see link for full report]

Communications Status Report for Areas Impacted by Super Typhoon Mawar

June 8, 2023

The following is a report on the status of communications services in geographic areas impacted by Super Typhoon Mawar as of June 8, 2023 at 10:00 p.m. Chamorro Standard Time (CHST) / 8:00 a.m. Eastern Daylight Time (EDT). This report incorporates network outage data submitted by communications providers to the Federal Communications Commission (FCC) Disaster Information Reporting System (DIRS). Note that the operational status of communications services during an event may evolve rapidly, and this report represents a snapshot in time.

The FCC activated the DIRS on May 23, 2023 with a modified reporting time of 10:00 p.m. CHST / 8:00 a.m. EDT, to coincide with Super Typhoon Mawar impacting the northern edge of Guam.

On June 5, 2023 the FCC released a Public Notice announcing the narrowing of the DIRS reporting area, deactivating DIRS for the Commonwealth of the Northern Mariana Islands. DIRS remains activated in Guam.

The following territories in Guam are in the current geographic area that is part of DIRS (the “disaster area”) for today’s report.

Broadcast:

Television stations status:

- 1 TV station reported as being out of service (KGTF). FM Radio stations status:
- 3 FM stations reported as being out of service (KSTO, KISH, K290CR).

AM Radio stations status:

- 1 AM station reported as being out of service (KTWG).

Appendix D: Attacks and Threats

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware and associated data breach incidents can severely impact business processes, leaving organizations unable to access data necessary to function. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Stop Ransomware Website (https://www.cisa.gov/stopransomware)
- CISA Stop Ransomware Guide (https://www.cisa.gov/resources-tools/resources/stopransomware-guide)
- Protecting Against Ransomware (https://www.cisa.gov/news-events/news/protecting-against-ransomware)

Social Engineering and Phishing

One of the most prominent tactics threat actors use to exploit network and system vulnerabilities is social engineering, which is the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing. Phishing is often executed via email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for compromising networks and evading intrusion detection systems without leaving a log trail, and it is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the involvement of human emotions. Organizations should take steps towards strengthening employee cybersecurity awareness training by incorporating trainings on identifying suspicious emails, instructing personnel on how to report them, and emphasizing the importance of keeping software systems up to date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks)
- Phishing Guidance: Stopping the Attack Cycle at Phase One (https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one)

Appendix E: Contacts and Resources

Federal Government Contacts

- CISA (contact: central@cisa.gov, https://www.cisa.gov)
- United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact https://www.secretservice.gov/contact/field-offices, https://www.secretservice.gov/investigation/cyber)
- Federal Bureau of Investigation (FBI)
    - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
    - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
    - National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; 855-292-3937)

State Level Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; 518-266-3460)
- National Governors Association (NGA) (https://www.nga.org/)
    - NGA Center for Best Practices (https://www.nga.org/bestpractices/divisions/hsps/)
- DHS Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- National Association of State Chief Information Officers (NASCIO) (https://www.nascio.org/)

Preparedness Resources

- CISA Cross-sector Cybersecurity Performance Goals (https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist)
- NIST Cybersecurity Framework Tools (https://csf.tools/)
- SLTT:
    - State and Local Cybersecurity Grant Program (https://www.cisa.gov/state-and-local-cybersecurity-grant-program)
    - CISA CDM Program (https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program)
    - CISA Find Help Locally (https://www.cisa.gov/audiences/find-help-locally)

Additional Resources

- InfraGard (https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf)
- Internet Security Alliance (https://isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
    - International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
    - National Council of ISACs (https://www.nationalisacs.org)

Appendix: Highlighted Cyber Response Guides

Preparedness CISA Cyber Essentials Starter Kit

https://www.cisa.gov/sites/default/files/publications/Cyber%2520Essentials%2520Starter%2520Kit_03.12.2021_508_0.pdf

Healthcare specific cybersecurity guidance from US Dept. Health and Human Services

https://405d.hhs.gov/

CISA: Federal Government Cybersecurity Incident & Vulnerability Response Playbooks

https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf