2023
North Carolina
PSAP Cybersecurity
Tabletop Exercise (TTX) Series

Harlan Squires, Exercise Facilitator
harlan.t.squires@saic.com

May 16 , May 18, June 6, & July 11, 2023

CISA/ICTAP-NC-PRES-008-R0

Purpose

- This Tabletop Exercise (TTX) will provide an opportunity to evaluate current:
  - PSAP/ECC Cybersecurity concepts
  - PSAP/ECC Cybersecurity plans and procedures
  - PSAP/ECC Cybersecurity capabilities and redundancies
- The TTX will focus on:
  - Key emergency responder coordination
  - Critical decision and notification processes
  - Integration of local, regional, and federal assets

Scope

- Throughout the exercise the emphasis will be on:
  - Public safety cybersecurity capabilities
    - Current and future/desired capabilities
    - Traditional and emerging communication and notification pathways
  - Implications of these capabilities on cybersecurity and communication policies, procedures, & plans
  - Strategies for incorporating new capabilities into the regional public safety ecosystem

Outcomes

- TTX outcomes should include:
  - A better understanding of how cybersecurity compromise can impact incident response coordination and notifications processes
  - A gap analysis of those cybersecurity and communication plans, policies, and capabilities that require additional consideration or improvement
  - An Improvement Plan consistent with Homeland Security Exercise and Evaluation (HSEEP) standards

Capabilities

- Capabilities-based planning takes an all-hazards approach to build capabilities that apply to a wide variety of incidents
- The National Preparedness Goal details a list of the five mission areas and the 32 **Core Capabilities**
- This TTX will target the following Core Capabilities
  - **Cybersecurity**
  - **Planning**
  - **Operational Communications**
  - **Operational Coordination**
  - **Public Information and Warning**

Exercise Goal

To discuss PSAP cybersecurity policies, procedures, plans, available assets, and capabilities used by agencies in response to a significant multi-jurisdictional incident or event.

Exercise Objectives

- Engage stakeholders of the PSAP critical system(s), to discuss the operations and applications of the system(s) in the occurrence of a cybersecurity compromise.
- Identify and discuss the necessary notification pathways that are critical during a cybersecurity related compromise.
- Discuss the NIST response cycle related to a cybersecurity compromise to a PSAP.
- Engage private partners to work with public safety entities to solve cybersecurity related problems.
- Identify redundant interoperable communication capabilities in the event of major disruptions to the primary communication system during a cybersecurity related incident.
- Enhance the overall readiness in the event of an actual emergency involving a large-scale cybersecurity event/incident.

Exercise Structure

- This TTX is a structured exercise focused on:
  - Knowledge and understanding of participants in identifying, mitigating, responding to, and recovering from a cybersecurity incident or event.
  - Ability of participants to communicate and coordinate their efforts using available and predicted assets.
  - Opportunity to engage in facilitated discussion of cybersecurity and communications capabilities
- Discussion will focus on various vignettes of potential cybersecurity related incidents or events.
- Facilitator will initiate each topic and encourage input from appropriate players

Exercise Planning Team Agencies

- Chatham County Emergency Communications
- CISA/ICTAP
- CISA/IOD
- Durham Emergency Communications
- Lincoln County E 9-1-1
- North Carolina 911 Board
- North Carolina Emergency Management
- Rowan County

Roles & Responsibilities: Players

- Respond based on knowledge of:
  - Response procedures
  - Current plans
  - Cross-jurisdictional agreements
  - Knowledge of cybersecurity and communications capabilities
- Consider your agency's communications processes and needs (whether called upon or not)
- Make written notes of communication gaps in Situation Manual, as desired

Roles & Responsibilities: Observers

- Provide information acting as subject matter experts
- Take written notes of communication gaps and capabilities in Situation Manual, as desired
- Provide input during the hotwash

Roles & Responsibilities: Evaluators

- Subject Matter Experts from CISA/ICTAP
- Take electronic notes of observed communication successes, gaps, and areas of uncertainty
- Collect and compile information necessary for the After-Action Report/Improvement Plan (AAR/IP)

Roles & Responsibilities: Facilitator

- Provide situation updates and moderate conversation
- Provide additional information
- Resolve or redirect questions as they develop

Assumptions and Artificialities

- The scenario is plausible
- There are no trick questions or hidden agendas
- All Players receive information at the same time
- Some necessary technical artificialities exist in order to approximate communication within the confines of the exercise environment

Assumptions and Artificialities

- Treat the TTX scenario as if it were occurring in the real world. Specifically, describe your response by detailing currently existing, or realistically predicted, communication capabilities, assets, jurisdictional agreements, and procedures.

Rules

- There is no single accepted solution
- Varying viewpoints, even disagreements, are expected
- Respond based on your knowledge of current communications capabilities, plans and in-place assets
- Where necessary, consider how you would incorporate future capabilities into existing plans and procedures

Rules

- This exercise is focused on public safety capabilities, not individual systems, products, or networks
- To provide input to the exercise:
  - Identify yourself
  - Describe your topic to the group

Schedule

- 8:30 Registration/Check In
- 9:00 Exercise Briefing
- 9:15 Cybersecurity Briefings
- 10:15 Exercise Begins
- 11:15 Break
- 11:25 Discussion Continues
- 12:30 End of Exercise
- 12:30 Lunch and Learn
- 1:30 Hotwash/Debriefing
- 2:30 Adjourn

QUESTIONS?

Introductions

Cybersecurity Briefings

Mike Reitz and Adam Gaines
Chatham County Emergency Communications
Chatham County Cybersecurity Incident

A PSAP in the Dark:

Chatham 911's Cyber Attack Experience

- Mike Reitz – Director
- Adam Gaines – Assistant Director

- Emergency Communications
- Chatham County
- Pittsboro, North Carolina

Your network was hacked. Your ID: 99

All your important files are encrypted. We have your sensitive data.

At the moment, the cost of private key for decrypting your files is 5 BTC ~= 212,200 USD.
Your Bitcoin address for payment: http://thisisnotreal.onion

You can also make a payment with PayPal or Cash Card.

If you do not comply, your important files will be unretrievable and your sensitive files will be released.

Day of Cyber Attack

Wednesday,
October 28, 2020

D-Day

14th day of Early Voting

237th day of COVID19 response

6 days before Election Day

Early AM – Indicators of Compromise detected. Chatham MIS (IT), security vendor, and NCLGISA engaged.

8AM - County managed phones, email, voicemail, Internet, and file servers are down.

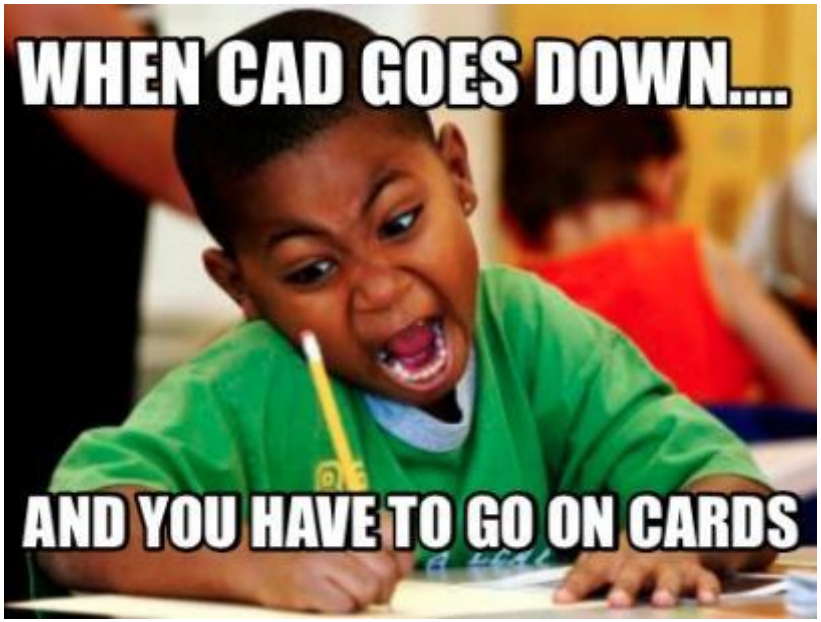
9AM – After SITREP from MIS, County EOC is activated, assumes lead for Continuity of Operations, Continuity of Government, and traditional IT services.

3PM - All departments instructed to stop use of any device that has been on the County network.

Dirty, Borrowed or Purchased

FIRSTNET®
Built with AT&T

Direct Operational Impacts



Unable to use:

CAD, ProQA, DCI/NLETS, Email, county network

Not affected:

Radio system

Phone system (911/admin)

Recorder

Cardsets

Observations & Lessons Learned

- Invest time in planning with your County EM.
- The EOC should be a source of information as well as resources.
- Cloud hosted and decentralized systems remained available.
- Plan and build relationships with vendors
- Need to communicate early and often with the public.
- Need better plans for printing during incident.
- Secure means to store and access essential files.
- Expect EOC Priorities to shift over time.
- Expect each step of restoration to take time.

P.A.C.E Plan

- Primary
- Alternate
- Contingency
- Emergency

Cybersecurity Briefings

Ronald Rombs
Lincoln County E9-1-1
Lincoln County Ransomware Incident

Ransomware Attack
July 26, 2019

Lincoln County E9-1-1 Presentation

Lincoln County E9-1-1 Historical Data (At the Time of Incident)

- 911 center was housed inside the Lincoln County Sheriff's Office.
- PFSense Firewall separating Sheriff's Office and 911 systems
- Shared Spirit fiber internet connection provided by the Sheriff's Office, as well as a redundant Charter 10mb connection
- Two Dell CAD physical servers located in the Sheriff's Office
- One Utility PC
- One Domain Controller PC
- One User Share/Documents Server
- 6 Call Taking Positions, 3 Administrator PCs
- Solacom Phone System
- MCC7500 Radio Consoles – State VIPER Network

Lincoln County E9-1-1 – Ransomware Attack

- The evening of July 26th, 2019, around 1800, I had a conference call with CentralSquare to help with facilitating some CAD updates.
- During the call, we were noticing some inconsistencies and disconnects from remote sessions.
- Roughly around 2030, CentralSquare was kicked completely out of their remote desktop session, and I watched as icons on the CAD server started changing to Ryuk filename structure and then connections were severed.

Lincoln County E9-1-1 – Ransomware Attack (2)

- Attempts were made by myself and CentralSquare to get back into the servers, but we kept getting kicked out.
- I immediately notified my Director and IT staff at the Sheriff's Office.
- I began unplugging all network cables on all the servers. At this point, CAD stopped functioning, so I worked on ensuring that the on duty telecommunicators had paper CAD sheets to start tracking information.
- The 911 center was notified by several on-duty officers that their mobiles were not working as well.

Lincoln County E9-1-1 – Ransomware Attack (3)

- County IT staff arrived on scene (Director and Network Analyst) and began assisting 911 and Sheriff's Office staff on attempting to trouble shoot any issues and see what avenues we had to attempt to return to an operational state.
- Phone functionality and radio functionality were not impacted at all due to both systems being on their own networks.
- The IT Director began making notifications to external agencies to make them aware of the attack impacting our 911 center and Sheriff's Office.

Lincoln County E9-1-1 – Ransomware Attack (4)

- As the night went on, the entire administrative staff of the 911 center and Sheriff's Office had arrived to help delegate tasks and help improve dispatching practices.
- We deployed a laptop running on a wireless hotspot to access our local GIS website and data to confirm proper dispatch of Fire Departments.
- We also utilized a laptop with the state VPN connection to continue to function on DCI, since we are the alt-route for the Sheriff's Office and Lincolnton Police Department after 5pm and weekend/holidays.

Lincoln County E9-1-1 – Ransomware Attack (5)

- As early morning approached, what started as an 8-hour day turned into an 18-hour day.
- Resources from outside agencies started showing up to assist with the ransomware incident. It was as if the entire sheriff's office building was transformed. Conference rooms became workstations for National Guard, server rooms became crime scenes for FBI and SBI.
- For someone who had very limited resources and IT background, this process became very educational very quickly. What seemed like hours became days as the first couple of days were investigational and studying.

Lincoln County E9-1-1 – Ransomware Attack (6)

- For our small center, with limited IT support from the County and internally within the department, the informational gathering was tedious.
- We spent many hours in the ceiling and under the raised floors, tracing cables to their locations, finding switches we didn't know existed, basically building a network diagram from scratch to verify all the connectivity and locations of all internally networked devices to determine what other services or devices could have possibly been impacted by the ransomware.

Lincoln County E9-1-1 – Ransomware Attack (7)

- As the investigation moved forward, further resources started coming in.
- National Guard showed up with a team of about four staff as well as members of the Cyber Taskforce, in particular, Randy Cress.
- When I tell you that this resource is invaluable, I can say with confidence, the restoration would have not gone anywhere as good as it went without Randy and the team that came in. As soon as they arrived, we started the process of cleaning the hardware and preparing for the rebuild.

Lincoln County E9-1-1 – Ransomware Attack (8)

- With the assistance of County IT, we relocated all impacted hardware to the County IT Department Conference Room. This became the focal point of all PSAP related work during the restoration process.
- We began by turning all the physical servers into virtual machines. We ensured that all devices were no longer network connected and migrated the virtual copies to laptops to start sorting through what settings and information was available on the machines to help begin the rebuild process.

Lincoln County E9-1-1 – Ransomware Attack (9)

- Once we had gathered all the available information from the servers, in particular our Domain Controller, National Guard took the lead in starting to ensure the hardware was completely wiped and began rebuilding the machines with their STIGs and best practices.
- STIG is based on Department of Defense (DoD) policy and security controls and is an implementation guide geared to provide high level security for devices.

Lincoln County E9-1-1 – Ransomware Attack (10)

- This process took several days and long hours of building and patching and updating each individual server.
- The National Guard and Cyber Taskforce worked hand in hand each step of the way as we slowly went through each machine and ensured all settings were restored to the best of our ability, while finetuning and adapting some settings to create a new baseline of security for the PSAP.
- This process was then replicated to the workstation desktops as well.

Lincoln County E9-1-1 – Ransomware Attack (11)

- The total process took about 28 days from onset of symptoms within the networks to standing back up the core infrastructure of the PSAP itself. The commitment that was brought to the table by the Cyber Taskforce and National Guard was astounding. So much was given from each member of these teams, countless hours sitting in front of the monitors pecking away, to 10-minute shut eyes on the conference floor while waiting for updates.

Lincoln County E9-1-1 – Ransomware Attack (12)

- It was the dedication and hard work of these members that motivated me to pursue my Associates in Networking and Cybersecurity. This process, while providing many sleepless nights and a bunch of heartburn, provided much insight on how things were handled and best practices that were completely overlooked.
- The caveat to all this, was at the same time, we were finishing up building our new Primary PSAP facility, and this allowed much needed improvements to our technical planning and processes.

Lincoln County E9-1-1 – Ransomware Attack (13)

- As of today, we have improved the security of the entire PSAP, from providing redundant networking paths into the building, latest and greatest firewall technologies, as well as a completely isolated and stand-alone network that operates autonomously from the County and Sheriff's Office networks.
- We moved to a hosted email through the State DIT and migrated to completely virtual machines for all our servers.

Lincoln County E9-1-1 – Ransomware Attack (14)

- The biggest lessons learned were:
  - Have a comprehensive network diagram and understanding of how things connect and function together.
  - Build relationships with IT support to have a better understanding of the functionality and IT needs of the PSAP.
  - Have ongoing education with internal staff on best practices for email usage and ongoing training for Phishing attempts.
  - Isolated network to prevent this type of spillover incident to occur.
  - Maintaining best practices and building a baseline for updates and maintenance on servers to isolate possible attack vectors.

Cybersecurity Briefings

Randy Beeman
City of Durham
Durham Emergency Communications
Ryuk Ransomware Incident

Durham Emergency Communications Center (DECC)

- Full-Service Agency
  - Call Processing for the City of Durham (Population ≈352,161)
  - Dispatch City & County Fire
  - Dispatch Durham County EMS
  - Dispatch all 5 jurisdictions of Durham Police Department (DPD)
- Average Call Volume
  - 525,113 (2022)
  - Approx 1,439 per day

Ryuk Ransomware Attack
Incident Summary

- Technology Solutions provided notification of the monitoring detection provided by a 3rd party agency
- This resulted in a manual disconnection of networks in the main data center, DECC, and DPD
- Initial assessment showed a citywide impact to 700 workstations which quickly increased to 2500 workstations and 80 data center servers
- Proposed Solution from Technology Solutions:

  Isolate
  Clean
  Restore Data & Applications
  Reconnect workstations and servers to network after steps 1-3 has been performed

Ryuk Ransomware Attack
DECC Impact

No Impact

- 911 call processing through the ESiNet Hosted Solution
- Motorola Radio System

Direct Impacts

- Computer Aided Dispatch (CAD)
- Toning & Paging Software
- Geographical Information Systems (GIS)
- Message Switch- Mobile Data Terminals (MDTs)
- Police Identification Network (authority of NCIC)
- Recorder Systems

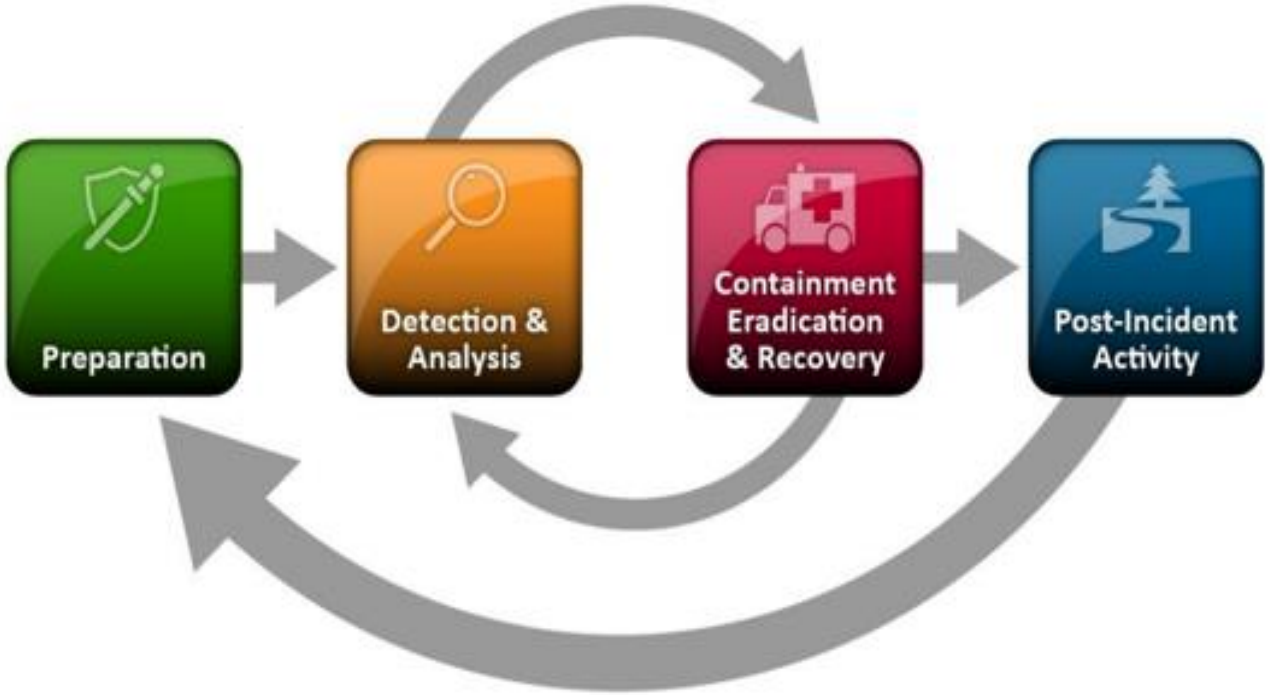
Ryuk Ransomware Attack
Lessons Learned

- Ensure that all software applications are updated to most recent versions
- Staff Preparedness:
  - Disaster Recovery Plan
  - Semi-Annual Manual Radio Dispatch Training
  - Access to hard copied map data, response plan data
- Strategic Cyber-Security
- Implementation of Immutable Repository i.e., Rubrik Technology
- Next-Generation Antivirus Platform i.e., Sentinel One

Collaborative Operational Support

- Durham City/County Police, Fire, EMS
- Technology Enterprise Solutions
- Duke University Technology Solutions
- NC National Guard Information Technology
- NC Department of Information Technology
- 3rd Party Contract Services

National Institute for Standards in Technology Incident Response Cycle



NIST Cycle

Prevention:

- What steps could be taken to prevent cyber incidents in your Communications Centers?

Detection and Analysis:

- What steps will be taken to detect the impact on the system?
- What further analysis is necessary to understand how to prevent future incidents?

Containment, Eradication, and Recovery:

- How is this contained so it will not impact the rest of the radio system?
- What steps can be taken to remove the problem (files, virus, Trojan horse, malware, etc.) from the system?
- What is the process for recovery from an incident?

Post Incident Activity:

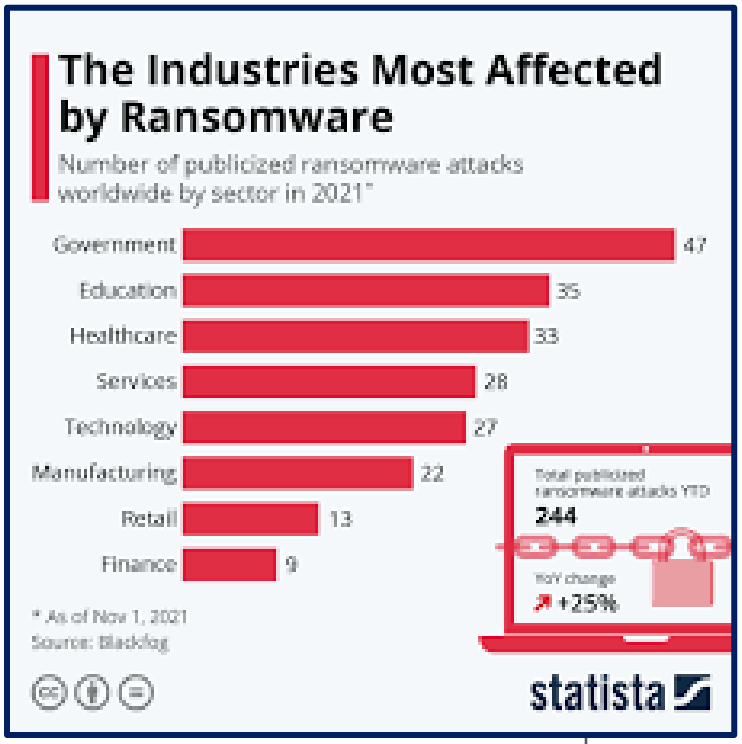
- How do you prepare for future incidents and prevent them?
- What is the After Action Reporting process for an incident like this and what is the policy for sharing those findings with partner agencies?

Cybersecurity Roles and Responsibilities

What are the various roles and responsibilities for users of information technology systems and networks?

State and Local

- Telecommunications Personnel
- Supervisors
- Information Technology/ Cybersecurity Personnel
- Land Mobile Radio Personnel



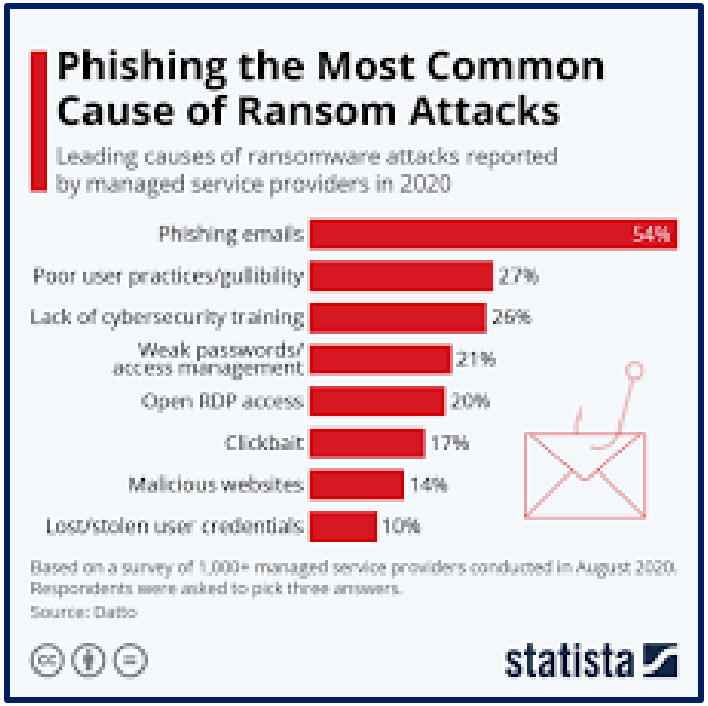
Scenario 1: Work Station Compromise

It is a fairly normal day in the county. There are a few activities going on that responders are watching closely. Around 9:00 AM a call comes into dispatch from a patrol officer asking why they are not answering on the radio. Upon further investigation the supervisor on duty realizes that they are not able to transmit or receive on the radio system.

Later it is determined that malware was uploaded into the system via a dispatcher's infected phone plugged into a monitor USB port that was unrestricted.

Scenario 2: Vendor Access

Vendor has installed a firmware update remotely and they failed to save your data sets prior to installation. The data sets were lost during the update and will take a significant amount of time to recover.

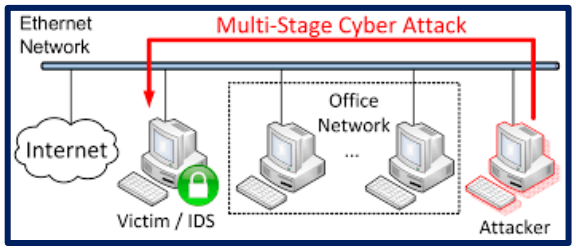


Scenario 3: Ransomware

Access to your agency's CAD system has been locked out. There is no expectation of being able to access the system within the next 48 hours. The IT department determines this was a Ransomware attack, although no demands have been made at this time.

Later it is determined that malware was uploaded into the system via a dispatcher's infected phone plugged into a monitor USB port that was unrestricted.

Requests for information/interviews relating to the attack have begun coming in from members of the media.



Thank You!

- Please complete the Participant Feedback form (last page of Situation Manual)
  - Turn in as your ticket to lunch
- Turn in your Situation Manual at the Registration Table, if desired

Cybersecurity Best Practices

North Carolina PSAP Tabletop Exercise
Eric Zach

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Common Entry Vectors:

- Spear Phishing (90%)
- Social Engineering
- Credential Reuse Attacks
- Poor/No implementation of security controls
- USB/External Media
- Unverified or Insecure code dependencies

Sophisticated Entry Vectors:

- Cloud compromises
- Compromising a 3rd party
- Compromising Managed Security Providers
- Internet of Things
- Zero Days
- Supply Chain

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Proactive Resources

- **Security Assessment/Penetration Testing Support:** The Assessment Team provides cybersecurity hygiene audits/ assessments on networks and infrastructure.
  - Work hand-in-hand with each agency
  - Provide a comprehensive evaluation on their technology and environment,
  - Utilize industry best practice solutions to identify vulnerabilities, gaps in security policy, along with detailed recommendations for improvement.
  - Past 12 months completed more than 50 assessments across state

- **Quick Reaction Support (Cyber QRF):** The QRF has trained Incident Responders who can lead agencies into initial triage and through the completed process
  - Scoping call in minutes
  - On scene of the cyber attack anywhere in the state within hours
  - Contain the incident
  - Provide technical expertise to restore services as quickly as possible.
  - Past 12 months completed more than 20 Incident Responses

Strategy - Cyber Hygiene Cycle

- Address vulnerabilities discovered in penetration testing report
- Identify additional risk acceptance and document mitigation strategy
- Evaluate processes, policies, and procedures to ensure comprehensive coverage
- Leverage report to determine additional resource requirements

- Assessment of information security program, environmental factors, and technical area review
- Identify potential gaps in coverage as provide baseline of improvement recommendations
- Conducted using industry best practices and DOD Security Technical Implementation Guidelines (STIGs)
- Output is comprehensive report outlining vulnerabilities and recommended solutions

- Validate the steps taken during remediation to ensure appropriate resolution
- Identify additional areas of concern including user awareness and network monitoring capability
- Output is comprehensive report detailing actions taken and recommended solutions

- Assessment report prioritizes and addresses vulnerabilities
- Determine acceptable risk levels and document risk mitigation strategy
- Develop internal processes, policies and procedures to improve security posture
- Leverage report to determine additional resource requirements

Top 10 NCAAT Recommendations

- Remove or secure RDP
- Systems must be patched
- Restrict anonymous shares
- Segment critical assets and admin accounts from the Internet
- Disable Autorun
- Disable Windows Installer Always with elevated privileges
- Use proper procedures with admin accounts (no sharing or using default)
- Mitigate risk of out-of-date equipment
- Follow proper backup procedures
- Implement port control solution

These fixes cost little to no money, but they do require time and effort.

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Reporting Cybersecurity Incidents

The state has multiple means to report cyber incidents, as indicated in the following table.

State Agencies	Local Governments, Academic Institutions & Private Sector Entities
Contact the NCDIT Customer Support Center at 800-722-3946.	Report cybersecurity incidents to the N.C. Joint Cyber Security Task Force by contacting the N.C. Emergency Management 24-Hour Watch Center, at NCEOC@ncdps.gov or at 1-800-858-0368.
Use the Statewide Cybersecurity Incident Report form.	For general inquiries or support, contact the N.C. Joint Cyber Security Task Force at ncisaac@ncsbi.gov.
Contact the Enterprise Security and Risk Management Office at DIT.ThreatManagement@nc.gov.	

Regardless of which method is used, the data is consolidated, tracked and acted on by the Joint Cyber Security Task Force. The state entity (e.g., N.C. Department of Public Safety or N.C. Department of Information Technology) receiving the initial report, will ensure coordination with relevant CSTF members.

Please note, this reporting does not override any other mandated federal reporting requirements.

- Resources to find more information on Cyber security incidents and when/how to report
- How to Report a Cyber Incident

- State Cybersecurity and Risk Management Resources
- Cybersecurity and Risk Management Resources

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

NCLGISA Cybersecurity Strike Team

A volunteer group of local government IT professionals, working directly with peers to improve cyber posture, reduce risk of exposure/attack, and provide incident response services during events.

Leadership and Core Members

Scott Clark, CIO, Town of Fuquay-Varina

Randy Cress, Assistant County Manager/CIO, Rowan County

Mark Seelenbacher, CIO, Henderson County

Chad Coble, CIO, Stanly County

Ted Norris, Deputy CIO, Onslow County

Logan Steese, CIO, Currituck County

Amy Walker, CTO, Ashe County Schools

Rob Hudson, IT Infrastructure Mgr, City of Greenville

Brian May, CISO, Wake Technical Community College

Chris Puryear, CIO, Person County

Shannon Tufts, UNC SOG Professor

Cybersecurity Briefings

Randy Cress / Alex Reinwald
Rowan County / NC National Guard
Joint Cyber Task Force (JCTF)

NC Public Sector
Significant Cybersecurity Incident Statistics

- Significant cyber attacks happen every 14 seconds worldwide
- Increase of 350% since 2018

NC Public Sector Statistics

- **2019**: 10 (reported) significant cyber incidents
- **2020**: 24 significant cyber incidents
- **2021**: 20+ significant cyber incidents; 160+ orgs remediated*
- **2022**: 15+ significant cyber incidents as of October 15, 2022 (+6-10 smaller cases)
- Downtime from significant cyber incidents increased 200 percent
- NC public sector incident costs average **~$700k-$1.5 million**

Initial Notification – NMAC

NMAC will notify NC Emergency Management for Significant Cybersecurity Incidents
Phone: **855-662-2911** E-mail: **911NMAC.admin@nc.gov**

State Joint Cyber Task Force (JCTF) Next Steps:

NCEM Cyber Lead to establish scoping call with impacted entity & JCTF

State 911 Board

National Guard Cyber Security Response Unit (CSRF)

NCDIT Enterprise Security and Risk Management Office (ESRMO)

Federal Partners (FBI, US Secret Service)

NCLGISA Cybersecurity Strike Team

NC Joint Cyber Task Force

Formalized by EO 254

State & Local Partners

--NCLGISA Cyber Strike Team *(onsite within 12-18 hours)*
--NC National Guard CSRF *(onsite within 12-18 hours)*
--NC DIT
--NC DPS (NCEM Cyber Unit & NC ISAAC)

Federal Partners

--FBI
--US Secret Service
--DHS CISA (Cybersecurity and Infrastructure Security Agency)

Other Partners Based on Impacted Entity

--911 *(any significant impact to PSAPs)*
--NC SBI
--State Board of Elections
--DHHS
--DPI *(for all K-12 engagements)*
--MCNC
--NC Community College System Office *(for all CC engagements)*

Boots on the Ground for Incident Response

Onsite at impacted entity within 4-12 hours of the initial scoping call

Work ~200 hours per significant incident (weekends, holidays, and after-hours are all within scope to get the job done)

Typical Strike Team and NCNG Incident Staffing:

2 people on-site for days 1-2

1-2 people on-site for days 3-6

12-16 hour operational periods when onsite

Syncs every evening for 2-3 hours to review logs, discuss game plans for rebuild during incident response

Team members not on-site are typically reviewing CyberTriage images, logs, etc to perform what we call “sys admin forensic review/threat hunting”

Some events take weeks or months, so those obviously consume more hours (usually after traditional day job hours and on the weekends)

Welcome to the War Room

NCLGISA Cybersecurity Strike Team

A volunteer group of local government IT professionals, working directly with peers to improve cyber posture, reduce risk of exposure/attack, and provide incident response services during events.

Leadership and Core Members

Scott Clark, CIO, Town of Fuquay-Varina

Randy Cress, Assistant County Manager/CIO, Rowan County

Mark Seelenbacher, CIO, Henderson County

Chad Coble, CIO, Stanly County

Ted Norris, Deputy CIO, Onslow County

Logan Steese, CIO, Currituck County

Amy Walker, CTO, Ashe County Schools

Rob Hudson, IT Infrastructure Mgr, City of Greenville

Brian May, CISO, Wake Technical Community College

Chris Puryear, CIO, Person County

Shannon Tufts, UNC SOG Professor

Key Cybersecurity Legislation

G.S. 143-800, amended by SL2021-180

G.S. 143B-1320, amended by SL2021-180

G.S. 143B-1379(c), amended by SL2021-180

Article 84, Various Technology Regulations.

GS143-800: State entities and ransomware payments.

(a) No State agency or local government entity shall submit payment or otherwise communicate with an entity that has engaged in a cybersecurity incident on an information technology system by encrypting data and then subsequently offering to decrypt that data in exchange for a ransom payment.

(b) Any State agency or local government entity experiencing a ransom request in connection with a cybersecurity incident shall consult with the Department of Information Technology in accordance with G.S. 143B-1379.

(c) The following definitions apply in this section:

(1) Local government entity. – A local political subdivision of the State, including, but not limited to, a city, a county, a local school administrative unit as defined in G.S. 115C-5, or a community college.

Cybersecurity Incident Reporting Requirement

G.S. 143B-1379(c), amended by SL2021-180

(c) Local government entities, as defined in **G.S. 143-800(c)(1)**, shall report cybersecurity incidents to the Department. Information shared as part of this process will be protected from public disclosure under G.S. 132-6.1(c). Private sector entities are encouraged to report cybersecurity incidents to the Department.

.

A Significant Cybersecurity Incident…

- **G.S. 143B-1320(a)(14a)** Ransomware attack. – A cybersecurity incident where a malicious actor introduces software into an information system that encrypts data and renders the systems that rely on that data unusable, followed by a demand for a ransom payment in exchange for decryption of the affected data.

- **G.S. 143B-1320(a)(16a)** Significant cybersecurity incident. – A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

  a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information: 1. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or 2. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.
  b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency

Methods of Contact to Report Cybersecurity Incident

- **NMAC:** 911NMAC.admin@nc.gov or (**855) 662-2911** (monitored 24/7)
- **NCLGISA Cybersecurity Strike Team:** itstriketeam@nclgisa.org or (919) 726-6508 (monitored 24/7)
- **NC EM 24 Hr Watch:** 800-858-0368 (monitored 24/7)
- **NCDIT:** https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form

Top Cyber Trends

Trend #1


SOCIAL
ENGINEERING
The clever manipulation
of the natural human
tendency to trust.

Recognize These?

- What was your favorite teacher's name?
- What was the name of your childhood pet?
- What was your childhood best friend's name?
- What was the first car you had?
- Where were you born?
- What was the name of your high school?

Trend #2 & #3

#2: Big Shift in TA Behavior: Data Exfil without Encryption

"When are we gonna stop calling it ransomware? It's just data kidnapping now!"

"LockBit has advised affiliates to exfiltrate & extort, not encrypt."

Data Exfiltration, No Encryption

- Conducted via various tactics (SQL injections or TA access to data within systems)
- Can happen over extended periods of time
- Ransom for data not to be sold/posted
- Recent cases indicate the impacted entity was unaware of the data exfiltration until it was found posted on the internet by a 3rd party
- Breach notification may be required depending on the type of data exfiltrated

Legal Issues with Data Exfil

Most agencies don't have sufficient logging to determine what data was removed

Hard to validate extent of breach notice requirements

#3: Ransomware

Ransomware is a type of malware that attempts to extort money from user or organization by infecting or taking control of the victim's computer, files, servers, etc.

Ransomware usually encrypts files, folders, machines, servers to prevent access and use unless the ransom is paid to receive the decryption key.

Data exfiltration has become more widespread as part of ransomware events in the past 24 months.

Ransomware Attack Timeline

- An employee opens a phishing email and clicks on a link containing ransomware.

M2
- The ransomware downloads onto the employee's computer and starts executing malicious code.

M3
- The ransomware creates a connection via the Internet with the threat actor's command and control (C2) server.

M4
- The ransomware steals/harvests credentials to gain access to more accounts.

M5
- The ransomware looks for files to encrypt on local computers and on servers via the network, moving laterally across the network to compromise multiple accounts. Data exfiltration might also be occurring during this timeframe.

M6
- The ransomware starts the encryption process, typically attacking domain controllers and backups first. The government is now aware they have been compromised. The threat actor leaves a ransom note demanding payment in exchange for the decrpytion key.

Common Attack Vectors

Phishing emails loaded w/ malware

Password brute forcing

Remote Desktop Protocol

VPN exploits

Other unpatched CVEs

- Microsoft applications

Outdated infrastructure

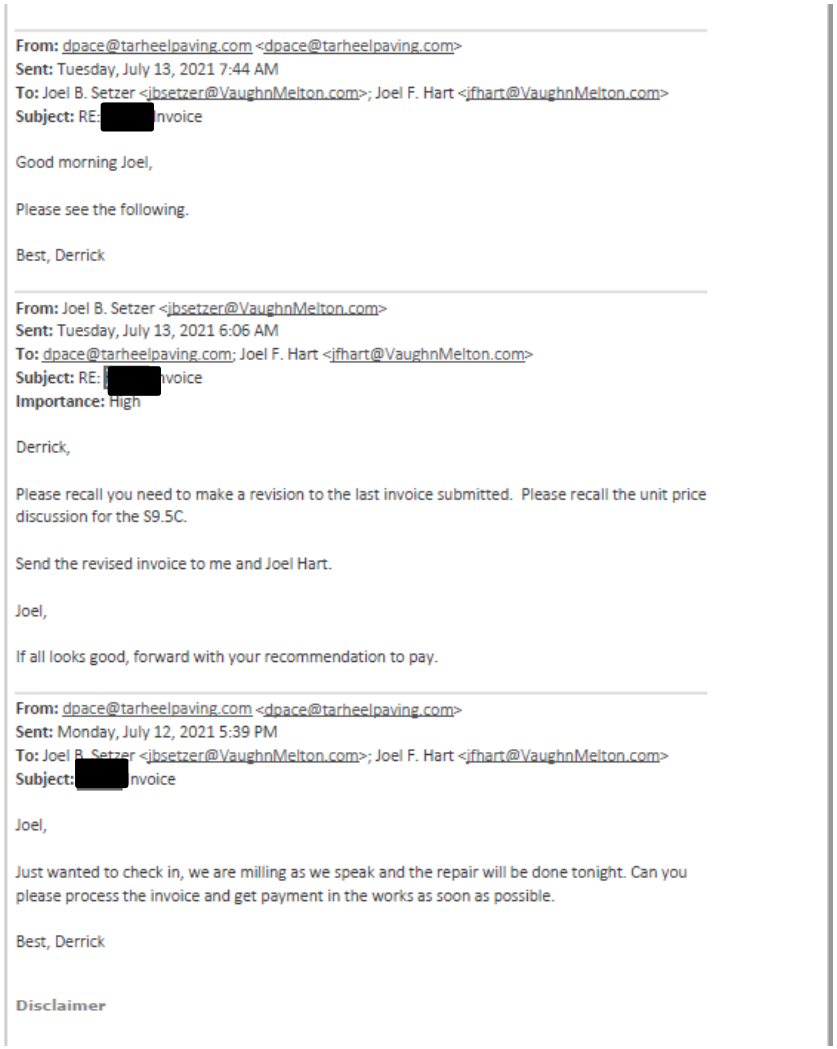
Open ports per vendor instructions

Trend #4


Business Email
Compromise:
The $9 Billion Security
Threat You Can't Ignore

Just a Normal Day…

Making Moves, Processing Payments



From: dpace@tarheelpaving.com <dpace@tarheelpaving.com>
Sent: Tuesday, July 13, 2021 7:44 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: RE: [redacted]nvoice

Good morning Joel,

Please see the following.

Best, Derrick

From: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Sent: Tuesday, July 13, 2021 6:06 AM
To: dpace@tarheelpaving.com; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: RE: [redacted]nvoice
Importance: High

Derrick,

Please recall you need to make a revision to the last invoice submitted. Please recall the unit price discussion for the S9.5C.

Send the revised invoice to me and Joel Hart.

Joel,

If all looks good, forward with your recommendation to pay.

From: dpace@tarheelpaving.com <dpace@tarheelpaving.com>
Sent: Monday, July 12, 2021 5:39 PM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>; Joel F. Hart <jfhart@VaughnMelton.com>
Subject: [redacted]nvoice

Joel,

Just wanted to check in, we are milling as we speak and the repair will be done tonight. Can you please process the invoice and get payment in the works as soon as possible.

Best, Derrick

Disclaimer

What Can Possibly Go Wrong?

Joel

JOEL BETZER, PE | OFFICE LEADER | SYLVA NC OFFICE
C: 828.226.9158 | O: 828.477.4993 | www.vaughnmelton.com
DEPENDABLE | PROACTIVE | CREATIVE | EMPATHETIC | CONSCIENTIOUS
P.E. Registration States: NC, KY, TN, OR, SC

From: Derrick pace <dpace@tarhealpaving.com>
Sent: Tuesday, July 13, 2021 9:30 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Cc: Joel F. Hart <jfhart@VaughnMelton.com>
Subject: Re: FW [redacted] Invoice

Hi Joel/Hart,

Find the attachment for our new bank details and make sure the payment is sent by ACH or Wire Transfer.

Let me know if you need anything else.

Best, Derrick

Disclaimer
The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

On Tue, Jul 13, 2021 at 3:58 PM Joel B. Setzer <jbsetzer@vaughnmelton.com> wrote:

> Joel,
>
> The quantities match the prior invoice. Per your prior email, I am assuming the quantities match your record. Please advise asap if there are any differences.
>
> Seth,
>
> We are hoping to close out the fiscal part of the project to assist with County accounting processes. The last discussions were mid-June. At the time, the concrete had passed testing and we were awaiting the asphalt testing results. Can this be expedited as it is needed to get closure?

Seems Good to Me… So Let's Cut That Check!

From: Marcus [redacted]
To: Samantha [redacted]
Cc: Randall [redacted]
Subject: FW: Tarheel Invoice - Recommendation to Pay
Date: Friday, July 16, 2021 4:40:25 PM
Attachments: image001.png
Paving & Asphalt Bank Details.pdf

Sam,

Next week we should get the approved invoice from Tarheel for the paving project at Solid Waste. The contractor's payment information is attached and note the highlighted information below from the engineer regarding timing for the work completed; I agree.

Thanks and please let me know if you have any questions,
Marcus

From: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Sent: Wednesday, July 14, 2021 1:34 PM
To: Marcus [redacted].gov>
Cc: Joel F. Hart <jfhart@VaughnMelton.com>
Subject: Tarheel Invoice - Recommendation to Pay

Good Afternoon,

We have evaluated the testing reports on the asphalt pavement. All aspects of the reports indicate full compliance with NCDOT specifications, except the density achieved on the surface (S9.5C) mix. The density requirements for this mix is 92% and they achieved an average of 90.9% on the four areas. Area 1, which carries the highest volume and weight of trucks did get a 92.0% density.

NCDOT does have waivers for "small quantities" which would also apply.

Given that the asphalt is in specifications in all other categories and given the highest volume area is meeting density, it is my recommendation to accept the work and pay Tarheel the invoice.

In regards to what was done before June 30 and after, all of this work was done prior to June 30. The slipped area repaired did not create any new pay quantities because it was basically warranty work.

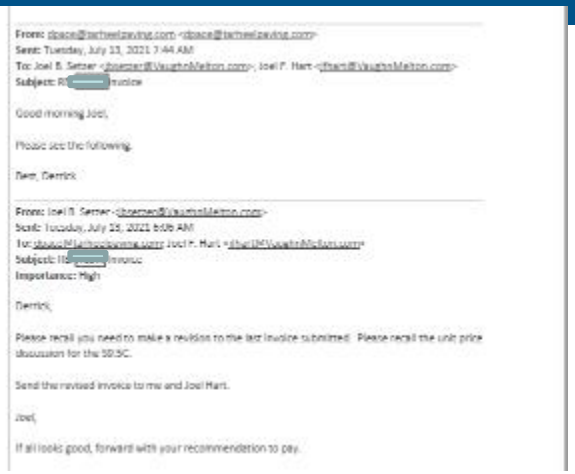
My recommendation is based upon an assumption that the repaired slipped area is still performing well. If it is not, please let me know.

Let me know if we need to discuss any of this information or the recommendation.

Thanks,

But Things Weren't As They Appeared

Did You Catch It?



Good morning Joel,

Please see the following.

Best, Derrick

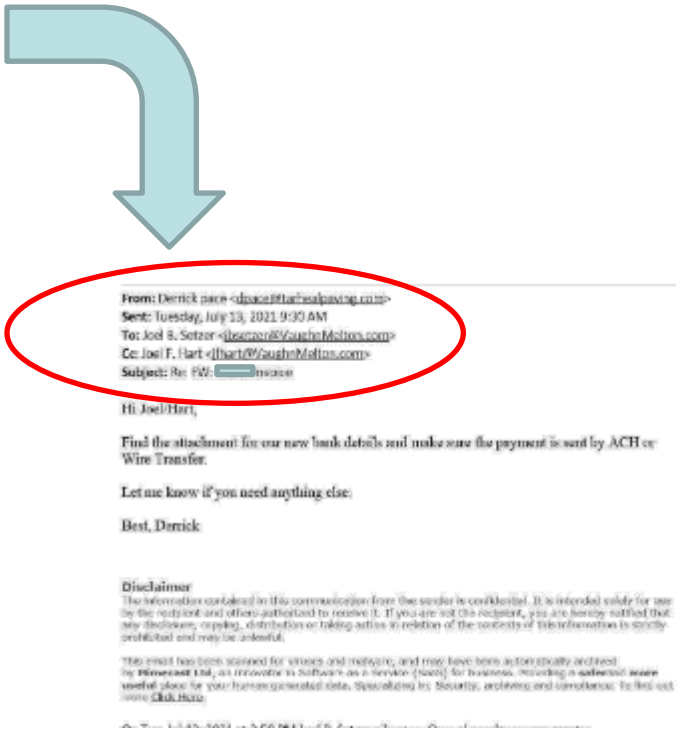
Derrick,

Please recall you need to make a revision to the last invoice submitted. Please recall the unit price discussion for the SD:SC.

Send the revised invoice to me and Joel Hart.

Joel,

If all looks good, forward with your recommendation to pay.



From: Derrick pace <dpace@tarheelpaving.com>
Sent: Tuesday, July 13, 2021 9:30 AM
To: Joel B. Setzer <jbsetzer@VaughnMelton.com>
Cc: Joel F. Hart <jfhart@VaughnMelton.com>
Subject: Re: FW: [redacted] invoice

Hi Joel/Hart,

Find the attachment for our new bank details and make sure the payment is sent by ACH or Wire Transfer.

Let me know if you need anything else.

Best, Derrick

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

Business email compromise scams & direct deposit scams are preventable.

Question everything

Require a formal process for changes, including physical confirmation

Ask IT to review before changes are made

#5: Third-Party Vendor Breaches

Security lapse left information on NC students vulnerable, district says

WSOCTV.com News Staff

October 21, 2022 · 1 min read

A lapse in security by a third-party vendor left the private data of students across North Carolina unsecured and vulnerable, according to Union County Public Schools.

A letter sent to parents earlier this week made them aware that students' records from multiple school districts and charter schools, including Union County, were left unsecure in a cloud-based storage space called iLeadr.

The North Carolina Department of Public Instruction discovered the information was susceptible over the summer, the message said. At the time, it was not clear which records had been disclosed, but a state cybersecurity taskforce investigation confirmed UCPS files were accessible.

CYBERSECURITY

Police Software Vendor Breach Exposes Personal Data, Raid Plans

Hackers reportedly stole nearly 20GBs of data from police agency vendor ODIN Intelligence, including personal information on suspects and convicted sex offenders as well as plans for upcoming police raids.

January 25, 2023 · News Staff

Contract Language to Include

Breach Notice/Cost Language

Breach Notification and Associated Costs: Where a breach or unauthorized release, as defined in NCGS 75-65 or in any other state or federal regulation, is attributed to a third-party vendor/contractor, the third-party entity shall pay for or promptly reimburse XXX entity for the full cost of the notifications, including any associated legal fees, either through the third party's cyber liability insurance provider or through their own entity funds.

COI Requirement

RFP Requirement for All Software-Based Services, Vendors Supporting Systems, etc.

Cyber Insurance: The contractor shall maintain cyber liability in the minimum amount of $1,000,000 per occurrence, including third-party coverage for incidents or associated impacts caused directly or indirectly by said vendor.

Insurance Coverage?

Notice with Reservation of Rights

Deny Claims for Out-of-Pocket Costs

Need Indemnity in Contract Language

Cloud Provider Risk Assessments via Insurance

- Pre-existing conditions

Security Requirements in Contracts

- Evidence of SOC II Certification
- Other attestations (use of State Vendor Readiness Assessment Report or similar tools)
- Security Scorecard

What Can You Do To Protect Yourself and Your Organization?

Recommendations for Non-IT Staff

1. If you suspect ransomware, contact your IT department immediately! They should start severing all Internet-based connections asap.

2. Don’t turn off your computer/server, just disconnect it from the Internet (ethernet and wireless)

3. Do not try to stay up and “functional”, as it will allow for rapid, catastrophic proliferation across your networks and into any interconnections you might have with neighboring entities. ** No, you cannot just turn on your computer really quickly and insert a flash drive for those files you really need.

4. Use strong passwords (and unique ones) plus MFA (multifactor authentication) in your organization and personally.

5. Do not allow vendors to have open tunnels into your environment for remote support. Use a documented process for external access.

6. Do not use the same credentials for domain, system or software administration and your local accounts. Many of the recent breaches have involved compromised domain administrator credentials, which often are found to be the same as cached local administrator credentials.

7. Ask for immutable backups that are stored physically and virtually apart from the network for critical systems. After attacking the domain controller(s), most current variants go straight to encrypting your backups.

8. Determine what servers contain sensitive data (PHI, PII, financial data, CJIS data, etc) and keep this on file outside of the network.

9. Know your cyber-liability insurance policy well and have conversations with them prior to an event to determine their standard course of action (preferred vendors, etc).

10. Require user education for phishing messages and aggressive response to mitigate anyone who falls for phishing. Exposed credentials and malware downloads are part of the problem and can be limited with proper education.

11. Create a Continuity of Operations plan for your entity including defining who will serve as Incident Commander and drill it to make sure it works for your team!

12. Work with senior leadership to create a prioritization document for bringing departments/applications back online.

NC 9-1-1
CISA CYBER RESOURCES AND TECHNICAL ASSISTANCE

Resources & Tools

Publications

Public Safety Communications Dependencies on Non-Agency Infrastructure and Services

Cyber Risks to 911 Fact Sheet: Telephony Denial of Service

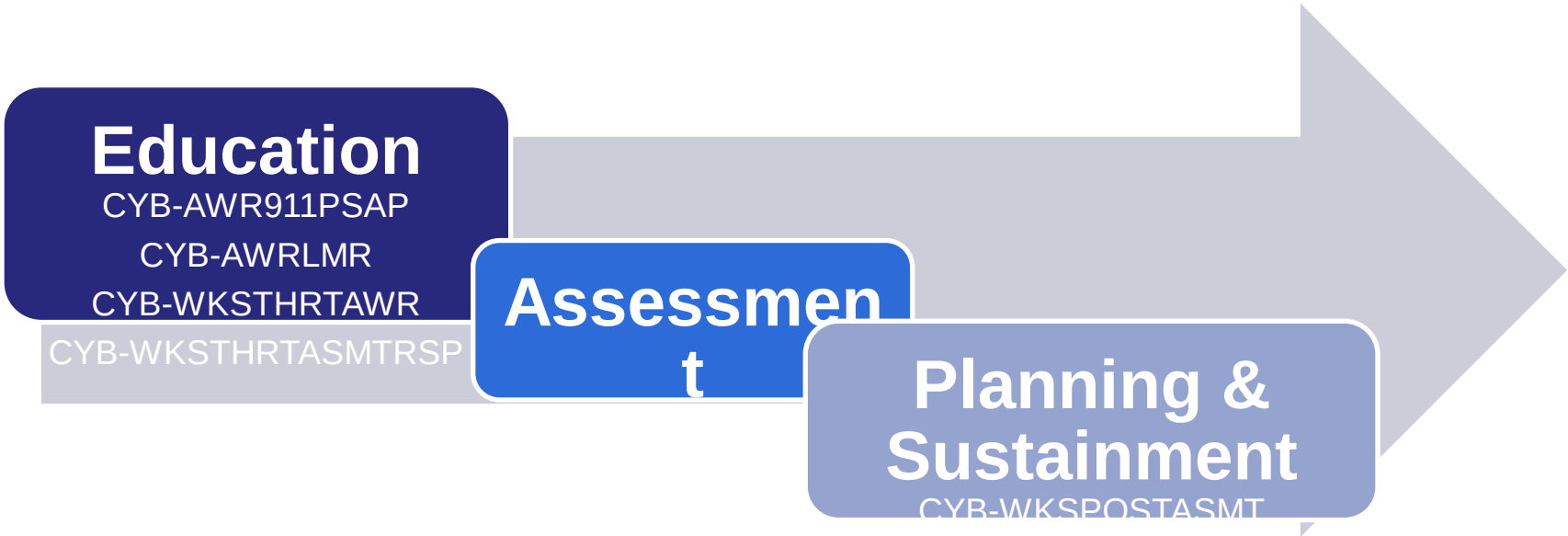
Cyber Risks to 911 Fact Sheet: Ransomware

Communications Resiliency Toolkit

- 30 resources over 10 topic areas
- Expandable and maintained as a living site
- Includes CISA guidance and guidance from other trusted resources

- cisa.gov/safecom/resources

ICTAP Cyber Offerings



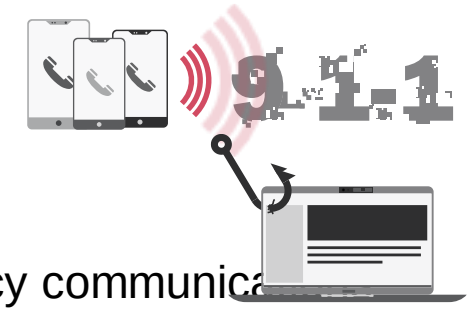
- CYB- offerings replace existing “blanket” OP-911PSAPCYBER Work Order category
- Additional Self Assessment & Continuous Monitoring Training(s) to be implemented as a future webinar offerings

9-1-1/PSAP Cyber Awareness Webinar (CYB-AWR911PSAP)

Education

Offering Overview: Introduces public safety communications sta common cybersecurity threats and vulnerabilities affecting 9-1-1/PSAP/ECC environments

- Ransomware attacks and their impact
- Telephony Denial of Service (TDoS) attacks against administrative lines and 9-1-1
- Exposed networks and devices
- Why individual logons and password protection is critical
- Cryptojacking and email phishing
- Basic best practices to improve the secure use of emergency communica technologies
- Guidance on responding to and reporting cyber incidents



TA Delivery Methods	In Person, Workshop, or Online Webinar
Recommended Participants	SWICs, State 9-1-1 Coordinators, Dispatchers, Call Takers, 9-1-1 Operators/ECC/PSAP Managers and System Operators

LMR CYBER AWARENESS WEBINAR (CYB-AWRLMR)

Education

Offering Overview: Introduces radio system owners to common cybersecu
vulnerabilities affecting Land Mobile Radio environments

- Ransomware attacks and their impact
- Exposed networks and devices
- Why individual logons and password protection is critical
- Cryptojacking and email phishing
- Basic best practices to improve the secure use of emergency communications technologies
- Guidance on responding to and reporting cyber incidents

TA Delivery Methods	**In-Person, Workshop, or Online Webinar**
Recommended Participants	**SWICs, ECC/LMR Managers and System Operators**

ONE-DAY CYBER AWARENESS WORKSHOP (CYB-WKSTHRTAWR)

Education

Offering Overview: This workshop is focused on helping PSAP leadership and emergency managers understand the common cybersecurity threats and vulnerabilities affecting PSAP and LMR environments. This class also discusses best practices to secure their daily operations and govern third party service providers. The day will end with an exercise meant to reinforce the learning objectives delivered.

***NOTE**: The session is not meant to be technical. IT personnel are welcome; however they may find the content to be remedial.*

TA Delivery Methods	❖ **In-Person, Instructor Led Training**
Recommended Participants	❖ **SWICs, State 9-1-1 Coordinators, 9-1-1 Operators/ECC/PSAP/LMR Managers and System Operators**

TWO-DAY THREAT ASSESSMENT AND RESPONSE WORKSHOP (CYB-WKSTHRTASMTRSP)

Education

Offering Overview: This workshop is focused on helping PSAP leadership and emergency managers learn how to develop a Cyber Incident Response Process and develop Cyber Incident Response Plans. To help the participants understand the nature of these incidents, the instructors will conduct several live demonstrations of different cyber-attacks including phishing/credential harvesting, ransomware, business email compromise, etc.

The second day of the workshop will begin with an overview of a typical Cyber Incident Response Plan. This will be followed by a discussion regarding the connection CSIRP and Continuity of Operations Planning. The remainder of the day will be used to help participants use the template to build a response plan for a ransomware attack.

***NOTE**: The session is not meant to be technical. IT personnel are welcome; however they may find the content to be remedial.*

TA Delivery Methods	❖ **In-Person, Instructor Led Training**
Recommended Participants	❖ **SWICs, State 9-1-1 Coordinators, 9-1-1 Operators/ECC/PSAP/LMR Managers and System Operators**

FULL CYBER ASSESSMENT (CYB-ASMTFULL)

Assessment

Offering Overview: Provide organizations with an in-depth understanding of their cyber security posture through a representative sampling process (e.g., sites, personnel, systems, and documentation) to aid in planning security management efforts.

The assessment consists of a review of LMR or PSAP target systems' security mechanisms against the **complete LOW Baseline** security control set using the nationally-recognized best practice guidelines NIST SP 800-53 revision 5. The control set will be tailored depending on the needs of the agency and system being assessed. Additional controls may be added to support systems that store, transmit or process sensitive data or privacy information, or state/county regulations.

This technical assistance provides 9-1-1/PSAP managers and LMR system owners with critical information for improving the cyber security posture of their systems. The resulting report can also serve as a foundation to assist in developing action plans, refining strategic plans, developing budgets, and developing staffing requirements.

TA Delivery Methods	❖ **In Person Assessment and/or Webinar**
Recommended Participants	❖ **SWICs, 9-1-1/ECC, and PSAP Managers or LMR System Owners**

RAPID CYBER ASSESSMENT (CYB-ASMTRAPID)

Assessment

Offering Overview: Provider organizations with a high level understanding of their cybersecurity posture through a representative sampling process (e.g., sites, personnel, systems, and documentation) to aid in planning security management efforts.

The assessment consists of a review of LMR or PSAP target systems' security mechanisms against a subset of critical or key security controls selected to assess the overall security posture of the 9-1-1/PSAP/LMR environment. The control set consists of **69 NIST separate controls** from the NIST SP 800-53 revision 5.

This technical assistance provides 9-1-1/PSAP managers and LMR system owners with critical information for improving the cyber security posture of their systems. The resulting report can also serve as a foundation for engaging CISA in a Full Assessment of their system(s), developing action plans, refining strategic plans, developing budgets, and developing staffing requirements.

TA Delivery Methods	❖ **In-Person, Workshop, or Online Webinar**
Recommended Participants	❖ SWICs, ECC/LMR Managers and System Operators

POST ASSESSMENT WORKSHOP (CYB-WKSPOSTASMT)

Planning & Sustainment

Offering Overview: This offering is designed to help a recent recipient of a Cybersecurity Assessment (either CYB-ASMTRAPID or CYB-ASMTFULL) develop a plan of action to address any findings which require attention. Delivery begins with an in-person workshop and is followed by up to 12 weeks of mentoring conducted over webinar/phone.

TA Delivery Methods	❖ **In Person Workshop and Virtual Meetings**
Recommended Participants	❖ **PSAP Managers or LMR System Owners**

CISA Cyber Tools

- Each State has a Cyber Security Coordinator (CSC) and at least 1 Cybersecurity Advisor (CSA)
  - CISA cybersecurity personnel can work with the State and local agencies for onsite training and assessments
- The CISA website has a significant number of documents to help prepare for, respond to and mitigate the impact of cyberattacks.
  - CISA.gov
- If you need more information, please reach out to the CISA ECC, Pam Montanari and she can work with you.

Vulnerability Scanning / Hygiene

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

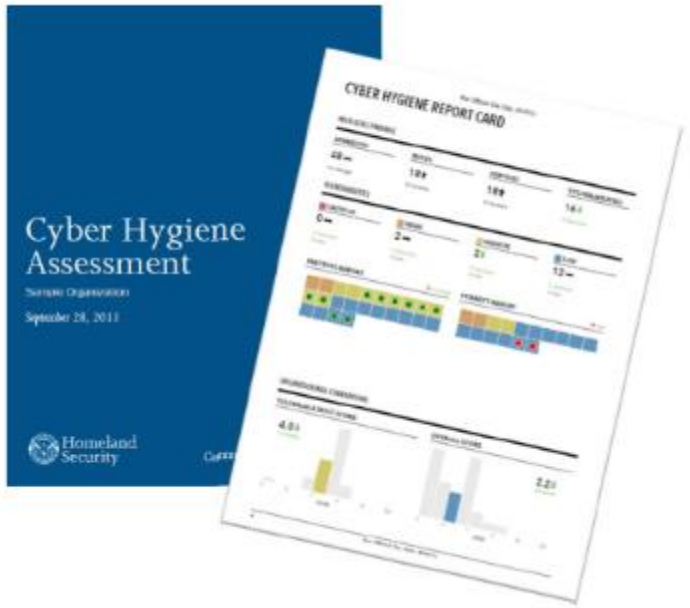
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

Network Vulnerability & Configuration Scanning:

- Identify network vulnerabilities and weakness



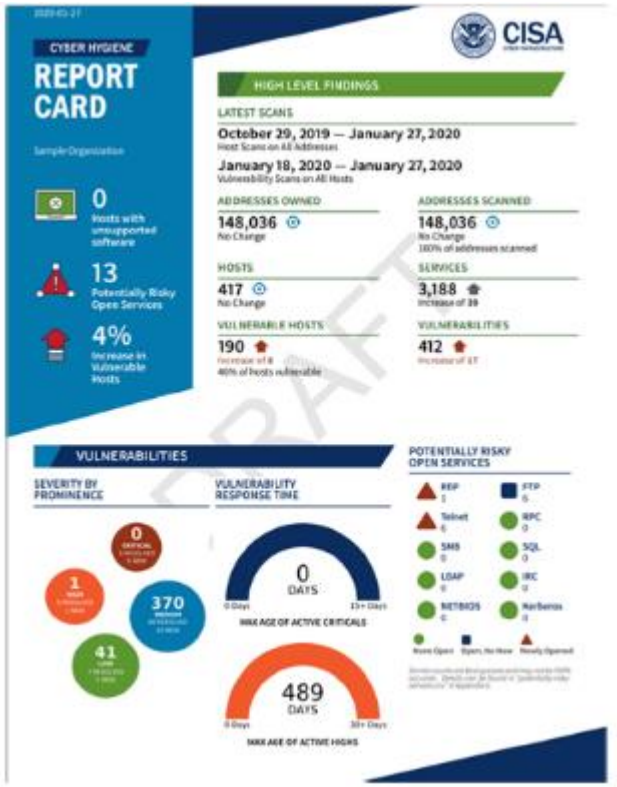
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



Contact: Vulnerability@cisa.dhs.gov to enroll!

CSET Tool

CSET is a self-assessment tool that agencies can download and use to assess their readiness

- Version 10.3 Added the Ransomware Readiness tool for 9-1-1
- Version 11.5 Added the LMR Module
- Access and Download 11.5
  - Releases · cisagov/cset (github.com)

SAFECOM NATIONWIDE SURVEY

The **SAFECOM Nationwide Survey (SNS**) is an online survey that helps assess nationwide emergency communications capabilities

SNS Data Can Help Your Organization:

- Make ***data-driven*** decisions
- Shape policy and ***funding*** decisions
- ***Tailor*** programs and services
- Bring awareness of ***capabilities and gaps***

Take Action!

- ✓ **Complete the survey**
- ✓ **Spread the word**
- ✓ **Reach out to CISA with questions**

cisa.gov/sns **sns@cisa.dhs.gov**

The SNS is Now Open!

Complete the survey by **July 21, 2023** to influence the future of emergency communications!

- Visit **CISA.gov/SNS** to learn more about accessing the survey!
- Submit questions to SNS@cisa.dhs.gov

SAFECOM NATIONWIDE SURVEY

Pam Montanari
Emergency Communications Coordinator
Pam.montanari@cisa.dhs.gov

Questions?

Hotwash

All Players and Observers are encouraged to comment!

Questions


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY