Global Information Assurance Certification Paper

Constructing a Measurable Tabletop Exercise for a SCADA Environment

GIAC (GICSP) Gold Certification

Author: Matthew Hosburgh, matt.hosburgh@gmail.com

Advisor: Chris Walker

Accepted: 3/6/2016

Abstract

The incident occurred back in November 2011, or at least that was the story. Initial reports that an advanced hacker had taken control of a Supervisory Control and Data Acquisition (SCADA) system started to surface. This system controlled a physical component: a water pump. Not many of these types of attacks had been reported in the past, and made the report more alarming. Riding on the heels of the Stuxnet discovery, a real and more common threat to critical infrastructure was being realized. The report was quick to attribute the attacker to a country notorious for hacking. The report also indicated the compromised system was forced to operate beyond normal levels, causing a pump to fail. But was it true? Weeks later, the report and attribution were under criticism from ICS-CERT, who had conducted the incident handling steps for the Curran-Gardner Public Water District. By drawing a parallel to the Curran-Gardner attack, a sound and measureable tabletop exercise can be developed to help an organization deal with a real-life incident affecting a SCADA system.

1. Introduction

It was the start of the evening shift. Because daylight savings just "fell back" it was already dark outside—at six o'clock PM central time. A long and bleak 12 hour shift awaited Steve, who was a seasoned Supervisory Control and Data Acquisition (SCADA) operator. His job required continuous monitoring of the water district's systems that control and monitor the valves, pumps, and other components. All of the systems he monitored played some role in the Curran-Gardner Public Water District. Tonight, however, was going to be different than any other night he had worked. Steve's phone rang. "Odd," he thought. He didn't get many calls, especially right at shift change. The voice on the other end sounded out of breath. It was Brett. He gasped, "One of our water pumps just failed!" Pausing, he continued, "I had to shut it down manually so that a pipe wouldn't burst." Steve looked over at his screen, and sure enough, there was a pump now red, indicating it was down—hard. Brett had to go because he said he had more work to do. Steve said "Thanks. Please keep us up to date." Not a typical start to an evening. Steve could feel his heart beating faster. He tried to collect his thoughts and his blood pressure. What Steve soon discovered would leave the entire water district in shock. At least for a few weeks.

It was in November 2011 that the Curran-Gardner Public Water District knew something was wrong. This time, there was an outside variable in the form of an attacker. This attacker's origin was attributed early on to a country notorious for hacking, and in many cases, being a persistent threat. An intriguing difference between this attack and others, was the physical component involved. This component, if taken down, had the potential to cause physical damage. Weeks after the initial public report came to light another update was published. "This report also alleged a malicious cyber intrusion from an IP address located in Russia that caused the SCADA system to power on and off, resulting in a water pump burn out" (ICSB-11-327-01, 2011). The report continued "After detailed analysis of all available data, ICS-CERT and the FBI found no evidence of a cyber intrusion into the SCADA system of the Curran-Gardner Public Water District in Springfield, Illinois" (ICSB-11-327-01, 2011). Much like a fitness program, the issue

Matthew Hosburgh, matt.hosburgh@gmail.com

is not with knowing what to do or eat. Instead, the issue is whether or not incident response actions are taken or not. Without validating the plan, a response to an incident can bring about collateral damage if it is not properly drilled. By drawing a parallel to the Curran-Gardner attack, a lightweight and measureable tabletop exercise can be developed to help an organization deal with a real-life incident affecting a SCADA system.

2. Incident Handling in a SCADA Context

Incident handling in a SCADA environment should be well defined prior to a real-life event, to minimize the Fog of War (FoW). The FoW, or the confusion, during a real-life incident is magnified. The main difference between a traditional IT and a SCADA environment is the physical nature. Simply put, life, safety, and significant outages are obtained by attacking certain SCADA systems. For that reason, having a well-defined set of definitions and what constitutes as an incident in the organization is imperative.

2.1 What an Incident is (and is Not)

The National Institute for Standards and Technology (NIST) defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Cichonski, Millar, Grance, & Scarfone, 2012). The key to this definition and the successful handling of an incident is with the organization. The policies that are defined and maintained by an organization frame the boundaries of what is and is not an incident. For example, a policy might state that if an organization's mobile device is observed making connections to a known botnet, it should be treated as an incident. Furthermore, an event could be something that is noteworthy, but not necessarily an incident. NIST defines an event as "any observable occurrence in a system or network" (Cichonski et al., 2012). A user's account was locked out due to three invalid password attempts, could be an example, but

also depends on what the organization defines as an incident and thus the criticality of having such definitions prior to an event occurring.

2.2 Handling versus Response

Incident handling and Incident Response both co-exist; however, there is a defining difference. Often used interchangeably, Incident Handling (IH) typically outlines the overall reaction to a defined incident or event. Think of this as the macro understanding of an incident. Similarly, Incident Response (IR) is the more detailed approach, or micro view, to dealing with a defined incident. Put another way "Incident Response is all of the technical components required in order to analyze and contain an incident. Incident Handling is the logistics, communications, coordination, and planning functions needed in order to resolve an incident in a calm and efficient manner" (De Beaupre, 2011). For this example, the six phases of Incident Handling will be the framework. An illustration of these phases is illustrated in figure 1.

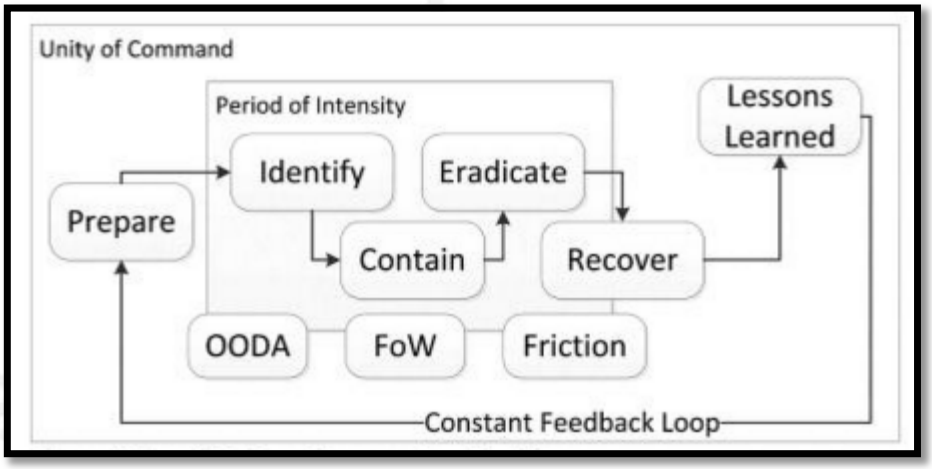


Figure 1. Six phases of Incident Handling with conflict superimposed (Murdoch, 2014)

The phases are further defined as:

- Preparation - efforts to get ready for an incident
- Identification - pinpointing all of the systems involved.
- Containment - isolating all systems infected or at risk.

Matthew Hosburgh, matt.hosburgh@gmail.com

- Eradication - removing the problem or threat from the environment.
- Recovery - restoring the system to normal use and function.
- Lessons Learned - lessons from the incident that can help with future incidents or process improvement.

Throughout the course of this paper, the six phases of IH will be used to step through the Curran-Gardner attack. Further, the table-top exercise for IT Directors will be loosely based on this attack. Failing to prepare for an incident can leave an organization in a very compromising position.

3. The First Phase: Preparation

Similar to training for a race, preparing for an incident can help to reduce the time it takes to respond to all types of incidents, regardless of priority. On November 10, 2011, Curran-Gardner reported that a cyber incident had occurred. Shortly after the report was published, ICS-CERT reached out to the Statewide Terrorism & Intelligence Center (STIC) to get more information. As it was provided, "initial analysis could not validate any evidence to support the assertion that a cyber intrusion had occurred" (ICSB-11-327-01, 2011). On this finding, it becomes apparent that defining what constitutes as an incident is needed to ensure the right response is initiated. This can be in the form of an incident classification guide, which can be established prior to the incident occurring. This guide should include a threshold of what is considered an incident, and if possible, what is defined as an event. By defining this ahead of time, the analyst can avoid a "boy who cried wolf" scenario and remain credible in the future. Figure 2 illustrates a few suggested categories for intrusions as detailed in *The Practice of Network Security Monitoring: Understanding Incident Detection and Response.*

Name	Description
Cat 6	Intruder conducted reconnaissance against asset with access to sensitive data.
Cat 3	Intruder tried to exploit asset with access to sensitive data, but failed.
Cat 2	Intruder compromised asset with access to sensitive data but did not obtain root- or administrator-level access.
Cat 1	Intruder compromised asset with ready access to sensitive data.
Breach 3	Intruder established command-and-control channel from asset with ready access to sensitive data.
Breach 2	Intruder exfiltrated nonsensitive data or data that will facilitate access to sensitive data.
Breach 1	Intruder exfiltrated sensitive data or is suspected of exfiltrating sensitive data based on volume, etc.
Crisis 3	Intruder publicized stolen data online or via mainstream media.
Crisis 2	Data loss prompted government or regulatory investigation with fines or other legal consequences.
Crisis 1	Data loss resulted in physical harm or loss of life.

Figure 2. Incident or intrusion categories (Bejtlich, 2013).

The second aspect to preparation in this case is knowing who to notify and when. The intrusion categories can help to in defining the scope of notifications. Using an escalation hierarchy for reporting incidents can provide another look at the data, which might help rule out known issues or authorized activity that may not have been known by the analyst. IH should not be done in a vacuum! Curran-Gardner helped to reveal some of the systems or personnel that might need to be further investigated or coordinated in order to recover from an attack. At minimum, someone with access to the system that controlled the pump, the Security Team, the operator and management would be a good start. Depending on the environment or organization structure, these roles might overlap,

but if known ahead of time the preparedness and reactionary ability of the Response Team can be greatly increased. Lastly, preparing for an incident should include exercises, starting with a tabletop exercise. This is an extremely effective method of validating the basics of the IR plan without requiring all resources be available, which can reduce the operational impact on an organization. A tabletop exercise, however, should not replace a full IR exercise, but can be used to help prepare for one.

3.1 Preparing for the Incident

Much like a real incident, preparation is a necessary step when developing a tabletop exercise. Like defining a mission, the preparation phase will help direct the conduct of the exercise. This phase should be used to first establish the overall goal. For example: *to improve overall communications between the IT Security Team and the SCADA operators when an incident occurs.* Once that is established, the objectives can be developed. These can range from general to specific, depending on the needs of the exercise. For this high level exercise, the following objectives would be a good start:

- Complete the incident response exercise within the allotted time.
- Obtain IT Director (or higher) participation in an exercise for the organization.
- Identify all of the infected or compromised systems indicated in the scenario.
- Contain all of the infected or compromised systems indicated in the scenario.
- Eradicate all of the infected or compromised systems indicated in the scenario.
- Recover the system to pre-incident status or normal operations.
- Discuss recommendations for improvements.

After the objectives are set, the agenda should be defined. The agenda should include the goals, objectives, participants and the timeline. The roles should be discussed and assigned as well. At the director level, this will ensure that all activities are enumerated and displayed. When time is a scarce commodity, every minute will count. By accurately showing the timing of the exercise, more participation can be expected because the IT Directors and other participants can plan accordingly. A sample agenda

containing the above listed can be found in Appendix A.

3.2 Measuring the Exercise

A significant area of preparation is deciding what to measure the exercise on. These metrics not only help track the progress and issues of the exercise, but can help compare the performance of future exercises. For an IT Director level tabletop exercise the following metrics can be used:

- Number of IT Director or Above Participants - Number of participants at the director level or above.
- Participants - Number of participants below the director level.
- Time to Identify All Systems at Risk or Compromised – The time it takes for the group to identify all known systems at risk or compromised after distributing the participant handout.
- Total Time to Complete - Overall time that the exercise took to complete.
- Time to Contain All Systems at Risk or Compromised - Time it takes for the group to identify all known systems at risk or compromised after distributing the participant handout.

Additionally, the feedback from the participants is a good way to discover deficiencies in the exercise and should be incorporated in the metrics. A more detailed version of the metrics can be obtained from Appendix D.

4. The Second Phase: Identification

The second most important step in handling an incident is identification. This step is similar to a battle that is part of a larger war. As outlined above, it is the first step in an iterative process and may need to be revisited many times throughout the handling of an incident. Failure to properly identify all affected systems can lead to further spread or compromise, usually requiring more time and resources needed to restore the systems to operation. Curran-Gardner had initially identified the compromised system. Early

reports implicated an IP in Russia based on evidence found in a log file (ICSB-11-327-01, 2011). What is not clear from the open-source reporting is if there were any other systems accessed by this IP address or if there were any other water pumps or equipment that failed around the same time. Figure 3, from Curran-Gardner's perspective, is the scope of the attack in this phase.

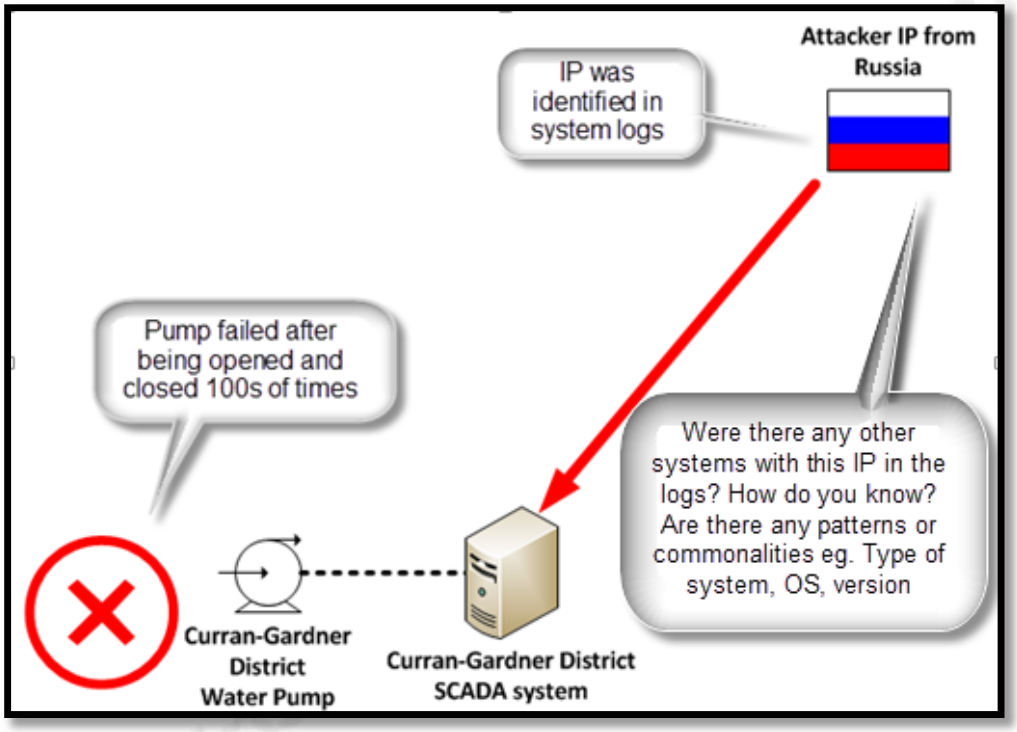


Figure 3. The identification phase in the Curran-Gardner incident.

In this step, it is imperative to identify all impacted systems and potentially impacted systems. Often, a Security Information and Event Management (SIEM) system is used for central logging and correlation. However, this information may not always be able to be sent to a SIEM from a SCADA system at the system level, due to a myriad of reasons, such as the age of system and limited functionality. Alternatively, network logs (firewall, proxy, router, or switch) traffic can be able to be used. In the case of SCADA system, network traffic, if visible, can provide a wealth of information. Failing to

identify all of the systems involved with an attack can have serious implications as the incident wears on. In the case of Curran-Gardner "unconfirmed information had already been leaked to the public, ICS-CERT and the asset owner/operator decided it was in the best interest of the community to collaboratively analyze all available data and disclose some of the findings" (ICSB-11-327-01, 2011). Jumping to conclusions early in the incident can be as damaging as not identifying all the affected systems. The tabletop exercise can help draw out critical thinking in terms of the extent of an attack.

4.1 Identification in a Tabletop

The identification phase in an exercise is extremely significant and can set the course of the tabletop. If this phase is done hastily, systems can be missed and patterns might be overlooked. In the exercise, this phase comes down to how well the participant guide is written. As the facilitator, the details should be as clear as possible without giving up the answer. For example, the exercise could establish that a foreign IP was discovered in the logs, but not necessarily present that the IP is from a particular country. This keeps the door open for critical thinking and may get the participants thinking more completely around that piece of information. A lightweight exercise, at the IT Director or VP level and above, should be in-depth enough to facilitate the tabletop, but not too disruptive with respect to time. Simply put, brevity can go a long way and achieve the desired result. A sample participant handout is included in Appendix B. At minimum the handout should include the following items:

- Background information on the organization (or mock organization). This will help participants get into character.
- Incident details of what is known at that point in time.
- What is being asked of the participants? Is there a need to prepare a report, draw up the attack diagram or make phone calls to remote participants?

One method that proved to work well was issuing a two-part handout. The first handout included certain details about the incident and was intended for the first part of the

exercise. After a short break, the second handout was distributed. This handout included additional information about the incident and also other issues or indicators, causing the participants to revisit the identification phase. The handout does not need to be 100% complete in terms of details. Rather, it is often beneficial to distribute pieces of information as the exercise unfolds.

4.2 Injects

One of the easiest ways to get additional details into the exercise is to introduce injects. An inject is a mechanism of revealing additional information that is either directly related to, or secondary to the incident. In the tabletop conducted, the following types of injects were used:

- Standard inject – An inject that has direct impact or relation to the exercise.
- Optional inject – An inject that does not relate to or causes FoW.

Similar to a real-life incident, injects allow for the facilitator the ability to control the flow of the exercise. If participants are skilled in incident response, this is a way to insert distractors that might cause further questions on what is known so far. It is also a way to introduce helpful information if he participants seem to be stuck on a particular aspect of the tabletop. It is important to map these injects out prior to the start of the incident. The inject should include a number, time of when it is to be introduced, and a detailed description. Additionally, the facilitator should have an understanding of which injects are optional or distractors, which is why it is good to include this information in the facilitator guide (found in Appendix C). Appendix D has a separate list of standard and optional injects used for the tabletop. The next phase, once the group has identified the affected systems, is containment.

5. The Third Phase: Containment

The containment phase focuses on minimizing the damage to the system or from the system that is implicated in the identification phase. Put another way, "the focus of this step is to limit the damage as soon as possible" (Kral, 2011). Curran-Gardner appears to have minimized the damage from the failed pump. According to the ICS-CERT report, "At no time were any water district customers impacted by the pump failure" (ICSB-11-327-01, 2011). Even though a pump failed, it did not have any impacts to the end customer. That fact alone highlights that a plan, albeit it simple, was instituted to restore operations. The problem with how the events unfolded and how they were reported, fail to show or rule out any other systems that might have also been attacked. This actually takes a step back to the previous phase of identification; however, it is only compounded in the containment phase. Failing to contain the issue could create more damage. Furthermore, it limits any proactive solutions to contain a future attack. Joe Weiss of Applied Control Solutions hits the nail on the head by stating, "It is unknown if other water system SCADA users have been attacked" (Weiss, 2011). In this real-life incident, there are several opportunities that should be exploited for success in regards to containment (see figure 4).

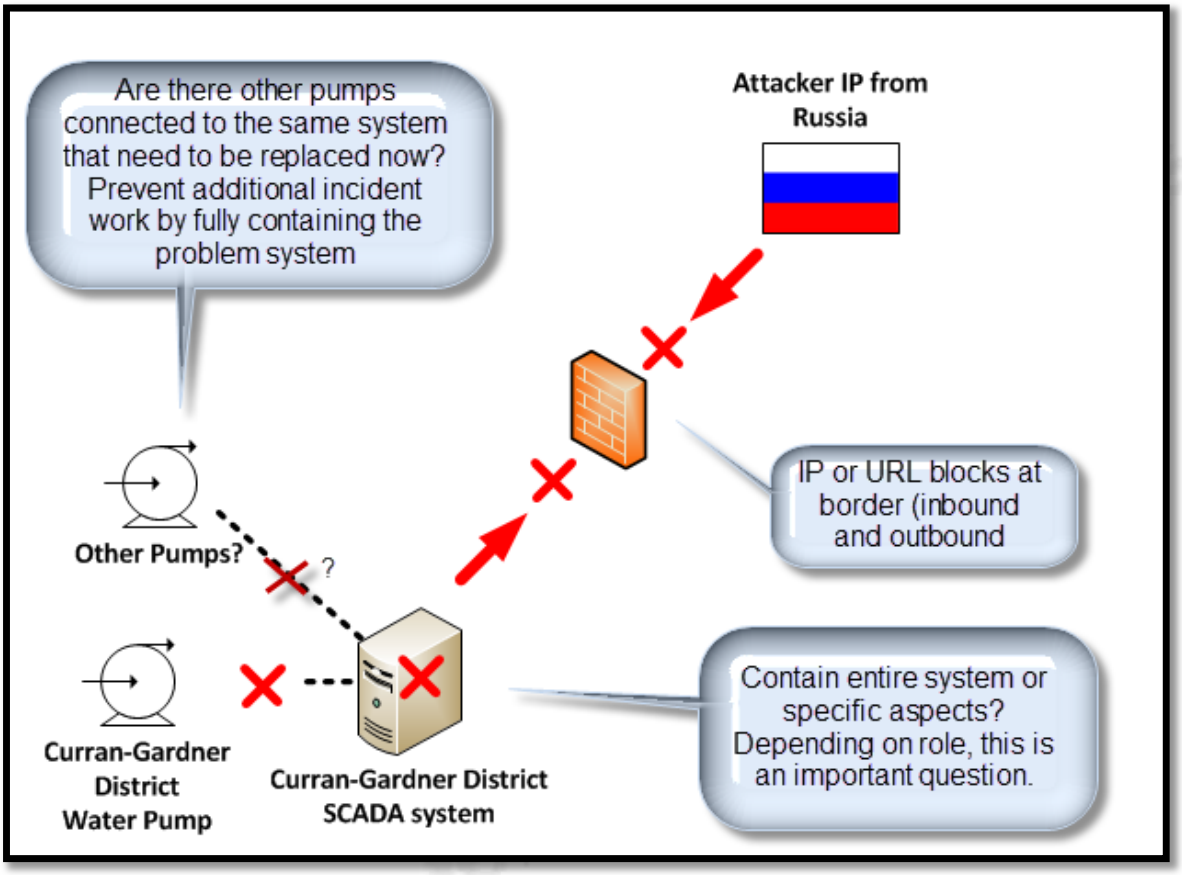


Figure 4. Containment in the context of the Curran-Gardner incident.

The containment phase is a key step in a real life and exercise alike.

5.1 Containment in a Tabletop

Just like in a real-life incident, containment focuses on minimizing the destruction by isolating the impacted systems. The exercise participants should be able to recommend steps to reduce the impact on the systems implicated in the incident, which is a natural progression if all of the systems have been identified. The problem is that not all systems can be contained due to business implications. The action can "range from doing nothing to full system shutdown (although full shutdown of an ICS [or SCADA system] is a highly unlikely response). The response taken will depend on the type of incident, and its effect on the ICS system and the physical process being controlled"

Matthew Hosburgh, matt.hosburgh@gmail.com

(Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2015). During the tabletop, based on this incident, our participants were given the opportunity to suggest containment ideas. A few of the suggestions were:

- URL or IP blocks.
- Network containment (disabling a port, blocking the system in a Network Access Control system, or isolated VLAN).
- Applying more restrictive firewall rules (in the case where operations cannot be impacted).

Although not all encompassing, these steps could be the first step in isolating the system(s). The participants came to their own conclusion about up time. They stated that having a plan ahead of time was critical, but even more beneficial was to have the response actions established. The point was made that it was vital to have an incident coordinator to keep the information flowing.

5.2 Monitoring the Containment (and Incident)

Information dissemination is an imperative and ongoing action during an incident. Having a good communications plan can drastically reduce the FoW in a real world incident. A lack of a plan will most certainly be highlighted in an exercise, which is why a tabletop is a necessity when developing an IR plan. In an interview with Chris Pierson, an attorney specializing in cyber security incident response, he states that the CISO must be the quarterback for the incident response. Furthermore, "all eyes, including those at the highest levels, are going to be on the CISO in terms of what people, internal and external, need to be brought in on the incident. It must be well dimensioned ahead of time" (Richards, 2014). Similar to a larger security program, there must be executive buy-in, especially when preparing a communications plan and how that information will flow before, during, and after the incident. This does not mean the CISO is the coordinator. It simply means that they need to be informed. In a real-world scenario, there would more than likely be a coordinator appointed who is closer to the "action",

reducing the telephone effect of the facts. Handling an incident in a vacuum will stifle resource engagement.

Monitoring an incident and reporting the status is central to resource engagement. In an exercise, this is a critical piece of understanding if the incident has been contained. If the response team is unaware that a network administrator or server admin has removed a system from the equation, it will be difficult to determine if the team can move forward to the next phase. For example, an exploited or infected SCADA server that caused a pump to fail should be contained to prevent further damage. If the system was not contained and the failed pump was replaced, there is a high probability that the pump would fail again. Communication that the server was contained helps to move the incident along. It can ensure that the proper steps are taken that will not require re-work or additional, redundant clean-up.

6. The Fourth Phase: Eradication

After the system has been isolated, it is ready for the next phase of eradication. Eradication can take on many depths and will be reliant on the scope of the attack, infection or even IR policy. It is unclear, with the supposed attack on the Illinois water pump attack, what steps were taken to remove the threat from their environment. It would be a safe assumption to say that the pump was replaced, at a minimum. If the logging capability was not comprehensive down to the host or server level, it would be difficult to determine what actually took place in terms of changes, exploits, or malware. That missing piece makes the eradication more difficult if cleaning is an option. On the other hand, it might make things simpler, which can be a policy mandate such as wipe, re-image, and restore from a known good back-up. In a SCADA environment, an infected system might be a candidate for an out-of-band hardware refresh if there is any doubt that a wipe and re-image would not eradicate the threat.

Matthew Hosburgh, matt.hosburgh@gmail.com

6.1 Eradication in a Tabletop

Eradication should be as realistic as possible, but appropriate for the exercise. When roles are assigned, such as a System Administrator, they can be called on or notified that action should be taken. A phone call or email could suffice for this step. Basically, once the systems have been identified and contained, it is time to start the clean-up. An email or phone call can be used to record when the action was taken in the context of the exercise and even be used as a data point for metrics. Another option would be for the facilitator to provide background information on the tools available to the team so that they can make a realistic recommendation. For example, if the organization had an effective response tool capable of cleaning or restoring the system to a known good state, that might be good enough for eradication in the tabletop. Because the incident handling steps are an iterative process, this phase should be looked at as a touch point for the exercise. Based on the findings, it is a good time to strengthen the defenses by removing the vulnerability that might have been exploited (Murdoch, 2014). Additionally, performing a vulnerability assessment is warranted to ensure that no other systems are impacted, such as verifying that a vulnerable version of the SCADA software is not present (Murdoch, 2014). If so, it should also be remediated before it too is taken advantage of. By leveraging the organization's tools, methodology, and policy, the more equipped the participants can be to address the real-world incidents in the environment. Once removed, it is now time to get things operating as they were.

7. The Fifth Phase: Recovery

Focusing on getting the organization's operations back online and free from an immediate incident is the ultimate goal. Failing to reach this step might mean that a larger Denial of Service (DoS) or rampant malware is running amuck. However, if the previous steps were successful, the "period of intensity" (Murdoch, 2014) should begin to subside. Looking to Curran-Gardner, the water treatment plant was able to restore normal business operations. It can be assumed that the failed pump was replaced in a timely manner because no customers were impacted, which is a good indicator that the previous steps

were handled correctly. Within the context of an exercise, this step could be as simple as a facilitator injecting information, based off of the containment and eradication steps, that the system has been recovered. Because no actual systems are in play during the tabletop, actual containment is a lot more expedient; however, it is still a good idea to run through the step so that the participants can see how each phase is integral in getting the organization back to normal operations. By examining the good and the bad of the exercise, the team can develop improvements to the tabletop and for real-world incidents that may be encountered in the future.

8. The Sixth Phase: Lessons Learned

A very key step when the dust settles after handling an incident is the lessons learned phase. This phase is the primary place to discuss what worked and did not work during the incident. During the tabletop, communication or information may be unclear, which can lead to cascading problems throughout. For that reason, it is good to highlight those issues. In the exercise performed within an actual organization, there were several lessons learned. The entire report can be found in Appendix F, but the summary of items found were:

Strengths were as follows:

- Well organized and facilitated
- Timely
- Cross platform participation (SCADA, IT, and Applications)
- Participants were engaged

Weaknesses of the exercise:

- No participation from teams or individuals outside of IT
- IT Security Team only facilitated and did not participate

Matthew Hosburgh, matt.hosburgh@gmail.com

- Actual systems were not tested, which may have added additional steps or issues while trying to contain or eradicate the threats.

These items help to figure out what steps should be taken to improve on the exercise in the future.

8.1 After Action Actions

By taking action based off of the feedback, the tabletop and real-world policies and procedures can be improved upon. "A man of words and not of deeds is like a garden full of weeds" (Green, n.d). The identified deficiencies throughout the exercise need to be put into action for the exercise to be of value to the organization. In the after action report (AAR) provided in Appendix F, there is a section that was used to collect the action items, who was assigned to the item and when it was due. If needed, a ticket might be opened and assigned to the respective participant for further action. Ideally, the item should be accomplished as soon as feasible and after being approved by the appropriate personnel. Another method for illustrating the value and effectiveness of an exercise is metrics.

8.2 Metrics

Collecting metrics throughout the duration of the exercise will help show the team's progress and help expose deficiencies in the tabletop. For an efficient tabletop, the metrics should be minimal, but enough to show the progress of the team in regards to the exercise. For the tabletop developed in parallel to the Curran-Gardner incident, the metrics collected were limited participant numbers, time it took to identify, contain and eradicate the threats. A running timer was kept during the exercise and the time was recorded when the team successfully completed an objective or metric enabled item. The overall performance of the group is shown in figure 5 and 6.

Matthew Hosburgh, matt.hosburgh@gmail.com

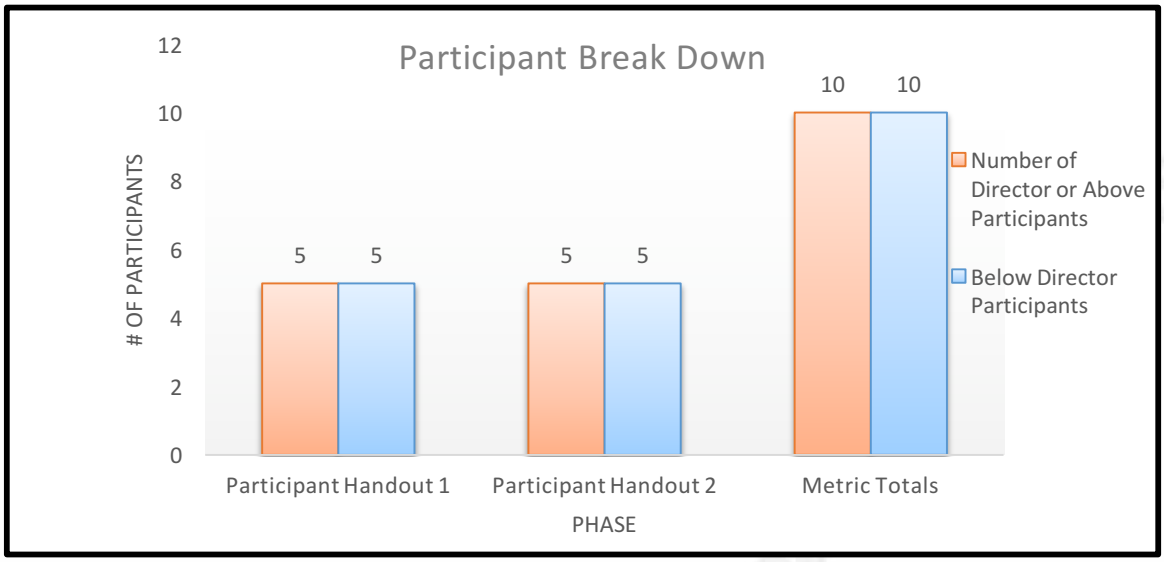


Figure 5. The metrics collected during the various stages of the exercise.

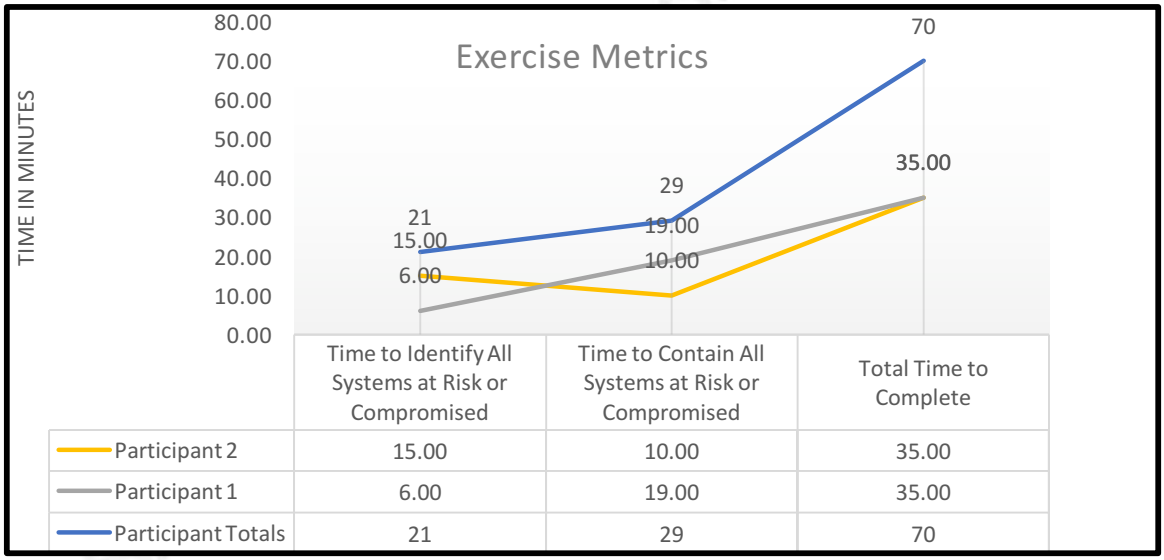


Figure 6. The metrics collected during the various stages of the exercise.

The next exercise conducted by the organization could be contrasted against these results to track the improvement of the response time. Ideally, the time metrics should go down and can be a direct result of the number of participants. More participants may not always be more efficient. For example 10 participants without properly defined roles, could cause delays and crosstalk during the tabletop.

Matthew Hosburgh, matt.hosburgh@gmail.com

Metrics and feedback provided from the participants can provide a wealth of information. When distributing participant feedback forms or evaluation, the facilitator and planning team can get insight into the exercise on a more detailed level. A participant may have had an issue that he or she did not want to bring up during the AAR discussion. With participant feedback, trends can be identified, and outliers can be made known. In the real-world exercise, the feedback from the participants was calculated and averaged as seen in figure 7.

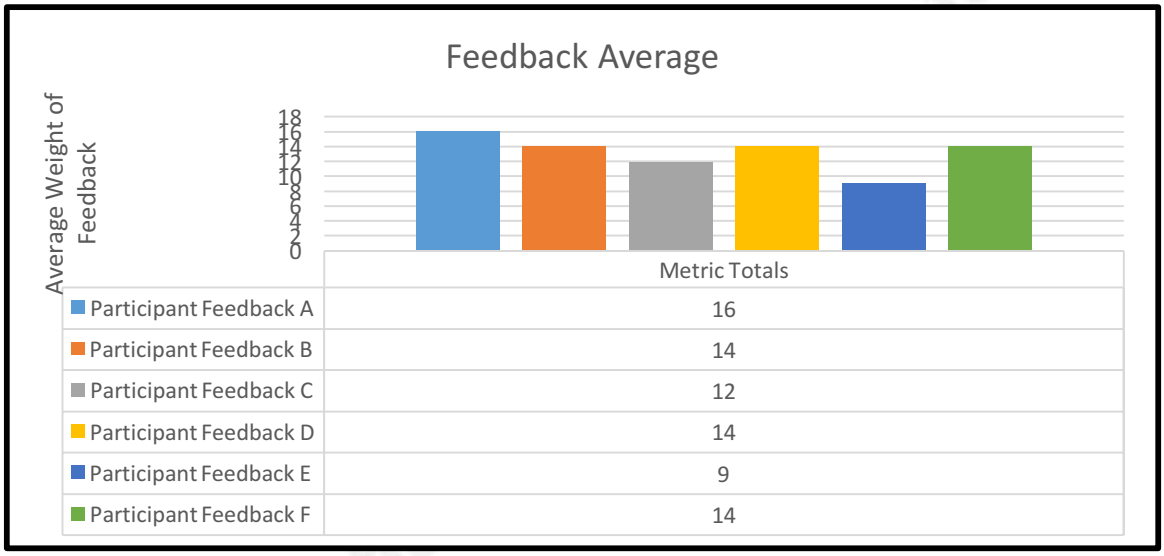


Figure 7. The average of the feedback questions after the exercise concluded.

From the graph, it is clear that question E was the lowest scoring question, which needs to be looked out. Question E was about including the right mix of people from the various teams. Because the exercise was targeted at the IT Director level, this feedback was not shocking; however, changes to future tabletops can be made based on this. For the sake of standardization, the feedback and metrics should be incorporated into the AAR, especially if there are action items required. By the end of the exercise, the critical thinking juices should be flowing and should be cultivated.

Matthew Hosburgh, matt.hosburgh@gmail.com

8.3 Threat Modeling

An impromptu threat modeling discussion can add another degree of value to the tabletop. By now the participants are thinking like a defender. This state of mind should not be neglected. If the organization does not have a formal threat modeling forum, the exercise can provide an excellent vehicle to facilitate this discussion. This discussion helps to answer the question of who is attacking, what are they after and what would be the implication should they succeed? "Intelligence-driven computer network defense [CND] is a risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations" (Hutchines, Cloppert, & Amin, n.d.). The value of a risk-based approach to the organization's threats can help to prioritize defense and response to incidents. Put another way, "The effect of intelligence-driven CND is a more resilient security posture" (Hutchines et al., n.d.). The tabletop is certainly an effective method for strengthening an organization's security posture by leveraging the people that need to be involved.

9. Conclusion

In summary, organizations need to be prepared to handle incidents. It is not a matter of if, but when the organization will fall victim. When SCADA systems are involved, the ability for the organization to deal with an incident becomes a necessity. The Curran-Gardner incident is a prime example of how an incident can be set off course if the wrong implications are made during the response phases. Curran-Gardner ultimately handled their incident in a manner to restore service and minimize damage to the organization. After further investigation, the Russian attacker was actually an authorized administrator accessing the SCADA system remotely from Russian IP space. Although Curran-Gardner was better off erring on the side of caution, the lessons learned from this incident can help other organizations better prepare for a real-life incident.

The tabletop exercise that was developed for an actual organization's SCADA systems was loosely based off of the Curran-Gardner incident. It follows the six incident

handling steps to help align with an existing incident response plan. It was developed to step participants through a lightweight and measureable exercise. The metrics collected provide immense value in improving on the tabletop and real-world policies and procedures. Finally, utilizing the exercise as a vehicle to conduct a brief threat modeling discussion can help bolster the value actually gleaned from an exercise. There are numerous moving parts to an incident that should always be considered. Organizations employing SCADA systems must have a plan to be able to effectively and accurately handle an incident that affect systems with kinetic abilities. Failure to do so can reap devastating consequences.

Matthew Hosburgh, matt.hosburgh@gmail.com

References

Bejtlich, R. (2013). The practice of network security monitoring: Understanding incident detection and response. No Starch Press.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 1). Computer Security Incident Handling Guide. Retrieved January 17, 2016, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

De Beaupre, A. (2011). Incident Response vs. Incident Handling. Retrieved January 17, 2016, from https://isc.sans.edu/diary/Incident Response vs. Incident Handling/6205

Green, P. B. (n.d.). A quote by Percy B. Green. Retrieved February 04, 2016, from http://www.goodreads.com/quotes/528482-a-man-of-words-and-not-of-deeds-is-like

Hutchines, E. M., Cloppert, M. J., & Amin, R. M. (n.d.). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved November 4, 2015, from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

ICSB-11-327-01 - ILLINOIS WATER PUMP FAILURE REPORT. (2011, November 23). Retrieved January 17, 2016, from https://ics-cert.us-cert.gov/tips/ICSB-11-327-01

Industrial Control Systems (ICS) Security Resources and Tools. (n.d.). Retrieved November 15, 2015, from http://www.chemicalcybersecurity.org/Cybersecurity-Tabletop-Exercise.zip

Kral, P. (2011, December 5). Incident Handler's Handbook. Retrieved January 17, 2016, from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Murdoch, D. (2014). Blue team handbook: Incident response edition: A condensed field guide for the cyber security incident responder (Version 2.0 ed.). United States: CreateSpace Independent Publishing.

Matthew Hosburgh, matt.hosburgh@gmail.com

Richards, K. (2014). Before and After: Don't Neglect Incident Response Management. Information Security, 16(10), 11-15.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015, February). Guide to Industrial Control Systems (ICS) Security. Retrieved January 25, 2016, from http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf

Weiss, J. (2011, November 17). Water System Hack - The System Is Broken. Retrieved January 25, 2016, from http://www.controlglobal.com/blogs/unfettered/water-system-hack-the-system-is-broken/

Matthew Hosburgh, matt.hosburgh@gmail.com

Appendix A

Incident Response Table Top Agenda

Date: mm-dd-yyyy

1) Introductions

a) Explain the roles for the exercise.

Role	Actions
Facilitator	The facilitator role will be filled by *individual*. This role will ensure: • The exercise is moving along • The running timer is set • Handouts and questions are explained and answered
Information Security Manager	The Information Security Manager is the conduit between the participants and the VP of IT. This individual will: • Answer questions related to the incident • Collect answers and action items to present to the VP of IT • Relay communications from higher-up to the participants
VP of IT	The VP of IT is in charge of IT, to include the Security Team. This individual will: • Relay information from the Information Security Manager to the CEO • Relay information from the CEO to the Information Security Manager
Participants	The participants will be anyone who does not have a specifically assigned role. They will: • Provide input on how to address the issues/incidents at hand • Collaborate with other team members • Use the whiteboard or other resources to diagram or document the problem (informal). • Ask questions if there is confusion.

Matthew Hosburgh, matt.hosburgh@gmail.com

Time	Role	Action
10 minutes	Facilitator	Background: • Introduction to facilitator and exercise (roles and IH Steps) • Goal of the session • Objectives
10 minutes	Facilitator	Phase 1: Introduce scenario: • *Individual* will be the Information Security Manager for the exercise. • Have the participants nominate a VP of IT. • *Individual* will be the CEO for the exercise. • Distribute Participant Handout 1. • Have participants read Handout 1. • Display On-Screen content (IH Steps)
35 minutes	Group	Phase 1: Discuss the scenario and work out an action plan: • What are the issues? • What are your priorities? • Who is affected and how? • Who else did you bring in? • What decisions did you make? • What is your action plan?
10 minutes	VP of IT	Present report to the CEO.
5 Minutes	Group	Break
10 minutes	Facilitator	Phase 2: Update scenario. • Distribute Participant Handout 2. • Have participants read Handout 2.
35 minutes	Group	Phase 2: Discuss scenario and update action plan. • What are the issues? • What are your priorities? • What decisions did you make? • What is your action plan?

Matthew Hosburgh, matt.hosburgh@gmail.com

10 minutes	CEO	Present report to the CEO.
20 minutes	Group	Lessons Learned: • What are we good at? • What knowledge, tools or processes need to improve? • Distribute feedback forms • Impromptu Threat Modeling
10 minutes	Facilitator	Wrap up.
Time: 2.5 hours		

b) Explain the incident handling steps (on screen).

2) Exercise Goals and Objectives

a) Goal: To improve the organization's incident response capabilities and communications when dealing with IT and IT based SCADA systems.

b) Objectives:
- **i)** Complete the incident response exercise within the allotted time.
- **ii)** Obtain director level participation in an exercise for the organization.
- **iii)** Identify all of the infected or compromised systems indicated in the scenario.
- **iv)** Contain all of the infected or compromised systems indicated in the scenario.
- **v)** Eradicate all of the infected or compromised systems indicated in the scenario.
- **vi)** Recover the system to pre-incident status or normal operations.
- **vii)** Discuss recommendations for improvements.

3) Timeline

Table Modified from the ICS-CERT Industrial Control Systems (ICS) Security Resources and Tools site

4) Discussion Items

a) Metrics – what we are being measured on
- **i)** Total time to complete
- **ii)** Number of participants
- **iii)** Time to identify all systems at risk or compromised
- **iv)** Time to notify and contain all known
- **v)** Time to eradicate

Matthew Hosburgh, matt.hosburgh@gmail.com

vi) Time to recover

b) Lessons Learned
- **i)** Discuss the good and bad
- **ii)** Process improvements

c) Action Items
- **i)** Feedback forms
- **ii)** Evaluation forms
- **iii)** Any remaining items

5) Closing

Appendix B

INCIDENT RESPONSE TABLE TOP PARTICIPANT HANDOUT 1 OF 2

Date: mm/dd/yyyy

1) Date/Time: January 4, 2016 / 10 PM MST

2) About the Organization

Company X a public company that is "engaged in the gathering, processing and transportation of natural gas; the transportation, fractionation, storage and marketing of NGLs; and the gathering and transportation of crude oil. *Company X's* datacenters reside in North America with numerous field sites (plants and offices) scattered throughout the United States.

From an IT and Security perspective, *Company X* employs numerous teams to support the organization. There is an IT department with smaller teams such as the Application, Network, Systems and Security Teams. The business (plant sites) operate 24 hours a day and 7 days a week. IT maintains a 40 hour work week with on-call assignments for after hour support.

Although many of the plants maintain their own control networks, there are portions of the network that might be bridged into the Supervisory Control and Data Acquisition (SCADA) network. The local control networks often have the capability to conduct basic control of the physical devices e.g. valves, pumps, etc.

A core business function for *Company X* is the availability of the plants and their ability to process natural gas. When a plant is unable to operate normally, the business loses money. Furthermore, there are safety concerns if a plant is not functioning properly. In many cases, safety mechanisms will prevent a catastrophe.

3) Current Issue

One of the *Company X's* plants in Oklahoma is reporting issues. A valve at the site failed and is currently causing a partial outage. The partial outage is preventing the processing of natural gas, which is causing a monetary loss for the company. Onsite engineers have been dispatched and are working to replace the valve.

Matthew Hosburgh, matt.hosburgh@gmail.com

About this same time, the Security Team received two alerts, both within short sequence of each other. There is some additional suspicious behavior noted around the same time. Right now, the two alerts look to be related to outbound traffic to a known botnet from a workstation (WKS-1234) and server (SVR-OPC-2) located in Colorado. Additionally, the two systems both have logs of going to the Schneider Electric website prior to the botnet traffic being observed.

The VP of Information Technology has asked for an initial report from the Information Security Manager of the situation within 15 minutes. He would like to know what happened, the scope of the issue and what action items the team is planning.

Matthew Hosburgh, matt.hosburgh@gmail.com

INCIDENT RESPONSE TABLE TOP PARTICIPANT HANDOUT 2 OF 2

Date: mm/dd/yyyy

1) **Date/Time:** January 5, 2016 / 9 AM MST

2) **Current Issue**

The CEO's laptop is now appearing to be part of the same botnet as identified by the Security Team yesterday. A recent phish report from his assistant indicates a suspicious email.

Further analysis by the Security Team indicates there is a link contained in the email with the following subject:

SUBJ: *Emergency Updat and Advisery by Schneider Electric READ NOW!*

Additional reports from the owner of the workstation WKS-1234 indicate that the user clicked on a link just prior to the botnet traffic appearing. The user said their screen flashed and their browser closed.

Shortly after the infection of SVR-OPC-2, an abnormal amount of traffic was observed by the Network Team going to SVR-VALVE-1, after WKS-1234 was observed scanning for open OPC ports.

SVR-VALVE-1located in Arkoma, Oklahoma is now being reported as down. A local technician has reported back to the Systems Team that the server is actually on but the screen appears frozen. A reboot of the system appears to have returned the system to normal operation.

A review of the log file on SVR-VALVE-1indicate that this system opened and closed the valve hundreds of times, which is why it presumably failed.

During this time, a report that gas volume is not "normal" as compared to the previous day.

The CEO is requesting another update due to the magnitude of this incident. The CEO has asked the VP of Information Technology for an update. The VP of Information Technology should plan on addressing how the incident response is progressing, how this

Matthew Hosburgh, matt.hosburgh@gmail.com

type of incident might be mitigated in the future, how much time and effort has gone into the and possibly who might be behind this attack.

Matthew Hosburgh, matt.hosburgh@gmail.com

Appendix C

INCIDENT RESPONSE TABLE TOP FACILITATOR GUIDE

Date: mm/dd/yyyy

Facilitator Note:

Metrics to collect:

a) *Number of Director or Above Participants:*
b) *Number of Participants:*
   Time to Identify All Systems at Risk or Compromised in Participant Handout 1 once clock has been started after the group has been given the okay to move forward:
c) *Time to Contain (or suggest a containment strategy) All Systems at Risk or Compromised in Participant Handout 1 once clock has been started after the group has been given the okay to move forward:*
d) *Total Time to Complete Participant Handout 1:*

Injects:

Standard Inject 1	*10 Min after handing out participant handout **1***	*The server that had an alert appears to have a SCADA function. Its name is WKS-1234 and is presumably an Open Platform Communications (OPC) server.*
Standard Inject 2*	*20 Min after handing out participant handout **1***	*The Service Desk is reporting that about 10 users had to reset their username and password to access the VPN. This seems a bit out of place at 10:30 PM.*
Standard Inject 3	*25 Minutes after handing out participant handout **1***	*The field technician reports that the system has 2 network interface cards (NICs). After a reboot, the system appears to have returned to normal operation.*

1) **Date/Time:** January 8, 2016 / 10 PM MST

2) **About the Organization**

Company X a public company that is "engaged in the gathering, processing and transportation of natural gas; the transportation, fractionation, storage and marketing of NGLs; and the gathering and transportation of crude oil. *Company X's* datacenters reside in North America with numerous field sites (plants and offices) scattered throughout the United States.

Matthew Hosburgh, matt.hosburgh@gmail.com

From an IT and Security perspective, *Company X* employs numerous teams to support the organization. There is an IT department with smaller teams such as the Application, Network, Systems and Security Teams. The business (plant sites) operate 24 hours a day and 7 days a week. IT maintains a 40 hour work week with on-call assignments for after hour support.

Although many of the plants maintain their own control networks, there are portions of the network that might be bridged into the Supervisory Control and Data Acquisition (SCADA) network. The local control networks often have the capability to conduct basic control of the physical devices e.g. valves, pumps, etc.

A core business function for *Company X* is the availability of the plants and their ability to process natural gas. When a plant is unable to operate normally, the business loses money. Furthermore, there are safety concerns if a plant is not functioning properly. In many cases, safety mechanisms will prevent a catastrophe.

3) Current Issue

One of the *Company X's* plants in Oklahoma is reporting issues. A valve at the site failed and is currently causing a partial outage. The partial outage is preventing the processing of natural gas, which is causing a monetary loss for the company. Onsite engineers have been dispatched and are working to replace the valve.

About this same time, the Security Team received two alerts, both within short sequence of each other. There is some additional suspicious behavior noted around the same time. Right now, the two alerts look to be related to outbound traffic to a known botnet from a workstation (WKS-1234) and server (SVR-OPC-2) located in Colorado. Additionally, the two systems both have logs of going to the Schneider Electric website prior to the botnet traffic being observed.

Facilitator Note:

The valve shutdown is very suspicious and a cyber-attack is highly suspected.

The initial infection vector appears to have come from an infected vendor site, hosting an exploit kit. Once users browse to the infected site with a vulnerable browser and operating system, they are infected. After successful infection, the workstation/server will begin to beacon to a command and control IP.

Identify Infected: WKS-1234 and server SVR-OPC-2

Matthew Hosburgh, matt.hosburgh@gmail.com

The VP of Information Technology has asked for an initial report from the Information Security Manager of the situation within 15 minutes. He would like to know what happened, the scope of the issue and what action items the team is planning.

Facilitator Note:

Need to identify the two infected systems: WKS-1234 and server SVR-OPC-2
Need to contain the two infected systems and prevent further infection.

Possible ideas for containment: move systems to "infected" VLAN, disconnect network connection (Network Team), disable in NAC, or power off. Add infected URL to blacklist. Might be good to notify vendor so other users/customers do not get infected.

Possible remediation ideas: wipe and reimage, image device and submit to ICS-CERT for forensic investigation.

PART 2
Facilitator Note:

Metrics to collect:
a) *Number of Director or Above Participants:*
b) *Number of Participants:*
Time to Identify All Systems at Risk or Compromised in Participant Handout 2 once clock has been started after the group has been given the okay to move forward:
c) *Time to Contain (or suggest a containment strategy) All Systems at Risk or Compromised in Participant Handout 2 once clock has been started after the group has been given the okay to move forward:*
d) *Total Time to Complete Participant Handout 2:*

Injects:

Standard Inject 4*	*10 Minutes after handing out participant handout **2***	*The user network and a financial application have been reported running slower than usual.*
Standard Inject 5	*15 Minutes after handing out participant handout **2***	*Daily "Volume & Energy" Interface from marketing system fails to reconcile correctly.*

1) **Date/Time:** January 5, 2016 / 9 AM MST

2) **Current Issue**

The CEO's laptop is now appearing to be part of the same botnet as identified by the Security Team yesterday. A recent phish report from his assistant indicates a suspicious email.

Matthew Hosburgh, matt.hosburgh@gmail.com

Facilitator Note: The CEO in this case looks to have clicked the link and did report the email to the Security Team.

Infected: CEO's Laptop

Further analysis by the Security Team indicates there is a link contained in the email with the following subject:

SUBJ: *Emergency Updat and Advisery by Schneider Electric READ NOW!*

Facilitator Note: It looks like this attack is more than just an infected vendor website. Rather, the email noted above was sent directly to the CEO, which also contained a link to the infected website. Once the link is clicked, the target user would become infected. This indicates a targeted attack. Additional indicators that this email is fake is the misspellings.

Additional reports from the owner of the workstation WKS-1234 indicate that the user clicked on a link just prior to the botnet traffic appearing. The user said their screen flashed and their browser closed.

Facilitator Note: Another indicator that several users were targeted.

Shortly after the infection of SVR-OPC-2, an abnormal amount of traffic was observed by the Network Team going to SVR-VALVE-1, after SVR-OPC-2was observed scanning for open OPC ports.

Facilitator Note: The next stage of this attack looks to conduct scanning for OPC systems. Once one is found, the attacker zeros in on the real targets.

From Inject: A new report from the Security Team indicates that the daily "Volume & Energy" interface from marketing system fails to reconcile correctly.

Facilitator Note: In addition to the OPC system, the attacker seems to be going after financial or marketing systems.

Infected: marketing system

SVR-VALVE-1 located in Oklahoma is now being reported as down. A local technician has reported back to the Systems Team that the server is actually on but the screen appears frozen. A reboot of the system appears to have returned the system to normal operation.

Matthew Hosburgh, matt.hosburgh@gmail.com

Facilitator Note: The attacker looks to have further exploited the SVR-VALVE-1 system with some sort of exploit, enabling remote access. After issuing hundreds of commands (scripted presumably), the system hangs due to the buggy exploit. When the local support person rebooted the system, the server was reset to a normal state.

A review of the log file on SVR-VALVE-1 indicate that this system opened and closed the valve hundreds of times, which is why it presumably failed.

Facilitator Note: A targeted attack, traversing the network is the ultimate cause of the valve failure. What is not known is who is behind the attack or why they would want to attack us.

The CEO is requesting an update due to the magnitude of this incident. The CEO has asked the VP of Information Technology for an update. The VP of Information Technology should plan on addressing how the incident response is progressing, how this type of incident might be mitigated in the future, how much time and effort has gone into the and possibly who might be behind this attack.

Facilitator Note:

Need to identify the two infected systems: CEO's Laptop, SVR-VALVE-1, Marketing system
Need to contain the three infected systems and prevent further infection:

Possible ideas for containment: move systems to "infected" VLAN, disconnect network connection (Network Team), disable in NAC, or power off. Add infected URL to blacklist. Might be good to notify vendor so other users/customers do not get infected.

Possible remediation ideas: wipe and reimage, image device and submit to ICS-CERT for forensic investigation.

Appendix D

INCIDENT RESPONSE TABLE TOP PARTICIPANT INJECTS

Date: mm/dd/yyyy

1. Standard Injects

#	Time	Description
Standard Inject 1	10 Min after handing out participant handout **1**	The server that had an alert appears to have a SCADA function. Its name is SVR-OPC-2 and is presumably an Open Platform Communications (OPC) server.
Standard Inject 2*	20 Min after handing out participant handout **1**	The Service Desk is reporting that about 10 users had to reset their username and password to access the VPN. This seems a bit out of place at 10:30 PM.
Standard Inject 3	25 Minutes after handing out participant handout **1**	The technician at Arkoma reports that the system has 2 network interface cards (NICs). After a reboot, the system appears to have returned to normal operation.
Standard Inject 4*	10 Minutes after handing out participant handout **2**	The user network and a financial application have been reported running slower than usual.
Standard Inject 5	15 Minutes after handing out participant handout **2**	Daily "Volume & Energy" Interface from marketing system fails to reconcile correctly.

** Fog of War (FoW)*

Matthew Hosburgh, matt.hosburgh@gmail.com

Appendix E

INCIDENT RESPONSE TABLE TOP PARTICIPANT FEEDBACK FORM

Date: mm/dd/yyyy

The Participant Feedback Form and will be analyzed and utilized to improve future iterations of this, and the creation of other exercises.

The Participants were asked to rate the following questions based on the given scale. Please rate the same from the Planner/Facilitator point of view. Space has been made available after each question for additional comments and to summarize Participant views.

	Assessment Factor	**Exercise Satisfaction Rating** *Strongly Disagree* 1	2	3	4	5 *Strongly Agree*
a.	The exercise was well structured and organized.	☐	☐	☐	☐	☐
b.	The exercise scenario was plausible and realistic.	☐	☐	☐	☐	☐
c.	The documentation used during the exercise was a valuable tool throughout the exercise.	☐	☐	☐	☐	☐
d.	Participation in the exercise was appropriate for someone in my position.	☐	☐	☐	☐	☐
e.	The participants included the right people in terms of level and mix of disciplines.	☐	☐	☐	☐	☐

Matthew Hosburgh, matt.hosburgh@gmail.com

Assessment Factor	Exercise Satisfaction Rating *Strongly Disagree*				*Strongly Agree*
f. The presenter was well organized and communicated clearly.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐

2. What changes would you make to improve this exercise?
Please provide any recommendations on how this exercise or future exercises could be improved or enhanced.

3. Please calculate the average scores on each question and populate the database based on the following formula:
Participant response summed per question = Average score
# of Participants

Example: Question "a. The exercise was well structured and organized?"
# of Participants: 20
Responses: **5:**15 **4:**3 **3:**1 **2:**1 **1:**0 Responses summed: 15x5 = 75

92/20 = 4.6

Question "a" has an average score of **4.6**

3x4 = 12
1x3 = 3
1x2 = 2
0x1 = 0
92

Question	Ratings according to Participant 5	4	3	2	1	Average
a						
b						
c						
d						
e						
f						

(Industrial Control, n.d.).

Appendix F

Impact Metrics from Actual Exercise

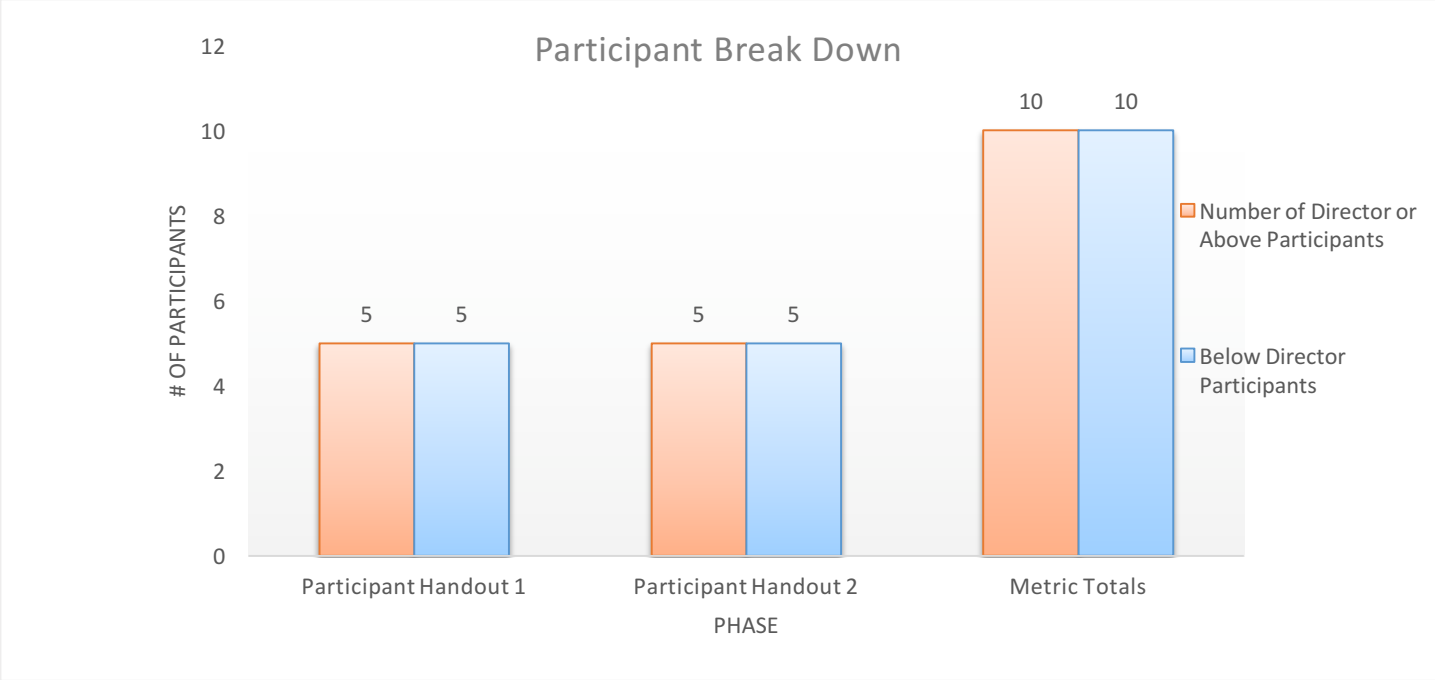
Matthew Hosburgh, matt.hosburgh@gmail.com

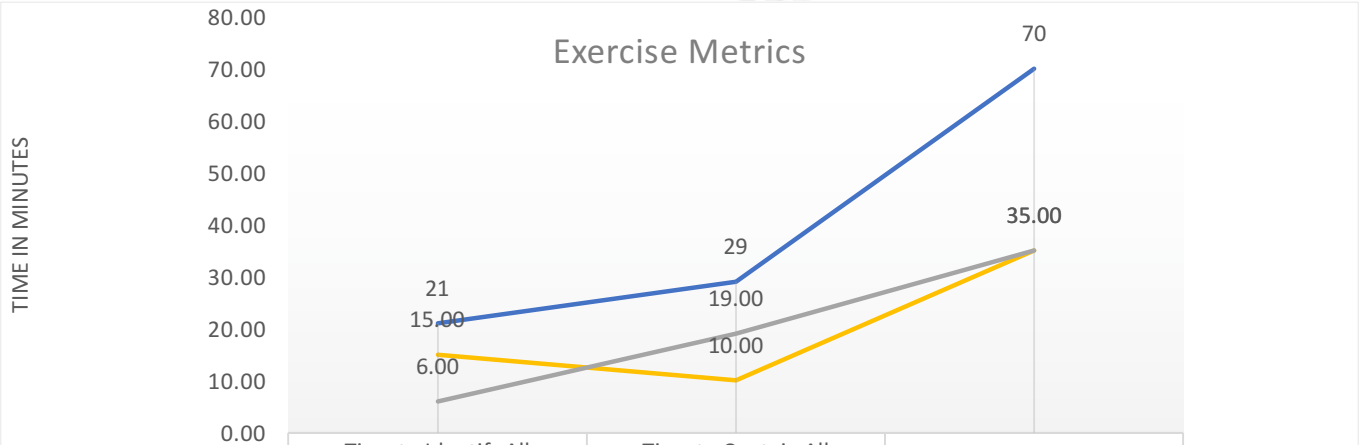
Metric Name	What Is Measured	How It Is Measured	Participant Handout 1	Participant Handout 2	Metric Totals
Number of Director or Above Participants	Number of participants at the director level or above.	Physical (in the room) and Virtual (any participants via chat or phone)	5	5	10
Number of Director or Below Participants	Number of participants below the director level.	Physical (in the room) and Virtual (any participants via chat or phone)	5	5	10
Time to Identify All Systems at Risk or Compromised	Time it takes for the group to identify all known systems at risk or compromised after distributing the participant handout.	Timer started when the participant handout is given	6.00	15.00	21
Time to Contain All Systems at Risk or Compromised	Time it takes for the group to identify all known systems at risk or compromised after distributing the participant handout.	Timer started when the participant handout is given	19.00	10.00	29
Total Time to Complete	Overall time that the exercise took to complete	Overall running timer	35.00	35.00	70
Exercise Totals			3.5	3.5	3.5

Participant Feedback Metrics from Actual Exercise

Metric Name	What Is Measured	How It Is Measured	Metric Totals
Participant Feedback A	The feedback received from the participants	Averaging the responses per question	16
Participant Feedback B	The feedback received from the participants	Averaging the responses per question	14
Participant Feedback C	The feedback received from the participants	Averaging the responses per question	12
Participant Feedback D	The feedback received from the participants	Averaging the responses per question	14
Participant Feedback E	The feedback received from the participants	Averaging the responses per question	9
Participant Feedback F	The feedback received from the participants	Averaging the responses per question	14

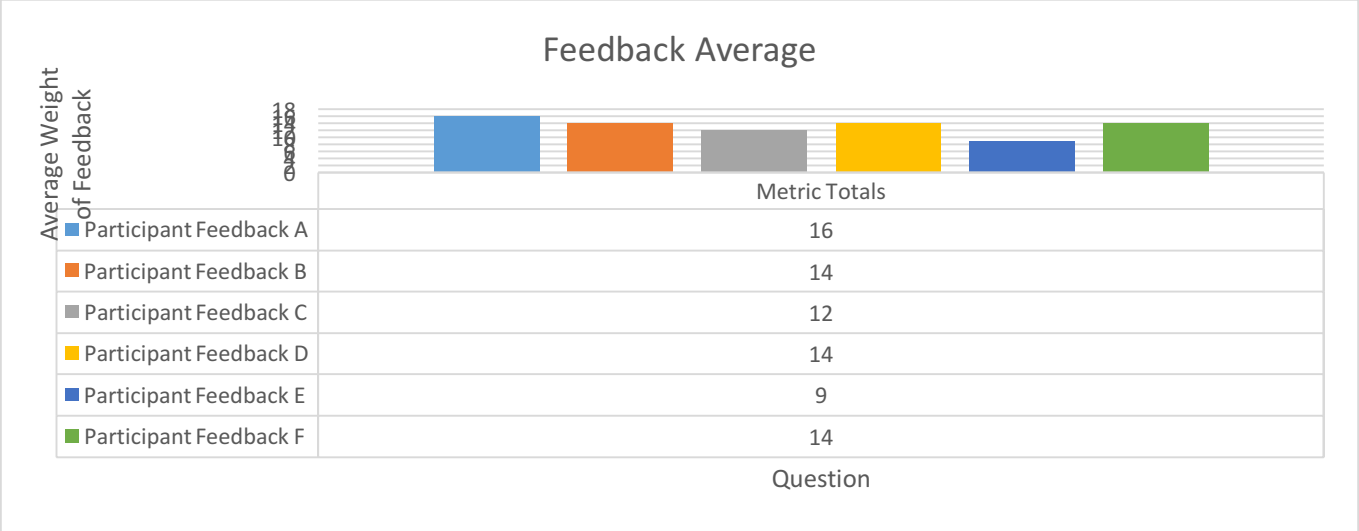
Matthew Hosburgh, matt.hosburgh@gmail.com





	Time to Identify All Systems at Risk or Compromised	Time to Contain All Systems at Risk or Compromised	Total Time to Complete
Participant 2	15.00	10.00	35.00
Participant 1	6.00	19.00	35.00
Participant Totals	21	29	70

Matthew Hosburgh, matt.hosburgh@gmail.com



Matthew Hosburgh, matt.hosburgh@gmail.com

Appendix F

INCIDENT RESPONSE TABLE TOP AFTER ACTION REPORT & LESSONS LEARNED

Date: mm/dd/yyyy

4) Summary

a) Explain what the scenario was about.

The Proton Torpedo 2016 table top exercise was conducted on January 8, 2016. Consisting of primarily of IT Directors, VPs and key SCADA system personnel, the exercise was kept small, due to time constraints.

The exercise depicted a scenario where a targeted attack occurred on the organization. The difference between this incident and a "normal attack" was that there were SCADA systems involved that caused a kinetic reaction. In this case, a valve that was attached to a SCADA system failed. Furthermore, a marketing application were both targeted, which added a degree of complexity to the scenario.

The scenario was broken up into two major parts. In the first section, general details were learned via the Participant Guide 1 of 2, which walked the participants through the major symptoms and alerts that were known at that time. The initial infection and alerts were deemed to be from an infected vendor site. After the infection, the workstation or server would begin to beacon out to a known command and control site.

The second section began to provide more details as they were learned via the Participant Handout guide 2 of 2. The major findings were that the spear phishing attacks were also launched to further infect users. In particular, the CEO of the organization received an email that linked back to the known malicious site. Additionally, there was notable OPC scanning taking place, which suggested the type of system that was being targeted. At the end of the scenario, it was discovered that the valve failed because the SCADA server attached to the valve opened and closed the valve hundreds of times, which is why it failed.

Various injects along the way implicated additional systems in the incident. Some of the injects presented were only to cause confusion or Fog of War e.g. the expired VPN user passwords.

Matthew Hosburgh, matt.hosburgh@gmail.com

b) Strengths of the exercise.

According to feedback, the strengths were as follows:

- Well organized and facilitated
- Timely
- Cross platform participation (SCADA, IT and Applications)
- Participants were engaged

c) Weaknesses of the exercise.

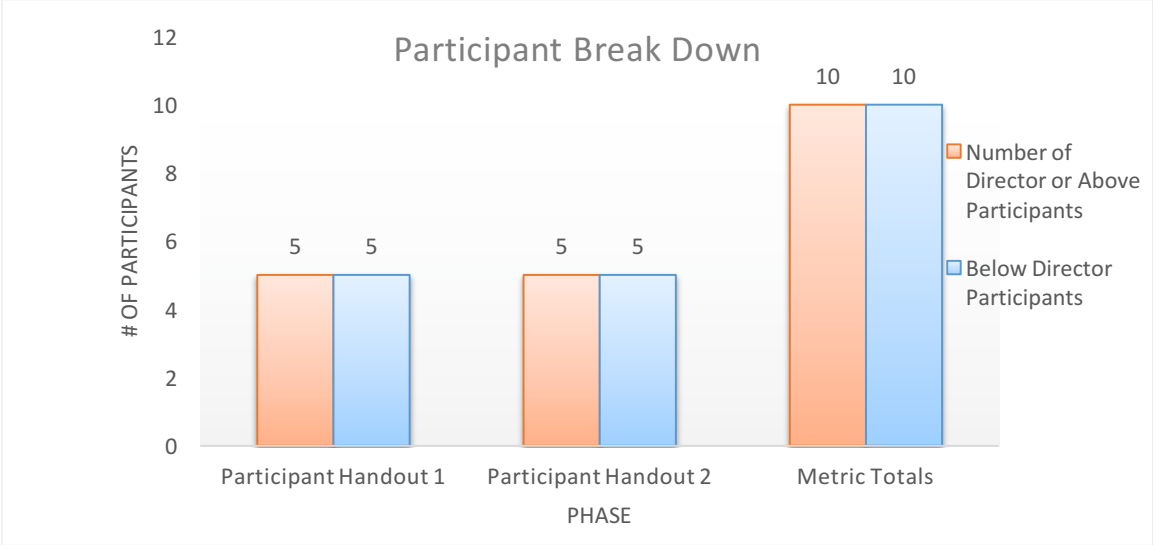
- No participation from teams or individuals outside of IT
- IT Security Team only facilitated and did not participate
- Actual systems were not tested, which may have added additional steps or issues while trying to contain or eradicate the threats.

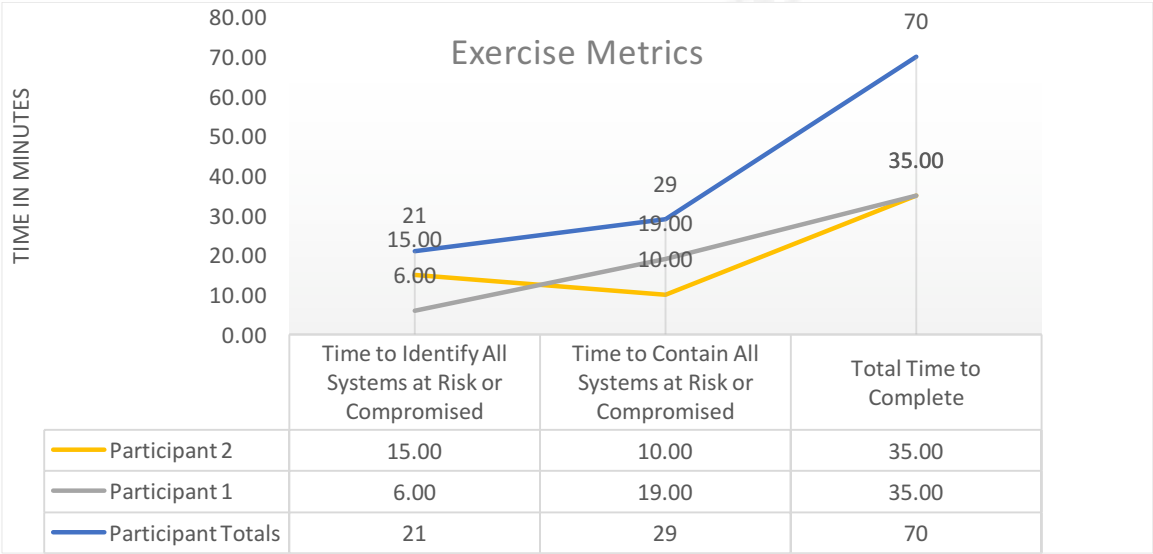
d) Explain whether or not the objectives were met.

1. All objectives were successfully met.

- Completed the incident response exercise within the allotted time.
- Obtained director level participation in an exercise for the organization.
- Identified all of the infected or compromised systems indicated in the scenario.
- Contained all of the infected or compromised systems indicated in the scenario.
- Eradicated all of the infected or compromised systems indicated in the scenario.
- Restored the system to pre-incident status or normal operations.
- Discussed recommendations for improvements.

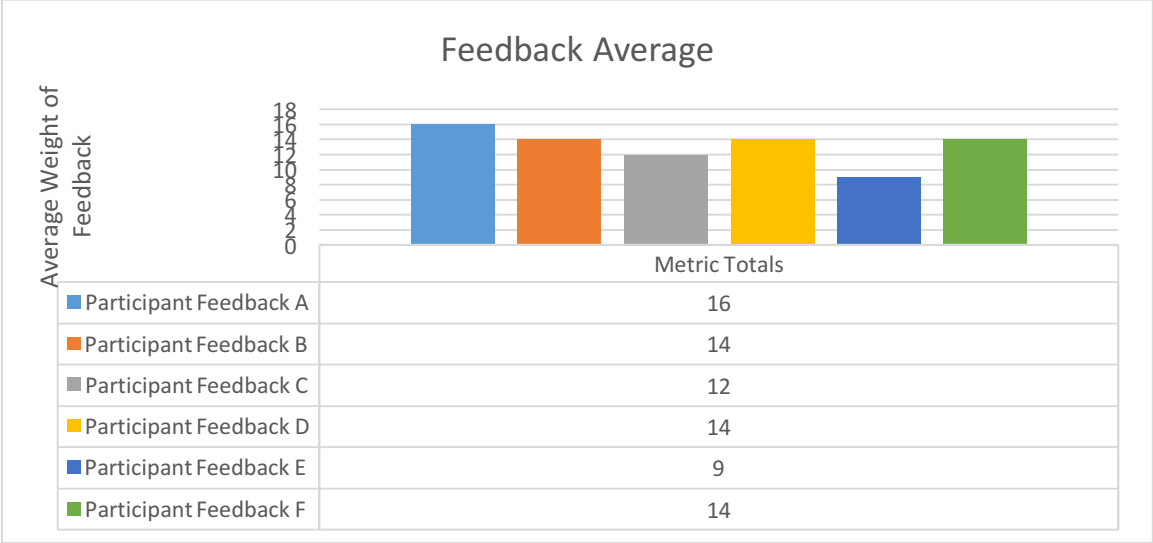
Additionally, the following metrics were captured:





	Time to Identify All Systems at Risk or Compromised	Time to Contain All Systems at Risk or Compromised	Total Time to Complete
Participant 2	15.00	10.00	35.00
Participant 1	6.00	19.00	35.00
Participant Totals	21	29	70

Matthew Hosburgh, matt.hosburgh@gmail.com



5) Action Items

Item Number	Assignee	Due Date	Action Item
1	Bob Smith	2/1/2016	Update slides 2 & 3 with new logo
2	Susie Que	2/15/2016	Update the Incident Response plan with new step to contain mobile devices and particular SCADA systems as detailed in the exercise
3	Steve Jobs	2/1/2016	Review the notification plan to ensure that all roles and responsibilities are up-to-date
4	Mike Gates	2/10/2016	Based on the feedback from question E, update plan for next exercise to incorporate discrepancy discovered

Matthew Hosburgh, matt.hosburgh@gmail.com