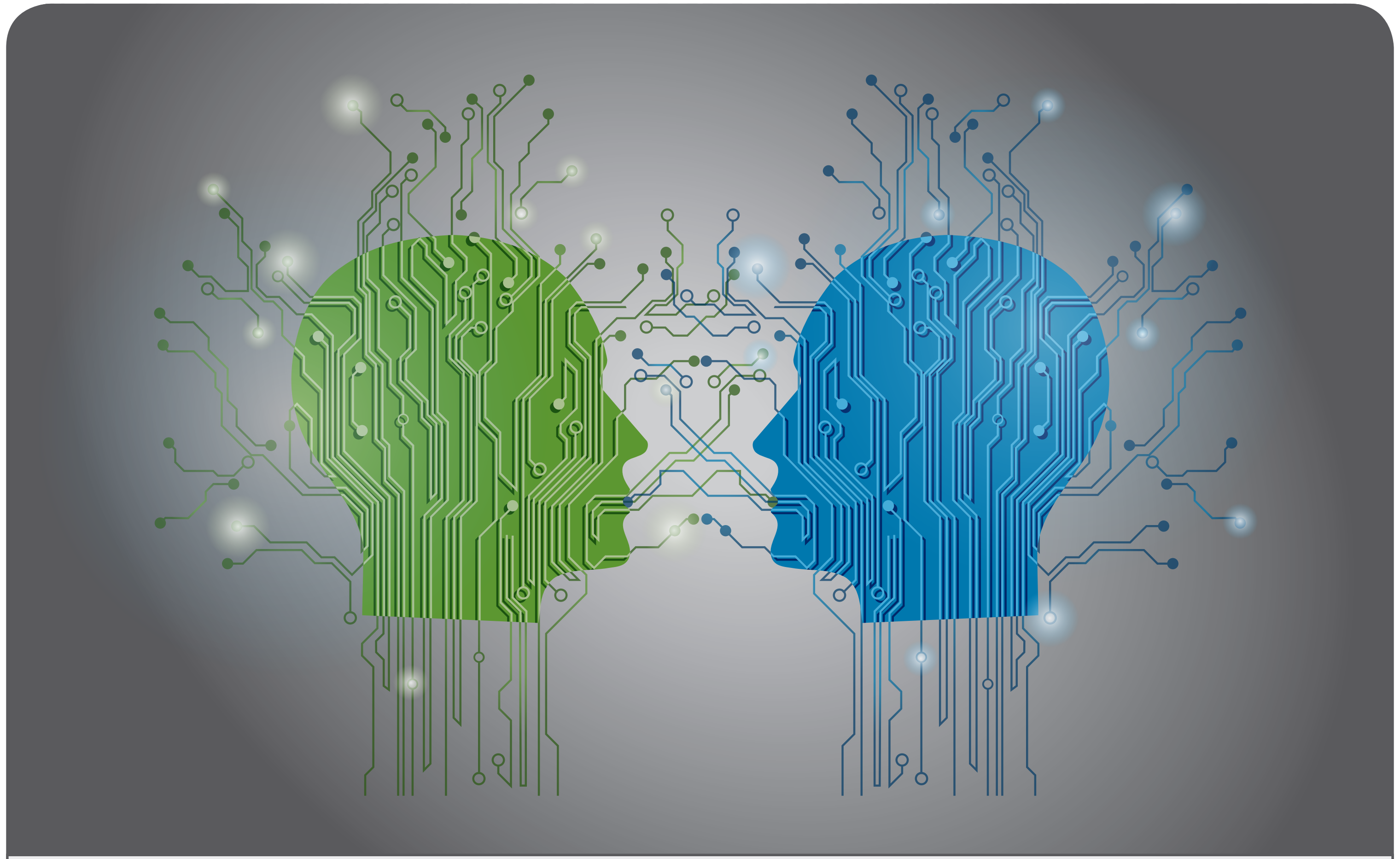
Discussion Questions (Senior Elected Officials)

1. What is your role Do you pay the ransom?
   a. Who decides?
   b. What's the process?
   c. What are the advantages/disadvantages to paying?
   d. What are the political ramifications?
   e. What outside partners/entities do you need to contact?
2. What capabilities and resources are required for the response to this cyber incident?
   a. What internal resources do you depend on? Are your current resources sufficient?
   b. Whom do you contact if you're in need of additional third-party assistance?
   c. Do you have personnel tasked with incident response or a designated cyber incident response team at your department and/or at the regional level?
3. What elements of your organization are involved in the cyber incident response?
   a. Who is responsible for coordinating these elements?
   b. Is this process part of your formal plan?
   c. Is it exercised regularly?
4. What are your organization's priorities in relationship to the scenario?
5. What processes are used to contact critical personnel at any time, day or night?
   a. How do you proceed if critical personnel are unreachable or unavailable?
   b. Has the process been tested?
6. What is your organizations process for knowing when and how to notify law enforcement?
   a. What are the advantages and disadvantages of notifying law enforcement?
7. Does your organization monitor social media?
   a. How do you respond to threats identified on social media platforms?
   b. Is your Public Information Officer trained to monitor social media platforms or another dedicated employee?

Contact

For questions or to learn more about the DHS National Cyber Exercise and Planning Program (NCEPP), please contact: *CEP@hq.dhs.gov* | (703) 235-5641

Homeland Security



State of Washington Homeland Security Region V: Blue Hat Cybersecurity
Tabletop Exercise

May 23, 2019

Exercise Purpose:

Examine the ability of Washington State Homeland Security (HLS) Region V stakeholders to coordinate, collaborate, and validate their continuity of operations plans, policies, and processes while responding to a significant cyber incident.

Objectives:

1. Increase senior official's cybersecurity awareness to include cyber risk management, cyber-related planning, and other issues related to cyber incident prevention, protection, response, and recovery of critical systems.
2. Assess cybersecurity integration into an organization's all-hazards preparedness.
3. Examine cybersecurity incident information sharing, escalation criteria, and related courses of action.
4. Review internal and external cyber resource requests and management processes within the Region.
5. Review, discuss, and validate the State of Washington Homeland Security Region V Draft Cybersecurity Resilience Concept of Operations (CONOPS).

U.S. Department of Homeland Security

MODULE 1: Information Sharing

March 31, 2019

A Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) National Cybersecurity and Communications Integration Center (NCCIC) Alert is released detailing a spear-phishing campaign which seeks to compromise both networks and servers in the education and healthcare sectors. The alert references a previously published Technical Alert (TA) detailing a type of malware that creates a backdoor within vulnerable systems, allowing intruders to manipulate or extract data.

April 6, 2019

The Multi-State Information Sharing and Analysis Center (MS-ISAC) shares an alert from the DHS CISA NCCIC detailing a spear-phishing campaign targeting state, regional, and local governments, as well as various sectors, to include healthcare and education. The alert explains that the campaign allows an unknown party to steal Personally Identifiable Information (PII) and other sensitive information through harvesting legitimate account credentials and masquerading as privileged users.

April 9, 2019

A local news station airs a story on the impact of a cyber attack occurring in Northwest Oregon. In the story, a local government official said, “we just weren’t prepared to handle an incident like this. We weren’t prepared at all.”

After seeing the news story on the breach in Northwest Oregon, concerned citizens in your region begin contacting their elected officials to ask what is being done to protect them from similar incidents and questioning their preparedness level for potential similar cyber attacks.

Discussion Questions (IT/Professional Staff)

1. Who is responsible for collating information across your organization and/or the region?
2. Describe how your organization would share this type of information.
3. Does your incident response plan or policies/procedures include a communications plan detailing the thresholds at which different internal and external notifications are made, to whom they are made, and what information is provided?
   a. Does it include public messaging requirements?
   b. Does it identify what information is needed from which departments to craft the public message?
   c. Does it identify who will be the spokesperson when addressing a cyber incident?
4. What do you see as the greatest cyber threat to your organization?
5. Would your organization receive the alert information presented in this scenario?
   a. Through what channels would this information be received and disseminated?
   b. Do you believe there are communication gaps? If so, who in your organization is responsible for addressing these gaps?
   c. What actions, if any, would your department take based on this information?
6. What sources of cyber threat information does your organization regularly receive (e.g. information from DHS/NCCIC, FBI/InfraGard, United State Secret Service, MS-ISAC or other Information Sharing and Analysis Centers (ISACs) [Health ISAC, Election ISAC, Research Education Network (REN) ISAC], State of Washington Fusion Center, open source reporting or security providers)?
   a. What cyber threat information is most useful?
   b. Is the information you receive timely and actionable?
   c. Are there established mechanisms to facilitate rapid information dissemination? If so what are they?
   d. How is this information shared with other state/local entities and fusion centers?

Discussion Questions (Senior Elected Officials)

1. What capabilities and resources are required for the response to this cyber incident?
   a. What internal resources do you depend on? Are your current resources sufficient?
   b. Whom do you contact if you’re in need of additional third-party assistance?
   c. What additional resources are available within the region? How do you request these resources?
   d. Do you have personnel tasked with incident response or a designated cyber incident response team at your department and/or at the regional level?
2. What criteria will be used to determine whether data owners, customers, or partner organizations need to be notified if their data or networks have been illegally accessed?
3. What is your organizations process for knowing when and how to notify law enforcement?
   a. What are the advantages and disadvantages of notifying law enforcement?
4. If you have a cyber incident response plan, how often does your organization exercise the plan?
   a. Who is responsible for the exercise planning?
   b. What agencies are involved in the exercise?
   c. What level of the organization is required to participate?
   d. What actions follow the exercise?
5. What are your organization’s priorities at this point?
6. Do you pay the ransom?
   a. Who decides?
   b. What’s the process?
   c. What are the advantages/disadvantages to paying?
   d. What are the political ramifications?
   e. What outside partners/entities do you need to contact?
7. What elements of your organization are involved in the cyber incident response?
   a. Who is responsible for coordinating these elements?
   b. Is this process part of your formal plan?
   c. Is it exercised regularly?
8. What processes are used to contact critical personnel at any time, day or night?
   a. How do you proceed if critical personnel are unreachable or unavailable?
   b. Has the process been tested?
9. What formal policies and procedures does your organization use for when and how to restore backed-up data, including measures for insuring the integrity of backed-up data before restoration?
10. Does your organization monitor of social media?

MODULE 3: Incident Response

April 27, 2019

Students who provided banking information for receiving their $50 surplus discover that their bank accounts have been emptied. Concerned over the loss of their funds, the cashier's students repeatedly contact their university's office to question what happen, as well as post on various social media platforms. Some responses advise calling local law enforcement to report the situation.

April 30, 2019

Staff throughout the St. Joseph network report that when trying to record patient data from physiological monitors, the system is unable to pull up patient records and indicates that "the record does not exist.

IT confirms that malware has infected the patient records system network-wide and further analysis indicates that a mass quantity of patient records have been deleted.

Almost simultaneously, upon attempting to access patient records throughout the network, personnel receive a screen demanding a payment of $ 15.000 within 24 hours in exchange for the missing patient records. Staff report that they are unable to access their terminals.

May 1, 2019

A report surfaces on the local news detailing the incidents at the universities and the hospital.

News media is setting up satellite trucks outside of The St. Joseph Medical Center Hospital requesting information and on-camera interviews about the cyber incident.

Various social media posts question the issues with Washington State University and The University of Washington. Concerned students demand answers, bombarding the university president's offices with requests for information.

Concerned citizens in your region contact local elected officials and post to various social media their concern and surprise that the region was not prepared based on previous cyber incidents in the Pacific Northwest.

Discussion Questions (Senior Elected Officials)

1. **How would you describe your cybersecurity culture?**
   a. **As a leader, what cybersecurity goals have you set?**
   b. **How have they been communicated?**
2. **How would you respond to concerned citizens contacting your office regarding the situation in Oregon?**
   a. **Is the process documented?**
   b. **Who is authorized to speak and are they trained on cyber terminology?**
3. **What do you see as the greatest cyber threat to your organization?**
4. **As it relates to your jurisdiction, what cybersecurity information do you find most useful?**
   a. **What do you receive?**
   b. **How do you receive it?**
   c. **Do you get the information you need?**
5. **What information would you share, if any, with the following:**
   a. **Employees?**
   b. **Incorporated townships or surrounding cities and counties?**
   c. **Private sector entities within the City?**
   d. **The Federal Government or non-governmental organizations (e.g., MS-ISAC)?**
   e. **Do you have information sharing relationships with any of the above?**
6. **Do you or your organization have awareness of or regular interaction with the State of Washington Fusion Center, MS-ISAC, or other ISACs?**

MODULE 2: Incident Identification

April 20, 2019

Staff and faculty at both Washington State University and the University of Washington receive an email directing them to login to the university sponsored retirement program and enter security questions to confirm their account. An embedded link is included in the email.

Employees at St. Joseph Medical Center receive emails appearing to be from the American Medical Association, the National Association of Physical Therapists, American Association of Nurse Practitioners, and other well-known medical professional associations with a subject line, "HIPPA Best Practices." A link in the email connects to a website of one of the associations listed in the "From" line of the email.

April 23, 2019

Students at both Washington State University and the University of Washington receive an email claiming to be from the cashier's office stating that they were overcharged by $50 at the beginning of the term. It provides them a link with instructions for either receiving the money via check, crediting it towards their dining budget, or crediting it towards a future semester. Several students contact the University of Washington's Department of Student Financial Services and Washington State University's Student Financial Services office to report questions about this email; while other students at both universities click on the embedded link.

April 24, 2019

Several tickets are submitted to St. Joseph Medical Center IT help desk. The tickets detail complaints regarding user machines running much slower than normal. By noon, at least 10% of your users have submitted a ticket concerning slower than normal performance.

Discussion Questions (IT/Professional Staff)

1. At what level would your IT service desk or incident response team elevate an incident?
    a. Does your organization have predefined thresholds for assessing the severity of cyber incidents?
    b. How would you prioritize the incidents presented in the scenario?
    c. At this point, what severity levels would be assigned?
2. How do employees report suspected phishing attempts?
    a. What actions does your department take when suspicious emails are reported?
    b. Are there formal policies or plans that would be followed?
    c. Does your department conduct phishing self-assessments?
3. Does your organization utilize multi-factor authentication to mitigate the potential effects of phishing?
4. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
    a. How often is training provided?
    b. Is training required to obtain network access?
    c. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your city's or county's information systems? How often do they receive the training?
5. Do you use third-party support vendors?
    a. How well-defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
    b. How often are contracts reviewed?
    c. How well do your service level agreements address incident response?
    d. Do you have cyber insurance?

Discussion Questions (Senior Elected Officials)

1. How has your jurisdiction prepared for a cyber incident?
    a. Does your jurisdiction have a cybersecurity incident response plan in place?
    b. Who is responsible for developing and maintaining the plan?
    c. How often is the plan reviewed?
2. What is your role in your organization's cyber incident response plan?
    a. Is your cyber incident response plan embedded into your business continuity plans?
    b. Have you exercised the plan?
    c. When do you become involved in a cyber incident?
    d. Have you exercised the cyber incident notification process?
    e. What magnitude of incident would require your notification?
    f. How does that notification process work? Is it planned?
    g. Have you exercised the process?
3. Describe your organizations cybersecurity training requirements?
    a. Are there different requirements for senior leadership/executives?
    b. Do you participate in cybersecurity training?
        i. How often
        ii. What does that include
4. How does your jurisdiction recruit, develop, and retain cybersecurity staff?
    a. What are your cybersecurity workforce gaps?
5. Does your organization conduct phishing campaigns?
    b. What is effective?
    c. Do you target senior officials?
    d. What happens if a specific official clicks on the phishing email?
    e. How can you improve phishing training for your organization?