Cyber Attack Public Relations Exercise

Disaster Ready Chippewa Valley
December 12th, 2018

Exercise Guidelines

- This is an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected
- Base your responses on the current plans and capabilities of your organization
- Decisions are not precedent setting; consider different approaches and suggest improvements
- Issue identification is not as valuable as suggestions and recommended actions that could improve efforts; problem-solving efforts should be the focus

Participant Roles and Responsibilities

- **Players:** Respond to situation presented based on current plans, policies, and procedures
- **Observers:** Support players in developing responses, but do not participate in moderated discussion
- **Facilitators:** Provide situation updates and moderate discussions
- **Evaluators:** Observe and document player discussions

Assumptions and Artificialities

- The exercise scenario is plausible, and events occur as they are presented

Exercise Schedule

Welcome and Introduction	1:00PM – 1:05PM
Discussion & Exercise Conduct	1:05PM – 3:00PM
Hot Wash	3:00PM – 3:15PM
Closing Comments	

Scenario Background

- Today is Tuesday, December 12th

- There news cycle over the last few weeks has been relatively normal, no major disasters have occurred around the country

- Your agency/company information technology (IT) department has been sending out additional warnings about phishing emails, advising employees not to click on unknown or suspicious links.

Scenario Update 1

- An employee notices something is not right with his computer. The cursor on his screen is moving around on its own. The employee does not recall clicking on any unusual links or opening any suspicious files

Scenario Update 2

- Several employees have reported that regularly used applications are freezing. Some have had to reset passwords to get access to their workstations as well as these applications. There were no regularly scheduled password updates scheduled.

Scenario Update 3

- The information technology (IT) department at your organization suspect (but have not confirmed) that several systems have been compromised. These include those that contain elements of confidential information belonging to both your employees and your customers

Scenario Update 4

- The media has just called your company asking for a statement about a cyber breach at your agency/company. They indicated they received an anonymous tip from an employee that confidential information may have been exposed during a “cyber-attack.”

Scenario Update 5

- Your internet service provider (ISP) and IT staff have confirmed that unauthorized access to confidential customer information has occurred.

- It is unclear at this time how much information was exposed, the investigation is ongoing.

Scenario Update 6

- A significant number of concerned customers begin calling your organization. Your agency/company's social media sites are also receiving inquiries from concerned customers about the situation.

Scenario Update 7

- Several large media outlets are now requesting on-air interviews regarding the situation.

Hot Wash

- Strengths
- Areas for Improvement
- After participating in this exercise do you feel your organization is prepared to handle this type of incident?
- What takeaways do you have from this exercise that can be included in your organizations Crisis Communications Plan?

Closing Comments