AIR UNIVERSITY | AIR FORCE CYBER COLLEGE

CASE #F02-2109R0

TEACHING NOTES

WIZARD SPIDER: Lethally Poisonous Ransomware

Joshua A. Sipper
Air Force Cyber College

CYBER COLLEGE CASE STUDY SERIES

Air Force Cyber College

Col David B. Bosko, USAF, Commandant

Dr. Karen Guttieri, Academic Dean

Please send inquiries or comments to:

Ms. Kay Adams
Air Force Cyber College
60 W. Shumacher Ave., Bldg 803
Maxwell AFB AL 36112

Tel: (334) 953-5591
E-mail: lillian.adams.1@au.af.edu

ABSTRACT

Ransomware has become the cyberattack of choice for many criminal hackers due to its relative low-tech/high-yield character. This is seen across private, government, and personal data stores as cyber criminals use ransomware to "datanap" information stored on personal computers and devices, servers, and even cloud stores, then demanding payment for the encryption key to unlock and restore the valuable data. Nowhere has this been more effective than in the healthcare industry where hospitals and clinics are responsible for and dependent on the data and also liable for any harm that may come to patients physically. This is not to mention the fact that if patient personally identifiable information (PII) or Health Insurance Portability and Accountability Act (HIPAA) medical data were to be kept and spread or used by the hackers, more consequences would cascade. A ransomware attack on the Druid City Hospital (DCH) Healthcare System in October of 2019 is a prime example of the consequences and ramifications of medical and patient data being held captive. In this case study, the attack itself will be recounted, issues and dilemmas will be characterized, and the implications of this attack will be discussed.

PRE-READING

All of the prereads are articles that were generated following the real world ransomware attack. These articles are simply to prime the students and get them thinking about what occurred and the accompanying dilemmas.

1. The first article presents the initial news concerning the attack and how the hospital lacked the capacity to care for patients. The dilemma associated is primarily concerned with the lack of patient care and discussions can revolve around what dilemmas can stem from a hospital lacking the capacity to deliver care (potential exacerbation of symptoms, death, maiming, lawsuits, etc.)

https://www.wtvy.com/content/news/Tuscaloosa-hospitals-crippled-due-to-ransomware-attack-561974121.html[1]

2. The second article details the federal lawsuits files by patients in response to absence of care. This supports the dilemma discussion in article 1.

https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html[2]

[1] WBRC Staff, (2019). Tuscaloosa hospitals crippled due to ransomware attack, WBRC News Report, accessed 4/29/2020: https://www.wtvy.com/content/news/Tuscaloosa-hospitals-crippled-due-to-ransomware-attack-561974121.html

[2] Koplowitz, H. (2019). DCH Health System patients file federal suit over ransomware attack, AL.com, accessed 4/29/2019: https://www.al.com/news/tuscaloosa/2019/12/dch-health-system-patients-file-federal-suit-over-ransomware-attack.html

3. The third article gives additional details regarding the federal lawsuit detailed in the narrative portion of the case study and allows deeper discussion into the dilemmas associated with the lawsuit.

https://healthitsecurity.com/news/dch-health-faces-federal-lawsuit-after-10-day-ransomware-attack[3]

4. The fourth article looks more closely at D CH's decision to pay the ransomware hackers the ransom and the associated dilemmas for paying versus not paying (paying = emboldening hackers to continue hacks or hack again versus not paying = continued/worsening of lawsuits, lack of patient care, loss of revenue, etc.)

https://www.fiercehealthcare.com/tech/alabama-based-dch-health-system-pays-hackers-responsible-for-ransomware-attack-as-fbi-warns[4]

5. The fifth article offers additional details to support the dilemmas referenced in article 4.

https://www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack[5]

6. The sixth article identifies that the ransomware attackers are Russian and give more details on the payment of the ransom. This is useful for the discussion as it allows students to consider the international, criminal, nation state, and other ramifications of Russian ransomware.

https://www.alreporter.com/2019/10/05/dch-hospital-system-pays-russian-hackers-in-ransomware-attack/[6]

PDFs also accessible and printable.

EXERCISE

In the following exercise, students will participate in activities structured to analyze the case. First, students will be assigned or can choose "actor" roles to play in order to further examine the different issues, dilemmas, and actions taken during the case. Students will also have the opportunity to discuss how actions and events might have been mitigated and provide lessons learned. Dilemmas will be identified by the students and deconstructed to see what courses of ac-

[3] Davis, J. (2020). DCH Health Faces Federal Lawsuit After 10-Day Ransomware Attack, HealthITSecurity.com, accessed 4/29/2020: https://healthitsecurity.com/news/dch-health-faces-federal-lawsuit-after-10-day-ransomware-attack

[4] Landi, H. (2019). Alabama health system pays hackers responsible for ransomware attack as FBI warns more to come, FierceHealthcare, accessed 4/29/2019: https://www.fiercehealthcare.com/tech/alabama-based-dch-health-system-pays-hackers-responsible-for-ransomware-attack-as-fbi-warns

[5] Eddy, N. (2019). Alabama hospital system DCH pays to restore systems after ransomware attack, Healthcare IT News, accessed 4/29/2019: https://www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack

[6] Burkhalter, E. (2019). DCH Hospital System pays Russian hackers in ransomware attack, AlabamaReporter.com, accessed 4/29/2019: https://www.alreporter.com/2019/10/05/dch-hospital-system-pays-russian-hackers-in-ransomware-attack/

tion (COAs) might have been taken and the consequences and ramifications of those COAs. Teaching objectives are included in the teaching notes and will assist the facilitator with directing the case study and assessing the outcomes. At the close of the case analysis, takeaways and lessons learned will be discussed and noted in an after action report (AAR) for further analysis and assessment. Finally, the implications will be discussed and appended to the AAR.

Actors

The actors in this case study include you, the students, who will role play the scenario through various perspectives in order to analyze what went wrong, what could have been done better, and how the varying views of healthcare providers, administrators, and law enforcement affected DCH. Additionally, the role of the hacker will be discussed to get a better perspective on why the hacker chose DCH, how the hacker will proceed in the future, and what the hacker expects to get out of future ransomware attacks.

Roles

In a class of 12 to 15 students, similar roles may be distributed to gain varying perspectives on similar roles. For larger/smaller class sizes, roles may be expanded or contracted, or some students may choose multiple roles.

- Healthcare providers:
    - ○ 2 nurses
        - Pediatric nurse – As a pediatric nurse, you care for children. Your career has been consumed with caring for and loving young children
        - ER nurse – ER nurses are at the forefront of care and are not used to turning people away for anything
    - ○ 2 doctors
        - ER doctor – Just like ER nurses, ER doctors are on the front line when it comes to triage and care
        - Heart surgeon – Heart surgeons are not many steps removed from front line care doctors as they often must perform emergency surgeries to correct heart and vascular issues that may lead to cardio-pulmonary problems or strokes
    - ○ 2 administrators
        - Hospital administrators span from financial management to chief of surgical staff and have a vested interest in the operations and welfare of the hospital and staff
- Law enforcement:
    - ○ 2 FBI

        - FBI agents are generally very specialized and experienced in a particular field, in this case cyber
    - 2 local
        - Local law enforcement generally do not specialize in a particular type of crime as much as FBI, DHS, etc. However, they are particularly interested in the well-being of their local community
- Hackers:
    - 2 hackers
        - Most people do not consider the interest or thought patterns of the assailants during or after they perpetrate the crime. But, it is important to think through their motivations and how they potentially view the unfolding situation
- Patients and family
    - 2 patients
        - Child patient – Children are different from adults in many ways, especially when it comes to their illnesses. A child patient will usually be more frightened and more dependent on adults during these situations
        - Elderly patient – Again, elderly patients are special. They may or may not understand what is going on and may have experience outside the norm
    - 1 Family member
        - Family members tend to be quite protective of their injured and sick loved ones. They might react angrily or be depressed or agitated or nervous.
- Local and State Politicians
    - Local politician – Local politicians would have a large stake in the outcome of this emergency situation, especially if they are up for reelection
    - State politician – State politicians, while not under as much scrutiny locally, would likely be concerned about how this situation turns out from a state and national perspective

DILEMMA DISCUSSION

In this part of the case study, the students will have the opportunity to note and struggle with the various dilemmas that arose in the narrative, supporting articles, and ransomware analysis. As the facilitator and instructor, it is recommended that you allow the students to exhaust at least one dilemma each before you interject the following possibilities (i.e., allow the students to completely explore the dilemmas and generate as many ideas as possible before prompting them to continue or consider additional dilemmas). These dilemmas are available for use and discussion in addition to and accordance with any dilemmas and issues identified by the students.

1. Hospital administrators chose to close the hospital to incoming patients except for emergencies. This caused the diverting of patients or delay of medical care to patients who then claimed denial and disruption of medical care. However, if the hospital had closed completely, loss of revenue and reputation could have occurred. If the hospital had not turned anyone away and attempted to treat the same number of patients as under normal circumstances, the possibility of malpractice and other legal action would have been more probable.

2. Doctors acting on administrative policy were forced to turn patients away and enact emergency treatment procedures which allowed for minimal medical operations to continue. Care was still available to patients, but at the risk of maltreatment due to reduced information concerning patient records, medications, and other vital treatment data. Ultimately, if doctors treated the patients, they opened themselves up to malpractice suits, but if they sent them away, other legal action might arise as they would have been denying patients medical care.

3. Nurses were able to provide some treatment, but with reduced access to information. Current patients were allowed to stay and remain under nurse and physician care. However, prescriptions were unavailable as well as other treatment necessities. Some patients were transferred, but suffered setbacks which precipitated legal action. Additionally, transfers could have potentially placed patients in mortal danger bringing with it the same problems encountered by the doctors

4. FBI agents responded and began investigations. However, ransomware is notoriously difficult to trace back to the malicious source, slowing the investigation significantly. The FBI encourages hospitals not to pay ransoms as it can embolden hackers to strike again and ask for more money. While paying the ransom might allow institutions to get back to operations earlier, it also prevents federal and local law enforcement from bringing their full investigative power and influence to bear. If the FBI cannot trace the hackers, the chance of lost revenue, reputation, and resources for the hospital rises quickly. Also, the reputation of the FBI is at stake as they are unable to find a solution to bring the perpetrators to justice and end the possibility of future attacks.

5. Local law enforcement faces many of the same dilemmas as the FBI. However, with local law enforcement, the effects are magnified and extended further into the future. While local law enforcement might bring in experts and analysts, the information may only serve to frustrate those who are affected by the attack. Questions like "But what are you doing to solve this?" abound. In other words, local law enforcement face the dilemma of attempting to solve problems for their local organizations only to potentially create deeper problems for themselves.
6. Hackers using the ransomware are not generally traceable. They can operate with virtual impunity. However, the attacks they use tend to educate and secure the institutions and organizations they attack making future attacks less simple. Ransomware is not necessarily a sophisticated cyberattack and therefore hackers face the dilemma of overuse of this type of attack and the resilience of institutions growing and making this type of attack less effective.
7. Patients under care at the hospital have options; none of them very good. If they choose to stay and be treated, they run the risk of maltreatment, lack of care, lack of medicines, and other potential inconveniences and perils. If they choose to be transferred, they still lack the medical information that cannot be transferred with them, making care at another location prone to similar difficulties.
8. Family members of patients face many of the same difficulties as the patients. As with the 7 year old girl who was taken to another facility, the time lag in treatment prolonged her suffering and the distress to her family. However, treatment at the local facility was not possible for a much longer period and may not have been effective due to lack of access to information, medicines, and other data.

TEACHING OBJECTIVES

The following are the objectives you as the instructor/facilitator should try to reach. You may share these with the students, but it is not necessary for the objectives to be achieved. Questions and exercises will be offered for use in meeting the objectives, however other questions and exercises may be developed by the instructor/facilitator if so desired. Measures of Assessment (MOA) are listed below each objective.

1. Students will demonstrate critical thinking skills through analysis of the case narrative and ransomware analysis.

   a. Student discussion.

   b. Concepts tied together.

   c. Student synthesis.

2. Students will indicate increased understanding of and urgency concerning ransomware attacks.
   a. Student comments of affective comprehension (fear, surprise, etc.)
   b. Questions related to mitigations.
   c. Ideas and suggestions of mitigations from students.
3. Students will produce potential courses of action (COAs).
   a Student examination of assigned/chosen role.
   b. Student choices concerning how to proceed through each phase of the narrative.
   c. Proposed resolutions and problems.
   d. Statement of consequences and ramifications.
4. Students will identify takeaways and lessons learned such as the following.
   a. Students identify the dilemmas and implications.
   b. Students indicate what they have learned thought the case study.
   c. Students produce AAR based on lessons learned and takeaways regarding dilemmas and implications.

CASE STUDY EXERCISE

The following section may be used by the instructor/facilitator to generate discussions, synthesis, and critical thinking regarding the case study. Student responses and reactions to questions, activities, and discussions may be used to assess student cognitive and affective learning objectives. At the end of the TN, you will find a rubric for each section to assist in assessing student learning outcomes.

Narrative Discussion

The students are given the narrative and the instructor reads it as all follow along. After the reading of the narrative, the following questions can be asked and discussed. The instructor should record or note the discussion as closely as practical to gain insights into the analysis of the narrative and the discussion enabled through the prompting questions. This information can be used to produce further discussion and generate ideas for the role playing exercise. AS the instructor, you simply need to write down the students' responses to the following questions. These notes will help you later as you revisit their responses and ask further questions to generate deeper discussion and reflection.

1. What are the major dilemmas in this story?

2. Who are the main characters in this story? What are their interests, desires, hopes, fears, etc.?

3. What are the consequences that emerge in the narrative?
4. What are the ramifications that emerge?
5. What are alternative COAs? What are benefits and shortfalls of each COA?

DISCUSSION RUBRIC

A discussion rubric to help instructors track student discussions and replies to other students. This can serve to provide feedback to students about their performance in the exercise. To simply agree or disagree with other students is not sufficient. Score is based on 100 point scale.

Criteria	Unsatisfactory	Limited	Proficient	Exemplary	Score
Critical Analysis **(Understanding of Readings and Outside References)**	Discussions show little or no evidence that readings were completed or understood. Discussions are largely personal opinions or feelings, or "I agree" or "Great idea," without supporting statements with concepts from the readings, outside resources, relevant research, or specific real-life application.	Discussions repeat and summarize basic, correct information, but do not link readings to outside references, relevant research or specific real-life application and do not consider alternative perspectives or connections between ideas. Sources are not cited.	Discussions display an understanding of the required readings and underlying concepts including correct use of terminology and proper citation.	Discussions display an excellent understanding of the required readings and underlying concepts including correct use of terminology. Postings integrate an outside resource, or relevant research, or specific real-life application (work experience, prior coursework, etc.) to support important points. Well-edited quotes are cited appropriately. No more than 10% of the posting is a direct quotation.	

Demonstrate Increased Understanding and Urgency toward Ransomware	Discussions do not indicate an understanding or urgency concerning ransomware and do not generate new conversation.	Discussions sometimes indicate an understanding or urgency concerning ransomware as evidenced by — affirming statements or references to relevant research or, — asking related questions or, — making an oppositional statement supported by any personal experience or related research.	Discussions contribute to the class' ongoing conversations as evidenced by — affirming statements or references to relevant research or, — asking related questions or, — making an oppositional statement supported by any personal experience or related research.	Discussions actively stimulate and sustain further discussion by building on peers' responses including — building a focused argument around a specific issue or — asking a new related question or — making an oppositional statement supported by personal experience or related research.	
Students Produce COAs	No real interaction; do not lead to production of COAs	Some of the interactions in the discussion lead to ideas, but not complete COAs.	Interactions on the lead to basic COAs with defined ways forward.	Interactions produce well-designed and mapped COAs with specific strategies associated.	
Takeaways and Lessons Learned	Responses contain no learning reflection, cognitive, or affective indications.	Responses contain some learning reflection, cognitive, or affective indications.	Responses contain practical learning reflection, cognitive, or affective indications.	Responses contain well analyzed and developed learning reflection, cognitive, or affective indications.	
TOTAL					

* Open class discussion is an important and significant part of any course. While class discussion whether online or face to face, can be characterized by free flowing conversation, there are identifiable characteristics that distinguish exemplary contributions to class discussion from those of lesser quality. The criteria found on the rubric above will be used to assess the quality of your discussions and responses to peers during class discussion.

Class Exercise

The class exercise is based on an exploration of the Case Study Narrative, Source Material, and Ransomware Analysis. The first step in the exercise is to have the students choose roles from the list of roles noted in the Roles section. Students will then engage in small group discussions (3-4 per group) where they may explore the dilemmas, potential alternative choices they would have made in their chosen role, and the consequences and ramifications associated with those potential choices. Each student shall note these choices in the discussion matrix provided.

Exercise Instructions

Divide the students into groups of 3 or 4 participants, depending on class size/number. Ensure that each group has a mixture of roles (e.g., not all family, nurses, etc.) for more developed discussion. Allow student groups to discuss for 20-30 minutes while noting their outcomes and inputting their choices in the matrix below.

Choices	**Consequences**	**Ramifications**
Based on your understanding of the readings and the dilemma discussion, what choices did the person in your role make and what were the consequences and dilemmas?		
What choices would you have made in your role and what do you see as the potential consequences and dilemmas of those choices?		
How did the choices made by the original person in your role affect others around them?		

How did the choices of others affect the choices made by the person in your role?		
In what ways would the choices you would make resolve or mitigate the problems introduced by the ransomware attack?		

EXERCISE RUBRIC

An exercise rubric helps track student actions and decisions throughout the exercise. Students shall note in-depth responses with entries in the provided discussion matrix. Score can, for instance, be based on 100 point scale.

Criteria	Unsatisfactory	Limited	Proficient	Exemplary	Score
Critical Analysis **(Understanding of Readings and Outside References)**	Entries show little or no evidence that readings were completed or understood. Discussions are largely personal opinions or feelings, or "I agree" or "Great idea," without supporting statements with concepts from the readings, outside resources, relevant research, or specific real-life application.	Entries repeat and summarize basic, correct information, but do not link readings to outside references, relevant research or specific real-life application and do not consider alternative perspectives or connections between ideas. Sources are not cited.	Entries display an understanding of the required readings and underlying concepts including correct use of terminology and proper citation.	Entries display an excellent understanding of the required readings and underlying concepts including correct use of terminology. Postings integrate an outside resource, or relevant research, or specific real-life application (work experience, prior coursework, etc.) to support important points. Well-edited quotes are cited appropriately. No more than 10% of the posting is a direct quotation.	

Demonstrate Increased Understanding and Urgency toward Ransomware	Entries do not indicate an understanding or urgency concerning ransomware and do not generate new conversation.	Entries sometimes indicate an understanding or urgency concerning ransomware as evidenced by — affirming statements or references to relevant research or, — asking related questions or, — making an oppositional statement supported by any personal experience or related research.	Entries contribute to the class' ongoing conversations as evidenced by — affirming statements or references to relevant research or, — asking related questions or, — making an oppositional statement supported by any personal experience or related research.	Entries actively stimulate and sustain further discussion by building on peers' responses including — building a focused argument around a specific issue or — asking a new related question or — making an oppositional statement supported by personal experience or related research.	
Students Produce COAs	No substantive entries; do not lead to production of COAs	Some of the entries in the discussion matrix lead to ideas, but not complete COAs.	Entries lead to basic COAs with defined ways forward.	Entries produce well-designed and mapped COAs with specific strategies associated.	
Takeaways and Lessons Learned	Responses contain no learning reflection, cognitive, or affective indications.	Responses contain some learning reflection, cognitive, or affective indications.	Responses contain practical learning reflection, cognitive, or affective indications.	Responses contain well analyzed and developed learning reflection, cognitive, or affective indications.	
				TOTAL:	

* Reflective exercises are an important and significant part of any course. Class exercises are characterized by free flowing conversation and well-thought-out written responses.

WRAP-UP DISCUSSION AND AAR

In the following section, the students will come back together from their groups and brief the class on their responses in their respective discussion matrices. The class will then synthesize an AAR from the inputs taken from the best practices identified within the discussion matrices. The AAR should include lessons learned, best practices, and takeaways gleaned during the exercise portion of the case study. The following template can be used to develop and construct the AAR. As the instructor, you need only guide the class as they fill in the AAR with the various lessons learned, best practices, and takeaways. The AAR is simply a way for the students to organize what they have learned so that you as the instructor can more readily identify and assess their learning. In the real world, an AAR would be used after an exercise or real world event to identify procedural and policy changes following an emergency or disaster situation.

[FULL EXERCISE NAME]

[Exercise Date]

AFTER ACTION REPORT/IMPROVEMENT PLAN

[Publication Date]

CONTENTS

EXECUTIVE SUMMARY

The [school or school district] [scenario type] [exercise type] exercise [exercise name] was developed to test [school or school district]'s Emergency Operations Plan. The exercise planning team was composed of numerous and diverse agencies/people, including [list of agencies/people participating in planning team]. The exercise planning team discussed [include a brief overview of the major issues encountered, discussed, and resolved during the exercise planning process. Topics to address in this section could include the length of the planning process, the reasoning behind the planning team's choice of objectives to exercise, etc.]

Based on the exercise planning team's deliberations, the following objectives were developed for [exercise name]:

- Objective 1: [Insert 1 sentence description of the exercise objective]
- Objective 2: [Insert 1 sentence description of the exercise objective]
- Objective 3: [Insert 1 sentence description of the exercise objective]

The purpose of this report is to analyze exercise results, identify strengths to be maintained and built upon, identify potential areas for further improvement, and support development of corrective actions.

[In general, the major strengths and primary areas for improvement should be limited to three each to ensure the Executive Summary is high-level and concise.]

Major Strengths

The major strengths identified during this exercise are as follows:

- [Use complete sentences to describe each major strength.]
- [Additional major strength]
- [Additional major strength]

Primary Areas for Improvement

Throughout the exercise, several opportunities for improvement in [jurisdiction/organization name]'s ability to respond to the incident were identified. The primary areas for improvement, including recommendations, are as follows:

- [Use complete sentences to state each primary area for improvement and its associated key recommendation(s).]
- [Additional key recommendation]
- [Additional key recommendation]

SECTION 1: EXERCISE OVERVIEW

Exercise Details

Exercise Name

[Insert formal name of exercise, which should match the name in the header.]

Type of Exercise

[e.g. seminar, workshop, drill, game, tabletop, functional exercise, or full-scale exercise.]

Exercise Date

[Insert the month, day, and year that the exercise was conducted.]

Duration

[Insert the total length of the exercise, in day or hours, as appropriate.]

Location

[Insert all applicable information regarding the specific location(s) of the exercise]

Response Protocol or Emergency Action

[Insert a list of the response protocol or emergency action addressed within the exercise.]

Scenario Type

[Name the exercise scenario type (e.g. chemical release).]

Exercise Planning Team

[The name of each member of the planning team leadership should be listed along with their role in the exercise, organizational affiliation, job title, mailing address, phone number, and e-mail address.]

Participants

[Insert a list of the individual participating organizations or agencies, including Federal, State, Tribal, non-governmental organizations (NGOs), local and international agencies, and contract support companies as applicable.]

Number of Participants

- Players: [#]
- Controllers/Facilitators: [#]
- Evaluators: [#]
- Observers: [#]
- Victim Role Players: [#] (*for operations based exercises only*)

SECTION 2: EXERCISE DESIGN SUMMARY

Exercise Purpose and Design

[This section should contain a brief (one-to-two paragraph) summation of why the exercise was conducted and what the exercise participants hoped to learn. It should also include a brief history of how the exercise was organized, designed, funded, etc.]

Exercise Objectives, Capabilities, and Activities

[The purpose of this section is to list exercise objectives and activities as identified by the emergency operations plan. A description of how the exercise objectives and activities were evaluated should be explained here.]

Based upon the identified exercise objectives below, the exercise planning team has decided to demonstrate the following activities during this exercise:

- Objective 1: [Insert a one sentence description of each objective].
    - [Activity 1];
    - [Activity 2]; and
    - [Activity 3].

Scenario Summary

[For an operations-based exercise, this section should summarize the scenario or situation initially presented to players, subsequent key events introduced into play, and the time in which these events occurred. For a discussion-based exercise, this section should outline the scenario used and/or modules presented to participants.]

SECTION 3: ANALYSIS OF CAPABILITIES

Objective 1: [Name]

Summary of Activities Associated with Objective: [Include an overview of the objective, and a description of how the objective was performed during the exercise or addressed during a discussion-based exercise.]

List of General Observations/Comments: [A strength is an observed action, behavior, procedure, and/or practice that is worthy of recognition and special notice.]

Analysis: [Include a description of the behavior or actions at the core of the observation, as well as a brief description of what happened and the consequence(s) (positive or negative) of the action or behavior. If an action was performed successfully, include any relevant innovative approaches utilized by the exercise participants. If an action was not performed adequately, the root-causes contributing to the shortcoming must be identified.]

Recommendations:

1. [Complete description of recommendation]
2. [Complete description of recommendation]
3. [Complete description of recommendation]

SECTION 4: CONCLUSION

[This section is a conclusion for the entire document. It provides an overall summary to the report. It should include the demonstrated capabilities, lessons learned, major recommendations, and a summary of what steps should be taken to ensure that the concluding results will help to further refine plans, policies, procedures, and training for this type of incident.

Subheadings are not necessary and the level of detail in this section does not need to be as comprehensive as that in the Executive Summary.]

APPENDIX A: IMPROVEMENT PLAN MATRIX

This IP has been developed specifically for [Enter school/district] as a result of [exercise name] conducted on [date of exercise]. These recommendations draw on both the After Action Report and the After Action Conference. [The IP should include the key recommendations and corrective actions identified in the Analysis of Capabilities, and the After Action Conference.]

No.	Objectives/Observations/ Issues/Expected Outcomes Not Met	Recommendation(s)	Specific Corrective Action to be implemented	Priority L/M/H	Assigned To	Expected Completion Date
1	*Example: Staff did not clearly understand instructions from Crisis Team, but knew how to activate SIP within the classrooms.*	*Maintain regular SIP training for teachers to keep concept fresh* *Fix communication issues from Crisis Team*	*Quarterly SIP training for teachers* *Training Crisis Team on appropriate language for messaging & use of radios*	*Low* *High*	*Principal Jones* *Crisis Team Training Leader*	*Ongoing (Quarterly)* *End of 2nd Quarter or by next drill*
2						
3						
4						
5						
6						
7						
8						

No.	Objectives/Observations/ Issues/Expected Outcomes Not Met	Recommendation(s)	Specific Corrective Action to be implemented	Priority L/M/H	Assigned To	Expected Completion Date
1	*Example: Staff did not clearly understand instructions from Crisis Team, but knew how to activate SIP within the classrooms.*	*Maintain regular SIP training for teachers to keep concept fresh* *Fix communication issues from Crisis Team*	*Quarterly SIP training for teachers* *Training Crisis Team on appropriate language for messaging & use of radios*	*Low* *High*	*Principal Jones* *Crisis Team Training Leader*	*Ongoing (Quarterly)* *End of 2nd Quarter or by next drill*
2						
3						
4						
5						
6						
7						
8						

CYBER COLLEGE CASE STUDY SERIES

Please send inquiries or comments to:

Ms. Kay Adams
Air Force Cyber College
60 W. Shumacher Ave., Bldg 803
Maxwell AFB AL 36112

Tel: (334) 953-5591

E-mail: lillian.adams.1@au.af.edu

AIR UNIVERSITY | AIR FORCE CYBER COLLEGE