Cybersecurity Tabletop Exercise  
(TTX)

April 27, 2018
Exercise Facilitators

David Stern | Robert Briggs | Richard Sisler
U.S. Department of Homeland Security
National Cybersecurity and Communications Integration Center (NCCIC)
National Cyber Exercise and Planning Program (NCEPP)
Security Protocol

- Traffic Light Protocol (TLP): **GREEN**

- Recipients may only share TLP: **GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

- For reference purposes and additional information on TLP: [https://www.us-cert.gov/tlp](https://www.us-cert.gov/tlp)
Agenda

- Module 1 – Information Sharing
- Module 2 – Incident Identification and Incident Response
- Hotwash and Closing Comments
Exercise Purpose

- An exercise demonstration based on a breach of Personally Identifiable Information (PII) that incorporates discussion focused on information sharing, incident identification, and response.
Exercise Scope and Structure

- Facilitated discussion/tabletop exercise.

- Modules will begin with a summary of key events, followed by guided discussion.

- Parameters
  - Focus on cyber causes and impacts rather than physical response.
  - Discussion will be non-technical.
Exercise Objectives

1. Discuss the preparedness of TAGITM member entities to respond to and manage a cyber incident;
2. Explore processes for identifying potential cybersecurity incidents or issues;
3. Examine communication and information sharing processes within and amongst TAGITM membership and state and federal partners;
4. Explore processes for requesting additional incident response resources once internal resources are exhausted; and
5. Discuss public information policies and procedures.
Participant Roles and Responsibilities

- **Players** participate and respond to the situation presented based on expert knowledge of current plans, policies and procedures, as well as insights derived from training.
- **Observers** support the group in developing responses to the scenario during the exercise, but are not a central part of the exercise discussion.
- **Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required.
- **Evaluators** document player discussion. Facilitators may also serve as Evaluators.
Exercise Guidelines

- This is a open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans, capabilities, and insights derived from your training.
- Decisions are not precedent setting.
- Issue identification is not as valuable as suggestions and recommended actions for improvement.
- Avoid using acronyms.
Assumptions and Artificialities

- The exercise is an opportunity to evaluate capabilities, plans, systems, and processes.

- There is no “hidden agenda,” nor are there any trick questions.

- The exercise scenario is plausible, and events occur as they are presented.
Evaluation and Quick Look Report

- Each participant will be asked to complete a Participant Feedback Form.

- NCEPP will document the exercise discussion.

EXERCISE DISCUSSION
MODULE 1: INFORMATION SHARING
March 12, 2018

- The Multi-State Information Sharing and Analysis Center (MS-ISAC) publishes an alert.

- The alert addresses a phishing campaign targeting state and local governments, as well as municipal utilities.

- The Alert explains that the phishing campaign has allowed an unknown party to steal Personally Identifiable Information (PII) and other sensitive information from the affected entities.

- Through harvesting legitimate account credentials, the attackers were able to masquerade as privileged users and obtain this information.
TO: All MS-ISAC Members, Fusion Centers, and IIC

MS-ISAC ADVISORY NUMBER:
2018-06AD4

DATE(S) ISSUED:
03/12/2018

SUBJECT:
Phishing Campaign Targeting State Governments, City Departments and Agencies, and Utilities

OVERVIEW:
A phishing campaign has been observed targeting a wide variety of state and local governments, City Departments and Agencies, as well as municipal utilities handling large volumes of personally identifiable information (PII). The nature of the email messages associated with this phishing campaign vary widely, but usually employ social engineering tailored to the targeted individual or entity. All reported instances of phishing associated with this campaign include the use of a malicious link or attachment. The emails appear to come from an automated notification system with the general theme of expired account passwords. The emails notify users that their account credentials have expired and direct them to update their passwords immediately or risk account deactivation. The emails generally provide a URL that masquerades as a legitimate login page familiar to the user and prompts the user to enter a new password along with their previous login credentials. This allows the attacker to harvest credentials and gain remote access to the host machine. Using legitimate credentials, the attacker attempts to escalate privileges or use privileged accounts to gain further access to a victim network in order to obtain proprietary data, including PII.

RISK:
Government:
- Large and medium state government entities: High

Businesses:
- Large and medium business entities: High
- Small business entities: High

RECOMMENDATIONS:
We recommend the following actions be taken:
- Remind users to only open email attachments from known users.
- Inform and educate users regarding threats posed by hyperlinks contained in emails or attachments, especially from untrusted sources.
April 1, 2018

- Local media reports begin to emerge detailing rumors of a data breach in a nearby city.

- The report leads to rumors on social media.

- Users speculate that the city’s utility billing and payment system has been compromised, leading to the exfiltration of large volumes of customer PII and payment information.
City Utility Breached

Reports are circulating that yesterday afternoon a Texas city’s energy provider was breached. TX Energy is a publicly owned utility providing electrical power to a number of cities in Texas. TX Energy is the United States’ 10th largest public utility, serving more than 415,000 customers and more than one million residents (as of 2015) within a service area of approximately 400 square miles (643 km), including multiple counties in the State.

Our sources report that TX Energy’s network was breached leading to exfiltration of data from their network, including customer personally identifiable information. Details about the breach are scarce but updates will be provided once more information is known including the extent of the breach and how many customers are affected. We have not received official notification confirming the breach but have reached out to the mayor’s office for comments. Our contacts have reported that Austin Energy has contacted the local FBI and other law enforcement agencies in the past few hours to request assistance.

In the past, companies who have been the subject of similar breaches involving personal information have provided customers with identity theft monitoring. Potential victims may want to consider putting credit freezes on their accounts and should monitor their credit reports for suspicious activity.
A series of emails have been sent to employees that access your organization’s municipal utility billing system, as well as end users, stating that the users’ passwords have expired.

A link is provided where the recipients are told to update their login information.
The local police department receives a series of emails from Texas Rangers requesting data related to an ongoing investigation.

The emails include PDF attachments detailing their requests.
Some police employees open the email attachments while others report the emails as phishing attempts.

In addition, over the last several days, some utility billing system users clicked the links provided, entering account information when prompted.

Others reported the emails as suspicious to the utility’s customer service email address.
Module 1 Discussion
Summary

- MS-ISAC publishes an alert regarding a phishing campaign targeting state and local governments, as well as municipal utilities.

- Local media reports emerge detailing rumors of a data breach in a nearby city, rumors circulate that a municipal utility billing and payment system has been compromised.

- A series of emails are sent to employees that access your organization’s municipal utility billing system, as well as end users, stating that the users’ passwords have expired (with embedded link).

- The local police department receives a series of emails from Texas Rangers requesting data related to an ongoing investigation (with PDF attachment).
Discussion Questions

1. What personnel in your organization would receive the alert detailed in this scenario?
   – Through what channels would this information be received and disseminated?
   – Would the information be shared with other departments or organizational leadership?
   – What actions, if any, would your organization take based on this information?

2. Who is responsible for collating information across multiple reports and sources?

3. What other threat information does your organization regularly receive (e.g., information from DHS/NCCIC, FBI/Infragard, Multi-State Information Sharing and Analysis Center (MS-ISAC), United States Secret Service, open source reporting, or security service providers)?
4. What information would you share with the following:
   – Incorporated townships or surrounding cities and counties?
   – Private sector entities?
   – The Federal Government or non-governmental organizations (e.g., MS-ISAC)?
   – Do you have information sharing relationships with any of the above?

5. Would citizens and employees know where to report suspected phishing attempts related to your organization or the services it provides? How would you become aware of the phishing attempts?
Discussion Questions

6. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
   – How often is training provided? Does it cover:
     • Review of department, and/or agency acceptable use and IT policies,
     • Prominent cyber threat awareness,
     • Password procedures, and
     • Whom to contact and how to report suspicious activities?
MODULE 2: INCIDENT IDENTIFICATION AND RESPONSE
A police employee has trouble logging in at their workstation and calls IT Support.

IT looks into the issue and notices the user’s account no longer exists.

After verifying that the user is a police employee, IT discovers that the user account in question was recently deleted.

After further inspection, multiple changes were made in Active Directory including the creation of new user accounts and granting of privileges to the new and existing user accounts.
A security researcher discovers a post on the dark web where a forum user claims to have compromised your organization’s municipal utility billing system as well as sensitive police records.

They claim to have stolen a large amount of PII belonging to citizens, and are willing to sell it for “the right price” alongside proprietary law enforcement records.

The user has provided a small number of data records to verify their claims.
The information appears to include citizens’ social security numbers, dates of birth, and addresses in addition to credit card data and bank account information.

One police record posted pertains to an ongoing investigation.

The researcher contacts local elected officials and law enforcement to make notification of their discovery.
Today I discovered some concerning news relating to your employees/customers. On the popular 1127NewsOn forum, a thread popped up where one user is allegedly selling Personally Identifiable Information (PII), which appears to include users of your city's utility billing system. The information includes name, billing address, phone numbers, payment information, SSN, and account information. Additionally, I was able to locate on this forum some sensitive police records, with one record pertaining to an ongoing police investigation. The seller is actively advertising the file, and it has already been sold to a forum member. There are a few interested parties, along with others just curious about how the information was obtained. The user selling the information didn’t make clear from whom they got the information, so no mention of a specific exploit or vulnerability used. But they did provide a PII file to verify their claim, and from my research they appear authentic.

Here is a screen grab of the forum for review:

Leaving you guys know so you can perform an internal investigation to further verify this claim and notify your folks.

Regards,

Darnimy Joolay

SecurityPatch+
Local media reports lead to social media rumors that your organization has been "hacked." Citizens demand information regarding whether or not they were affected by the utility billing system compromise.

The police department is overwhelmed with media inquiries regarding the potential release of sensitive law enforcement records.
Dear Public Information Officer,

GNN would be very interested in obtaining an official comment to the recent report regarding the potential release of sensitive law enforcement records within your department.

PLEASE respond!

Sincerely,
B Smith
GNN News
Module 2 Discussion
Summary

- A police employee has trouble logging into their workstation. IT discovers the employee’s account was recently deleted.

- Changes were made in Active Directory, including the creation of user accounts and changes to account privileges.

- A security researcher discovers a post on the dark web where a forum user makes claims of compromising your organization’s municipal utility billing system and sensitive police records.

- Local media reports lead to social media rumors that your organization has been “hacked,” and the police department is overwhelmed with inquiries.
Discussion Questions

1. What level of leadership/management would be notified at this point in the scenario? Is there a process or plan in place detailing the thresholds at which different notifications are made and what information is provided?

2. What response actions would the IT/IS department have taken at this point? Are these actions driven by a plan?
Discussion Questions

3. Do you have personnel tasked with incident response or a designated cyber incident response team?

– If so, what threshold must be reached for the cyber incident response personnel to be activated? Does this scenario reach that threshold?

– Who is responsible for activating or has authority to activate the cyber incident response personnel and under what circumstances?
Discussion Questions

– What would be the cyber incident response team/personnel’s roles and responsibilities?

– How do response processes differ based on whether a given information system is operated by a 3rd party vendor as opposed to your organization?
Discussion Questions

4. What are your public affairs concerns? Who is responsible for coordinating the public message? Is this process a part of any established plan?

   – What information are you sharing with citizens? employees? regulators? media?
   – Are public information personnel trained to manage messaging related to cyber incidents? Are they trained to manage your organization’s social media presence?

5. What is your primary concern? Mitigation of the incident (resolving the issue) or investigation (preserving the evidence to build a criminal case)? Who would make this decision? Are these mutually exclusive?
Discussion Questions

6. How would your organization verify the security researcher’s claims and confirm authenticity of the data records in question?

7. If it is confirmed the records originated with your organization, what additional actions are taken? Are any of these actions legally required?
   – Breach notification to citizens and employees?
   – Provision of identity theft monitoring?
   – Use of cyber/breach insurance?
Hotwash

- Strengths
- Areas for Improvement
- Next Steps

Please complete your feedback forms!
Contact Us

David Stern
DHS NCEPP
(703) 235-5692
David.Stern@hq.dhs.gov

Richard Sisler
DHS NCEPP
(703) 883-8861
Richard.Sisler.2@associates.hq.dhs.gov

Robert Briggs
DHS NCEPP
(703) 235-2895
Robert.Briggs@associates.hq.dhs.gov

NCEPP
CEP@hq.dhs.gov

TAGITM
Texas Association of Governmental Information Technology Managers

TLP: GREEN