DEVELOPMENT OF A HYBRID EXERCISE FOR ORGANIZATIONAL CYBER RESILIENCE

YUITAKA OTA, ERIKA MIZUNO, KOKI WATARAI, TOMOMI AOYAMA,
TAKASHI HAMAGUCHI, YOSHIHIRO HASHIMOTO & ICHIRO KOSHIJIMA
Nagoya Institute of Technology, System Management and Engineering, Japan

ABSTRACT

In recent years, COTS (commercial off the shelf, such as Windows OS, Intel PC, and open source applications) have been proposed to reduce the cost of deploying operational technology (OT) systems. Also, DX efforts are being made to shift from physical operation to virtual operation by using virtualization with IoT, AI, and cloud servers. Current ransomwares, therefore, infect without distinguishing between IT systems and OT systems. For example, in May 2021, the Colonial Pipeline Company, a major oil pipeline company in the United States, was infected with ransomware and shut down its pipeline operation. As a countermeasure against cyberattacks, many companies focus on creating a less vulnerable environment. However, attackers exist worldwide, and they are constantly searching for new attack surfaces and developing new attack methods. It is also difficult for defenders to prevent all attacks, no matter what measures they take. Therefore, companies need to educate employees to ensure the safety of their factories in the event of a cyberattack. The authors developed a series of table-top BCP (business continuity plan) exercises to acquire the meta-knowledge necessary to respond to cyberattacks targeting the OT system for the above reasons. However, we found that the learning effect of these exercises depended on how the participants imagined cyberattacks. Therefore, in this paper, we propose a hybrid learning system that combines cyberattack simulations and table-top BCP exercises to increase the cyber resilience of participants.

Keywords: cyber-incident, cyber resilience, business continuity plan, exercise.

1 INTRODUCTION

It is essential to recognize that cyberattacks are conducted against information technology (IT) systems, such as credit card fraud and information leakage, and against the operational technology (OT) systems used to operate plants. Since the cyberattack on the controller of a uranium enrichment plant not connected to the external net was discovered in 2010 [1], the number of cyberattacks on OT systems has increased every year [2]. Moreover, the HatMan malware [3], which targets controllers and safety instrumentation, was discovered in Saudi Arabia in 2019. In addition, in May 2021, a pipeline in the United States [4] was damaged by an attack not on the plant but on the management system that controls the plant, making it impossible to provide service for an extended period of time. Accordingly, companies that own plants must not only respond to cyberattacks on IT systems to continue their businesses but must also take measures against cyberattacks on OT systems in a way that considers their plants and the series of systems used to operate these plants.

1.1 Approaches to security measures targeting OT systems

To minimize damage from cyberattacks, many companies have now focused on building environments that are less vulnerable to cyberattacks, for example, introducing mail checkers, whitelists, and information security training for employees.

However, there are attackers worldwide and new vulnerabilities are discovered and reported every day [5], [6]. In addition, the reported vulnerabilities are only a fraction of the total, and there remains a high possibility of attacks (zero-day attacks) using unreported vulnerabilities. In other words, no matter how much a company takes measures to build an

WIT Transactions on The Built Environment, Vol 206, © 2021 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE210051

environment that is resistant to cyberattacks, it is impossible to reduce the possibility of cyberattacks to zero. We believe that in order for companies to respond to cyberattacks targeting OT systems, the following two points are required, based on the assumption that cyberattacks will occur, to build an environment that is resistant to cyberattacks.

- **Formulation of an industrial control system (ICS)-business continuity plan (BCP) considering cyberattacks**
  Usually, in companies that own plants, the production department prepares a safety-BCP for physical problems such as fires, spills of hazardous materials, and natural disasters and conducts drills based on this plan. In addition, the information system department develops an IT-BCP to deal with cyber-incidents on the business network, including information leakage. A cyberattack on an OT system uses IT systems to attack the target OT system to damage the plant or stop the services of a company. Therefore, it is essential to analyze the risks considering cyberattacks that can cause damage across OT and IT systems and to create a plan in advance to minimize the damage of such risks.
- **Human resource development**
  Even if an ICS-BCP is developed, if the employees who respond to incidents cannot do so, the damage from cyberattacks cannot be minimized. Therefore, companies need to educate their employees to respond based on the plan that they have developed.

However, many Japanese companies may have experience dealing with cyber-incidents involving IT systems but have little experience with cyber-incidents involving OT systems. Without sufficient experience with cyber-incidents targeting OT systems, it is not easy to understand the impact of cyberattacks on OT systems and imagine the actions that need to be taken in the event of such an incident. This makes it difficult for companies to formulate ICS-BCPs for OT systems and develop human resources.

1.2 Approaches to gaining experience with cyber-incidents

To get an accurate picture of cyberattacks, companies need to experience responding to cyber-incidents. However, as mentioned above, there are few opportunities to experience cyberattacks.

Thus, to address this issue, we developed an exercise to experience a simulated control system cyber-incident to help company personnel increase their experience with cyber-incidents and acquire the meta-knowledge necessary to respond to cyberattacks targeting OT systems. We developed a hybrid exercise that combines a table-top format with an operational simulation format using a simulated plant. The effectiveness of the hybrid exercise is enhanced because the exercise participants gain a better image of a cyberattack on an OT system.

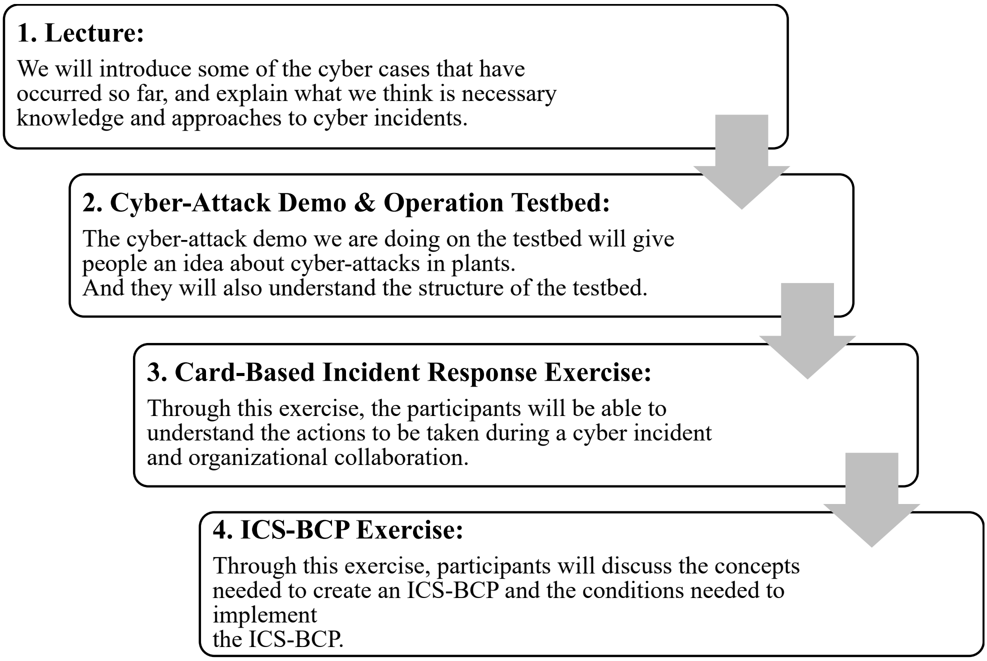
2 EXERCISES TO UNDERSTAND SAFETY RESPONSES

The purpose of this exercise is to understand how a cyberattack targeting OT systems affects a plant and to learn the actions (safety responses) and concepts required to make the plant safe after it has been rendered insecure by the cyberattack.

2.1 Structure of the exercises

This exercise is a combination of simulation exercises (cyberattack demo and operation testbed) based on our testbed and table-top exercises (card-based incident response exercise and ICS-BCP exercise). In this combination, we examine how a company would respond to a cyberattack as a member of a virtual company (card-based incident response exercise and ICS-BCP exercise).

Fig. 1 shows the objectives of each exercise and the flow for conducting the exercises. The exercise participants have different backgrounds in terms of work experience and knowledge. Prior to the exercise, classroom lectures are conducted in order to prepare the learning base of the exercise participants. Then, the participants operate the testbed to perform start-up, steady-state operations, and emergency operations. We deepen their understanding of plants and OT systems using these simulation exercises. Next, they engage in organizational collaboration during cyber-incidents via table-top-style exercises. By experiencing this sequence of events, the exercise participants deepen their knowledge of cyberattacks on OT systems and understand the safety responses required to make a plant safe.



1. Lecture:
We will introduce some of the cyber cases that have occurred so far, and explain what we think is necessary knowledge and approaches to cyber incidents.

2. Cyber-Attack Demo & Operation Testbed:
The cyber-attack demo we are doing on the testbed will give people an idea about cyber-attacks in plants.
And they will also understand the structure of the testbed.

3. Card-Based Incident Response Exercise:
Through this exercise, the participants will be able to understand the actions to be taken during a cyber incident and organizational collaboration.

4. ICS-BCP Exercise:
Through this exercise, participants will discuss the concepts needed to create an ICS-BCP and the conditions needed to implement
the ICS-BCP.

Figure 1: Relationship between the exercises.

2.2 Simulation exercises

This exercise aims to help participants understand the steps involved in a cyberattack on an OT system and how it can affect the plant via the network. The exercise participants observe a cyberattack demonstration on the testbed (Fig. 2) in our laboratory. In this cyberattack demonstration, the OT system operating the plant is attacked via the Internet through the IT system, and the control equipment of the plant is damaged. Then, the exercise participants experience the start-up, shutdown, and emergency operations of the testbed by themselves. In this experience, participants deepen their understanding of the relationship between the plant and the controller and the communication flow between the OT systems (e.g., the data management server, human–machine interface, and data-historian server) built to operate the plant. This simulation gives the exercise participants an idea of the actions that need to be taken to keep the plant safe and operational during a cyber-incident and the locations from which the effects of the cyber-incident need to be removed.

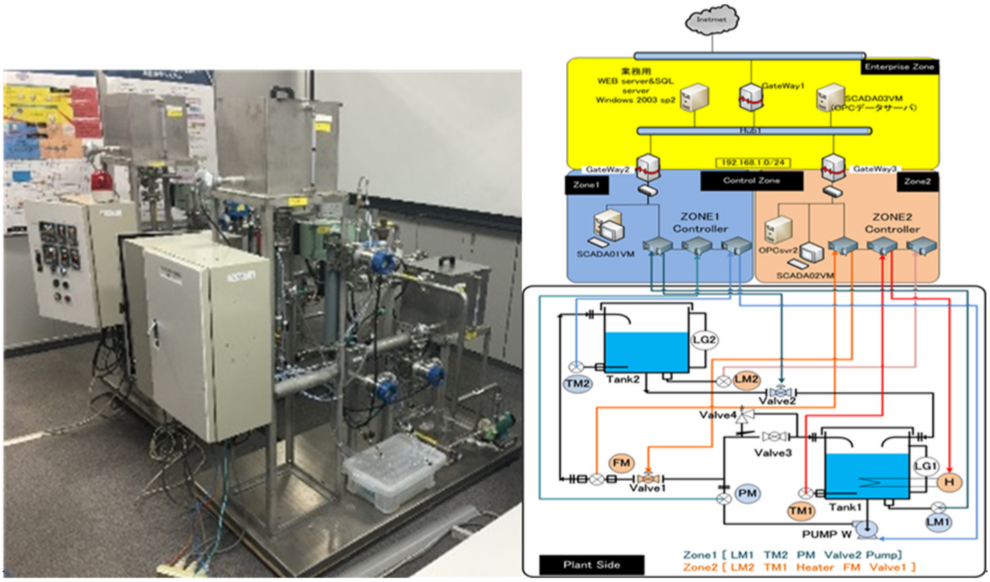
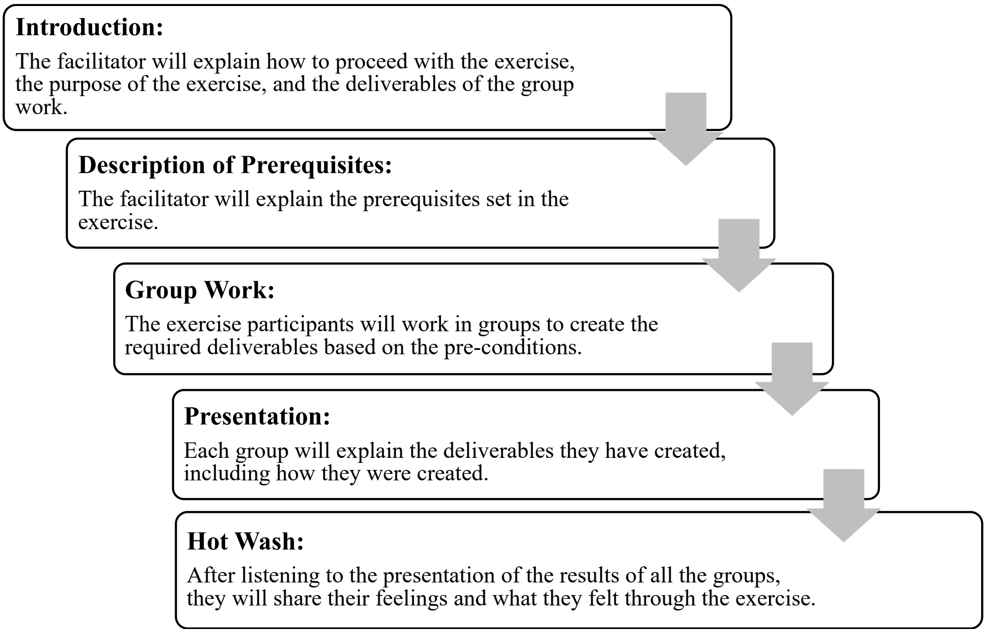


Figure 2: Cyber security testbed and industrial control system (ICS) network [7].



Introduction:
The facilitator will explain how to proceed with the exercise, the purpose of the exercise, and the deliverables of the group work.

Description of Prerequisites:
The facilitator will explain the prerequisites set in the exercise.

Group Work:
The exercise participants will work in groups to create the required deliverables based on the pre-conditions.

Presentation:
Each group will explain the deliverables they have created, including how they were created.

Hot Wash:
After listening to the presentation of the results of all the groups, they will share their feelings and what they felt through the exercise.

Figure 3: Human resource development training flow.

2.3 Table-top exercises

In this exercise, based on the knowledge and experience gained in the simulation exercise, the response to transition the plant to a specific state after a cyberattack on the plant and the response to remove the effects of the cyberattack that made the plant insecure are discussed.

In the table-top-style exercise, the exercise participants progress by role-playing as members of a virtual company. Each exercise consists of five steps: introduction, prerequisite explanation, group work, presentation, and hot wash (Fig. 3).

2.3.1 Card-based incident response exercise

This exercise mainly aims to increase the participants' understanding of the impact of cyberattacks on a plant and to discuss what actions are needed to protect the plant from cyberattacks. In this exercise, the participants need to understand the situation of the virtual company from the conditions provided by the facilitator and to examine and create a workflow to minimize the damage that a cyberattack can inflict on the plant. The group is given a total of 38 normal cards of three types, i.e., "Field-side action", "Head office action", and "Shut down/restart plant", and two special cards, "Suspect/confirm cyberattack" and "Information sharing". The normal cards contain the action details, the department-taken action, and the result after the taken action; the exercise participants then consider their subsequent action based on this information. The information sharing cards are used to share the information obtained by each department with other departments. In the group work, the participants need to create a workflow (Fig. 4) using these given cards.

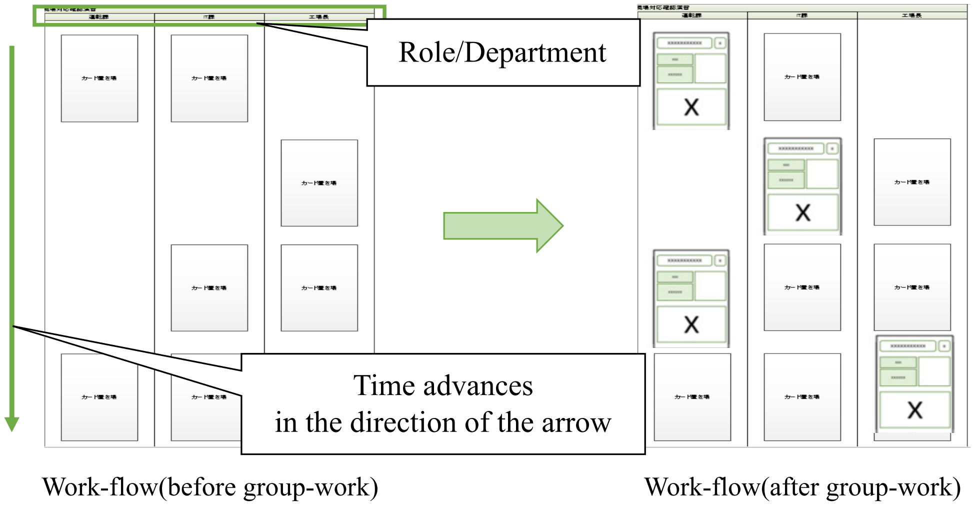

Role/Department
Time advances
in the direction of the arrow
X
Work-flow(before group-work)
Work-flow(after group-work)

Figure 4: Workflow development (image).

2.3.2 ICS-BCP exercise

This exercise guides participants in discussing the perspectives needed to create an ICS-BCP. The exercise requires creating a scenario, action cards, and worksheets to conduct a card-based incident response exercise. Group work is conducted as follows.

1. Participants analyze the possible risks from the hypothetical company and plant scenarios given by the facilitator.
2. Participants create a scenario of a possible cyberattack that could cause the analyzed risk and analyze the impact on a hypothetical company or plant caused by that scenario.
3. Participants examine how to respond to the cyberattack scenario to minimize the damage and create an ideal response workflow. Then, they create an action card based on these scenarios for a card-based incident response exercise.
4. Finally, participants review their exercise or workflow and improve the accuracy of the workflow by conducting their own card-based incident response exercise on other groups.

Figure 5: Team discussion in group work.

In this exercise, exercise participants experience the sequence of creating an ICS-BCP by (1) analyzing the risks to the company, (2) examining the possibility that these risks may occur, and (3) examining countermeasures by imagining the company's situation when the risks occur. This exercise helps exercise participants understand what perspectives are needed and what they should imagine to create an ICS-BCP.

2.4 Findings from these exercises

We have been conducting this exercise in workshops since 2015. We have received excellent evaluations from the participants indicating that the table-top exercise was easy to understand and that they were able to understand the safety measures necessary to make a plant safe, which was the primary purpose of the exercise, by experiencing the cyberattack demonstration and plant operation simulation using the actual equipment (testbed). At the same time, the results of the exercises revealed the following issues:

- **Lack of discussion on how to respond to cyberattacks before signs appear in a plant**
  These exercises focus on responses to ensure the safety of a plant after a cyberattack when the plant shows signs of abnormalities. Many of the exercise participants confirmed that they were able to gain an understanding of this stage. However, to

minimize the impact of cyberattacks, proactive measures should be taken prior to a cyberattack, and it is necessary to develop exercises that can discuss these security responses.

- **Space for setting up a simulated plant is required to conduct the exercise**
  One of the features of this exercise is that it was developed using a simulated plant that can be operated manually. The exercise participants can easily understand the impact of cyberattacks on the plant by touching the simulated plant and watching the demonstration of a cyberattack on it. Then, participating in the table-top exercises with an understanding of the subject of the exercise, the educational effect of this hybrid exercise is enhanced. However, it is essential to have a physical space for the simulated plant to conduct the exercises. As a result, the place where the exercise is provided is limited to the physical location of the simulated plant.
- **Structure makes it challenging to check the effects of the exercises**
  This exercise was developed to acquire the meta-knowledge necessary to respond to cyberattacks targeting OT systems. Feedback from the exercise participants has indicated that they feel that they have gained such meta-knowledge. However, we have failed to confirm whether the capabilities of the participants improved. Even if the exercise is conducted under a different scenario to measure the effect of the exercise, if the subject of the exercise (e.g., a simulated plant or a scenario of a disguised company) is the same, it may not be an exercise but rather a drill to confirm the procedures.
- **Structure makes it challenging to understand the point of view of the cyberattacker**
  To protect a plant from cyberattacks, it is essential to understand how cyberattackers think and conduct their attacks. These exercises focus on the perspective of the defender. A cyberattack scenario, including the point of view of the cyberattackers, was created during the scenario development phase of these exercises, and these exercises were developed based on this cyberattack scenario. However, these exercises were not designed to make the exercise participants intensely aware of the cyberattacker's perspective.

3 EXERCISE TO UNDERSTAND INCIDENT MITIGATION AND RESPONSE

The focus of the exercises developed so far has been on the aftermath of a cyberattack on a plant that results in its operational failure. However, to mitigate the effects of cyberattacks, it is necessary to develop an exercise that allows the user to understand proactive measures that should be taken before any abnormalities occur in the plant. The purpose of this new hybrid exercise is to understand the flow of cyberattacks on plants, the proactive measures that can be taken to protect plants from any cyberattack, and the responses that can be taken to eliminate the effects of cyberattacks when they occur. Accordingly, a new exercise was conducted by adopting a game called "Red vs. Blue gamification" [8] developed and provided by ThreatGEN for simulations (Fig. 6) using a simulated system.

This game from ThreatGEN meets our requirements as shown in Table 1.

3.1 About the Red vs. Blue gamification portal

ThreatGEN Red vs. Blue is the industry's first online multiplayer strategy computer game designed to teach real-world cybersecurity. The game consists of a turn-based system (3 min/turn) for a total of 75 turns, where the player chooses a given action (Fig. 7) under the constraints of time, money, and human resources. Players can play as either the attacker (Red) or the defender (Blue).

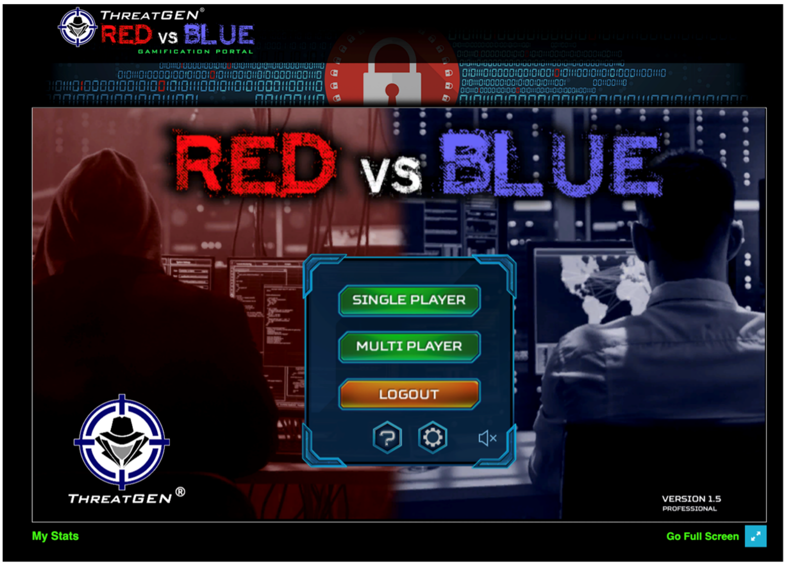


Figure 6: Red vs. Blue gamification portal.

Table 1: Reasons for adopting the Red vs. Blue gamification portal.

Our demands	Features of Red vs Blue gamification portal
The structure should make the exercise participants aware of the point of view of a cyberattacker.	Gain experience on both the cyberattacker and defender sides.
There should be a mechanism to check the effects obtained by the exercises.	Because the results of the game are expressed as a score, the learning effect can be measured.
The structure should be able to discuss actions to be taken after an operational abnormality occurs in the plant and the actions to be taken before an abnormality occurs in the plant.	Experience the sequence of a cyberattack. Experience in pre-action to build an environment that is less susceptible to cyberattacks and in incident response to control devices that have been subjected to cyberattacks.
Exercises can be conducted at any location without the need for a space to conduct them in.	Because it can be conducted online, there is no need to consider the location of the exercise as long as a network environment is available.

The Red side chooses actions to shut down the plant using various attack methods, whereas the Blue side chooses actions to protect the plant from attackers and continue their business. The method of play can be player vs. computer or player vs. player. Using ThreatGEN Red vs. Blue, players can enjoy learning about the actions and mindset of an attacker (Red side) during a cyberattack and the actions and mindset of a defender acting to protect (Blue side) the plant from that attack.

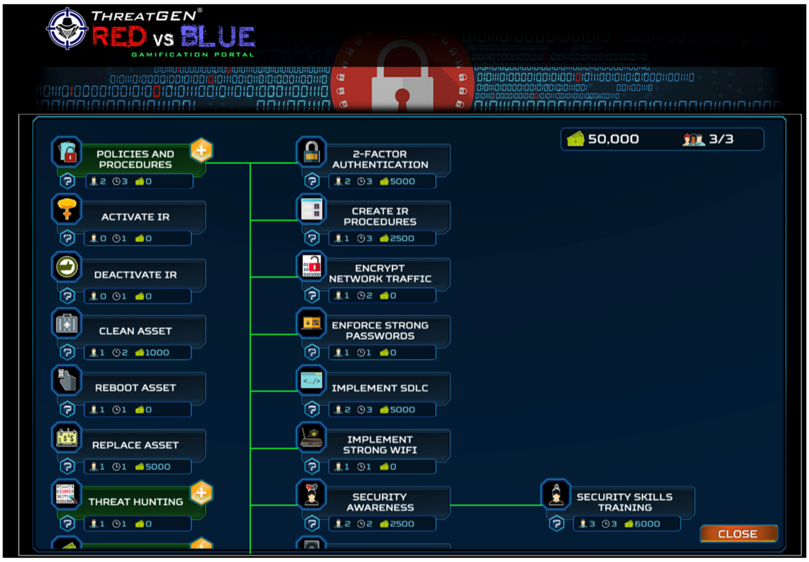


Figure 7: Play screen of the Blue side (select action).

3.2 Exercise method using ThreatGEN Red vs. Blue

In this game, exercise participants only have to select an action to proceed through the scenario. In other words, if they play the game without thinking about it, the benefits they obtain from the game are reduced. Thus, to increase the effect of the game, we combined ThreatGEN (the simulation exercise) with the following additional actions.

3.2.1 Lecture prior the game

As in the previous exercises, a classroom lecture is conducted before playing the game. This classroom lecture focuses on the NIST Framework [9] and Cyber Kill Chain [10]. The NIST framework can prioritize actions to reduce cybersecurity risks by classifying them into five categories, that is, identity, protect, detect, respond, and recover. Cyber kill chain, as proposed by the Lockheed Corporation, models the sequence of actions in a targeted attack and divides the attack into seven phases. The NIST framework is explained for reference when thinking about Blue side behavior, while the cyber kill chain is explained for reference when thinking about Red side behavior.

3.2.2 Play the game

After the classroom lecture, the exercise participants then play the game. The objective of this phase is to understand the primary usage of the game. After the game, exercise participants understand how to play the game, and the game play helps them understand their abilities. Then, they record their scores.

3.2.3 Analyze the action

In this phase, the exercise participants analyze the actions that can be selected in the game. At the same time, they analyze the actions selected in the game, the type of content they have, and their impact. Table 2 shows the phases of the cyber kill chain in which the Red side can choose actions.

Table 2: Categorize attacker's actions (Red-side).

RED ACTION	RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOTATION	INSTALLATION	COMMAND & CONTROL	ACTION ON OBJECTIVES
HOST SCAN	✓						
PORT SCAN	✓						
SERVICE ENUMERATION	✓						
FIND PUBLIC VULNERABILITIES	✓						
ATTACK				✓			
MANIPULATION				✓			
DENIAL				✓			
FUZZING	✓						

Next, exercise participants examine which categories of the NIST framework the Blue side can be chosen from for its actions. Table 3 is used to organize which phase of the cyber kill chain the selected actions are effective against.

Table 3: Categorize defender's actions (Blue-side).

BLUE ACTION	Category (NIST FRAMEWORK)	RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOTATION	INSTALLATION	COMMAND & CONTROL	ACTION ON OBJECTIVES
POLICIES AND PROCEDURES	Respond & Recover	✓		✓	✓			
2-FACTORS AUTHENTICATION	Protect	✓			✓	✓	✓	
CREATE IR PROCEDURES	Respond				✓			
ENCRYPT NETWORK TRAFFIC	Protect	✓						
ENFORCE STRONG PASSWORDS	Protect	✓			✓	✓	✓	
IMPLEMENT SDLC		✓			✓		✓	
IMPLEMENT STRONG Wi-Fi		✓		✓	✓			
SECURITY AWARENESS		✓	✓	✓	✓	✓	✓	✓
SECURITY SKILLS TRAINING		✓	✓	✓	✓	✓	✓	✓

By organizing the actions in this way, the attacker can have better a grasp on the phases required to accomplish the attack and selects the actions to be taken for each phase. On the other hand, the defenders select actions to prevent cyberattacks by understanding the attacker's attack flow and organizing the actions to be taken to stop this flow.

3.2.4 Play the game strategically

The participants then play the game again based on the actions and strategies they analyzed and discussed in Phase 3.2.3. They compare their new scores with their previous scores to see if the strategy they considered is appropriate or needs to be revised.

3.2.5 Hot wash

Participants in the exercise share their insights and impressions throughout the game-based exercise. They also share the strategies they developed and the results of the exercise. They then discuss what constraints exist in applying the actions in the game and the strategies they formulated to a real-world company to use what they learned in the game.

3.3 Exercise results

Using this exercise method, the scores of the exercise participants generally improved. We believe that the fact that they played the game a couple of times has an effect; however, we also believe that, now that they understand the perspective of the attacker/defender, they can strategically choose their actions. The exercise participants gave positive feedback, saying that they were able to gain various things through the game; at the same time, they were able to measure their growth by being evaluated by a score. However, the following areas for improvement were identified.

- **Participants need to be made very aware of the intent of the exercise**
  Because of the structure of the game, where selecting an action advances the scenario, the game can be carried out even if choices are made without thinking. When playing on the Red side, it is essential to understand the attack methods. It is also necessary to understand that, as the attack phase progresses, the target of the attack changes. When playing on the Blue side, participants can choose actions under the managing constraints, such as budget and human resources. Participants, however, may not be aware of the inter-organizational cooperation required to perform counter-actions. Therefore, we believe that a mechanism to make participants aware of the purpose and intent of the exercise (e.g., adding content to the classroom lecture) is necessary.

4 CONCLUDING REMARKS

In this paper, we presented elements required for companies to respond to cyberattacks targeting OT systems and described a hybrid exercise, which we developed and implemented, combining a table-top exercise with a simulation exercise to enhance resilience to cyberattacks on corporate plants. The hybrid exercise combines table-top and simulation exercises to enhance the resilience of corporate plants against cyber threats. A newly developed exercise was also described. In the future, we will further develop these exercises and consider and construct new hybrid exercises that combine video and other media to make it easier for participants to gain insights from the exercises. We will also create a system to measure the effectiveness of the exercises.

REFERENCES

[1] Kaspersky, Stuxnet: Zero victims. https://securelist.com/stuxnet-zero-victims/67483/. Accessed on: 7 Sep. 2021.

[2] Cybersecurity and Infrastructure Security Agency, 2021 Alerts. https://us-cert.cisa.gov/ncas/alerts/2021. Accessed on: 7 Sep. 2021

[3] MAR-17-452 HatMan – Safety System Targeted Malware (Update B). https://us-cert.cisa.gov/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B. Accessed on: 7 Sep. 2021.

[4] Pipeline Cybersecurity Initiative. https://www.cisa.gov/pipeline-cybersecurity-initiative. Accessed on: 20 Aug. 2021.

[5] Cybersecurity and Infrastructure Security Agency, National Cyber Awareness System, Bulletins. https://us-cert.cisa.gov/ncas/bulletins. Accessed on: 7 Sep. 2021.

[6] Software Engineering Institute. https://www.kb.cert.org/vuls/. Accessed on: 7 Sep. 2021.

[7] Aoyama, T., Koike, M., Koshijima, I. & Hashimoto, Y., A unified framework for safety and security assessment in critical infrastructures. *Safety and Security Engineering V*. WIT Press: Southampton and Boston, 2013.

[8] Red vs. Blue Gamification and Training. https://threatgen.com/red-vs-blue/. Accessed on: 7 Sep. 2021.

[9] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework/framework. Accessed on: 7 Sep. 2021.

[10] The Cyber Kill Chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed on: 7 Sep. 2021.