Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations

Ingrid Graffer, Maria B. Line
Dep. of Telematics, NTNU, Norway

Karin Bernsmed*
SINTEF ICT, Norway

Abstract

Industrial control organizations need to perform IT security preparedness exercises more frequently than today. However, limited support material currently exists. This paper presents a board game, *Play2Prepare*, which simulates a large scale attack on the electric power grid. The game consists of a number of scenarios and questions that are meant to trigger discussions and knowledge exchange. The intention with this board game is to support organizations in strengthening their incident response capabilities. Initial feedback from the electric power industry indicates that this board game is indeed a relevant tool for preparedness exercises for IT security incidents.

1 Introduction

Organizations must be prepared to respond to unexpected information security threats and incidents, and this requires training. Well documented procedures and clear definitions of roles and responsibilities are among the basic structures that need to be in place, but when an incident occurs, there is usually no time to study documentation; the involved personnel needs to be well trained and able to make the right decisions under pressure.

Current threat reports state that targeted attacks are on the rise [1] and industrial control organizations, such as oil and energy companies, appear to be attractive targets [8]. One type of industrial control organizations is Distribution System Operators (DSOs) in the electric power industry. DSOs own and manage the distribution grid, which is the low-voltage part of the power grid. Their customers range from private households to all kinds of businesses and industries, including critical services to society, such as hospitals and transportation. They are currently facing the evolution of smart grids, which will lead to a major increase in connectivity and technological, operational, and procedural changes. This implies a need for collaboration between industrial control staff and IT staff in responding to new information security threats that will arise [10]. Being prepared to handle these threats is of utmost importance in order to succeed with smart grids. DSOs must therefore respond effectively and efficiently to security incidents in order to protect themselves, their customers and society at large. Training for information security incident response is, however, not frequently performed by DSOs [13].

Our research aims to aid DSOs in performing preparedness exercises for IT security incidents. In this paper we present a board game, *Play2Prepare*, to be used as a tool in

*This work has been partially funded by the EU FP7 project OPTET, grant number 317631.
Presented at the Norwegian Information Security Conference 2015 (NISK-2015).

preparedness exercises for IT security incidents. The goal with this game is to improve the DSO's incident response capabilities by enabling discussions and reflections and increasing awareness among the participants.

2 Background

An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan [5]. Most preparedness exercises can be classified as either table-top exercises or functional exercises. Table-top exercises are discussion-based, and are well suited for getting familiarized with existing plans and procedures, communication structures and responsibilities in a organization. Such exercises are typically performed with all participants gathered around a table. Functional exercises, on the other hand, might include computer systems or other physical artefacts, as well as practical tasks.

The importance of training is widely acknowledged and guidelines exist on how to perform preparedness exercises [5]. Still, the literature on preparedness exercises for information security incident management is limited [16]. Two recent studies [12, 13] showed that training for information security incidents is seldom performed by the DSOs.

Games, such as card games and board games, typically support discussion-based exercises by simulating incidents and offering a number of "what if" situations. A number of games exist that concern information security awareness, threats, and incidents: *Ctrl-Alt-Hack* [2] was designed for increasing general computer security awareness. *[d0x3d!]* [3] simulates an attack against a computer network, and the participants cooperate in fighting this attack. The goal of *The Disaster Game* [14] is to develop quite detailed scenarios for emergency situations and hence challenge the participants in resolving these scenarios. *Pandemic* [17] is a board game that simulates that different types of diseases infect different parts of the world. In addition there are a number of digitalized IT security games, such as *Secure Empire* [15] and *"Cybersecure: Your Medical Practice"* [6]. Even though all these games are about threat, incident and/or disaster management, none of them support exercises where industrial control staff and IT staff are challenged to cooperate on information security incident management.

3 Play2Prepare: The Design

To fill the gap identified in the previous section we decided to design a prepardness exercise that is adapted to DSOs that need to practice on how they handle IT security incidents. Our main goals with the exercise were to:

1. *Increase awareness.* We wanted to provide the DSOs with an innovative approach to perform IT security exercises, which will help them increase their awareness and raise their competence regarding relevant IT security threats to the control systems.
2. *Enable discussions.* The exercise should include all parties that are involved in resolving an IT security incident, and the process should allow them to discuss relevant threats and to exchange knowledge and experience with each other.
3. *Improve the DSO's incident response capabilities.* The exercise should allow any shortcomings and/or grey areas in the organizations' current plans and procedures to be identified during the discussions.

To reach these three goals we decided to design a table-top exercise rather than a hands-on exercise. A hands-on exercise typically includes tampering with, and restoring, systems, and usually has a high degree of learning outcome. However, using control systems in a hands-on exercise is impractical due to the nature of the operations they

control, which demands availability and fully functioning systems at all times. The largest DSOs might have complete test systems, but we would not expect the smaller DSOs to have this. A table-top exercise is much easier to perform when it comes to resources. The main cost is the time spent by the participating personnel. Furthermore, a table-top exercise is easier to get started with since it requires very little preparations.

The table-top exercise that we created is designed as a classical board game, which we extended with domain specific technical content in terms of *scenarios*. In an information security context, scenarios are commonly used to increase organizations' knowledge on threats and risks. They are also often utilized in information security preparedness exercises [5]. To be useful the scenarios need to be adapted to fit the particular exercise where they will be used. The scenarios that are presented in this section have been designed to reflect real problems that DSOs may face and they have been customized to fit in a board game context. In addition to the scenarios, which are meant to create discussions amongst the participants during the game, we have also created a number of *questions* and *"did you know" facts*. The intention of these is to mix up the discussions with less comprehensive tasks. The questions also make it possible to reward correct answers in the game; something that can be used to motivate the participants.

An important criteria for creating a good exercise is that the participants consider it to be realistic [7]. A realistic exercise therefore needs to be based on scenarios that do not contain logical shortcomings and that appear to be credible from the participants point of view. In this work we have tried to ensure scenarios that are both realistic and broadly applicable by avoiding the inclusion of too many technical details about the system; instead the focus is on the attacks and their possible consequences. The scenarios that we have design are based on related work (cf. Section 2) and known vulnerabilities in existing control systems. Furthermore we have ensured the quality of the scenarios by asking stakeholders from DSOs to validate and to provide feedback on the scenarios. Our intention has been to create scenarios that cover threats, vulnerabilities and the impacts of security incidents, as well as the division of responsibility and roles in DSOs.

The Scenarios

The purpose of the scenarios in the board game is to make the participants reflect around a particular situation that may occur. Some of these scenarios describe the organization's point of view (when they work to solve an attack), while others try to make the participants understand the motivations behind an attack. A study by Line and Moe [11] shows that a multi-phase scenario description will help the participants to understand correlations over time and to detect attacks that would otherwise have remained undetected. All the scenarios are therefore created in a multi-phase shape with accompanying questions.

Scenario 1: Smart meters. A customer who has tampered with the radio signals from his smart meter, manages to modify the readings of the meter in order to lower his reported consumption of power.

- *How can a small scale attack like this be detected?*
- *What are the consequences of this attack and how can they be mitigated?*

The smart metering system in the area where the customer lives, suddenly reports on a large discrepancy between the collected readings from the customers and the reported amount of power that has been transformed through the corresponding substation. Apparently, the customer has bragged about his trick to some of his neighbours.

- *How does the situation change now that the discrepancy increases?*

- *What could be the worst-case scenario in this situation?*

Scenario 2: Social manipulation and insider threats. During a day with harsh weather leading to an unstable power network there is suddenly a breakdown in the central power network between the cities Nes and Aurland. You initially assume that the breakdown was caused by the weather, however, after a number of repeated similar breakdowns you start suspecting there is another reason; the system might be under attack.

- *Mention a few reasons why you would suspect a malicious intent behind these breakdowns? (How do you find out what has caused a power outage?)*
- *Assuming that you are the person who first suspect the breakdowns are caused by malicious activity; how would you proceed? Who should be contacted and what procedures should be followed?*

Eventually, it turns out that the breakdown was due to sabotage against a back-up system. The attackers had gained access by using information from the organization's public webpage, Facebook and LinkedIn to find out who were employed in what positions. This information was then cross-checked with credit card payment remarks to find a "victim" who was in need of money. The "victim" was offered a cash reward to introduce a backdoor into the system.

- *How can such events be prevented?*
- *Could this have happened in your organization? Why / why not?*

Scenario 3: A zero-day attack. Assume that you are working at the regional center. Suddenly the control system alerts about a number of errors in the power grid. After some investigation you realize that there are no real errors; all the alerts are false alarms.

- *What could be the reason for all the false alarms?*
- *What would indicate that the false alarms are due to attacks?*
- *What procedures are to be followed in this case?*

This turns out to be an attack that exploits an unpatched vulnerability (a zero-day attack) in the control system and the Incident Response Team (IRT) is called for. A check of the sub systems reveals that the firmware in the PLCs[1] in the key sensor units has been overwritten, which leads to erroneous control and switching data. This implies that the data from the control system cannot be trusted.

- *How serious are the consequences of this incident? When will it be necessary to switch to manual supervision of the power grid?*

Shortly thereafter you are notified about a massive denial-of-service attack that is blocking the network between the system operation, the manager and the IRT team. This makes it difficult to use your IT systems to coordinate the response to this incident

- *How can you ensure a smooth communication during this incident?*

Scenario 4: Privacy and smart meters. Accidently, a port in the firewall has been left open, which allows direct access from external networks. The vulnerability has been exploited by attackers, who manage to access the smart meter database where all customer data are stored; including their registered power consumption.

- *What could be the intention behind this attack?*
- *How can this attack be detected?*
- *What measures can be introduced to prevent this attack from happening?*

[1] PLC: Programmable Logic Controller

- *How likely is it that you would be fooled in each of the three situations?*
- *Identify the situation where you believe most of the employees in your HR department would be fooled and discuss what the consequences could be.*

Scenario 5: Threats and the media. NSM[2] has received a tip-off that their security experts consider to be trustworthy. A group of hackers claim to have gained access to the control system and threaten to black-out one of the largest cities in Norway.

- *Who is responsible for what in this situation (KraftCERT[3], NSM, public authorities, your own organization)?*
- *What actions must be taken to confirm that this is a real threat?*

After some investigation, you are still unsure whether this is a real threat.

- *How will the situation be handled?*
- *State some elements of an action plan.*

Shortly thereafter, the media get wind of the situation and you experience a storm of enquiries from both journalists and your customers.

- *What immediate actions should be taken in this situation?*
- *Identify some critical information and explain how this should be communicated to the customer support and to the media.*

The Questions and "Did You Know" Facts

The questions in the game are designed to create discussions amongst the participants and to increase their understanding of important concepts related to information security. Some examples of questions related to security are: *In an information security context, what is meant by "confidentiality"?* and *What is the difference between IT security and supply security?*. Other questions are related to internal procedures that are to be followed in case of an incident, for example *How can you make sure that someone making a phone call to customer support is the person he states to be?* and *Mention one situation where the procedure is to shut down the remote access to the control system?*.

The "did you know" facts are less comprehensive than the questions and consist of short inputs that aim to create dynamics and variation in the game. They will be read out loud by the participants and they are intended to be thought-provoking. Some examples are *USB thumb drives loaded with malware that are "accidentally" left behind can be picked up by employees who start to use them. Did you know that the worst attack against SCADA systems, Stuxnet, started this way?* and *In 2014 the most commonly used password was "123456" closely followed by "password"*.

The scenarios, the questions and the "did you know" facts represent the technical foundation of the table-top exercise and are meant to add a domain specific information security flavour to the game.

4 Playing the Game

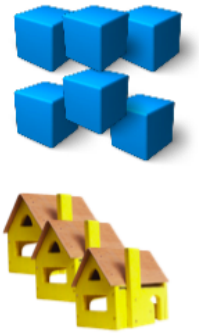
Play2Prepare is a cooperative board game where the players will work together to mitigate attacks against the power grid network. The players let their pawns travel around the board in order to neutralize local attacks, while the attack spreads in each round. The game is designed for 3-4 players, where each player is assigned a particular role with accompanying skills that have to be utilized in the best possible manner in order to win

[2]The Norwegian National Security Authority. `https://www.nsm.stat.no/`

[3]The cyber security IRT for the power industry in Norway. `http://www.kraftcert.no/`

the game. Play2Prepare has a similar logic functionality as the existing board game Pandemic [17] but has been heavily adapted to integrate information security management procedures into the context of DSOs. Fig. 1 displays the content of the game. [4]

(a) 6 pawns og 5 Mitigate markers



(b) 30 Attack cubes og 5 Research Stations

(c) 6 Role cards

(d) 6 Attack!! cards

(e) The board

(f) 38 Attack Propagation cards

(g) 38 Player cards with city and phase

(h) Scenario, Question and "Did You Know" cards.

Figure 1: The content of the game (note that the cards are printed in Norwegian)

Setting up the Game

The game is set up as follows:

1. Place the board in the center of the table within easy reach of all the players. Place six Research Stations, three Mitigate markers and all the Attack cubes near the side of the board. Put one of the Research Stations at the Frogner city on the board.
2. Put the Attack Rate Marker on the first space of the Attack Rate Track *(Norw.: Angrepsrate)* and the Breakdown Marker on the "0" space of the Breakdowns Indicator *(Norw.: Sammenbrudd)*.
3. Draw 3 Attack Propagation cards and put 3 Attack cubes on each of the corresponding cities. Draw 3 more cards and do the same thing as above, but add 2 cubes to each city. Finally, draw 3 cards and do the same as above, but add 1 cube to each city. Put the used Attack Propagation cards facing up aside the pile of cards.

[4]Due to space limitation we can only give a brief introduction to the game is this paper. More thorough instructions, as well as a sample turn of the game that shows the situation and explains the possible actions after several turns have passed, can be found in the report [4].

4. Let the players choose 1 Role card each. Shuffle the Player cards and deal them to the players face down: 3 player game - 3 cards each, 4 player game - 2 cards each.
5. Shuffle 4-6 Attack!! cards (depending on how difficult you want to make the game) into the pile of remaining Player cards. Shuffle a number of Scenario, Questions and "Did You Know" cards into the pile. Put the pile of cards onto the board.
6. Put all the pawns at the Hamang city on the board. The player who most recently shifted his/her password will start the game.

The prepared board game (printed in Norwegian) is illustrated in Fig. 2.

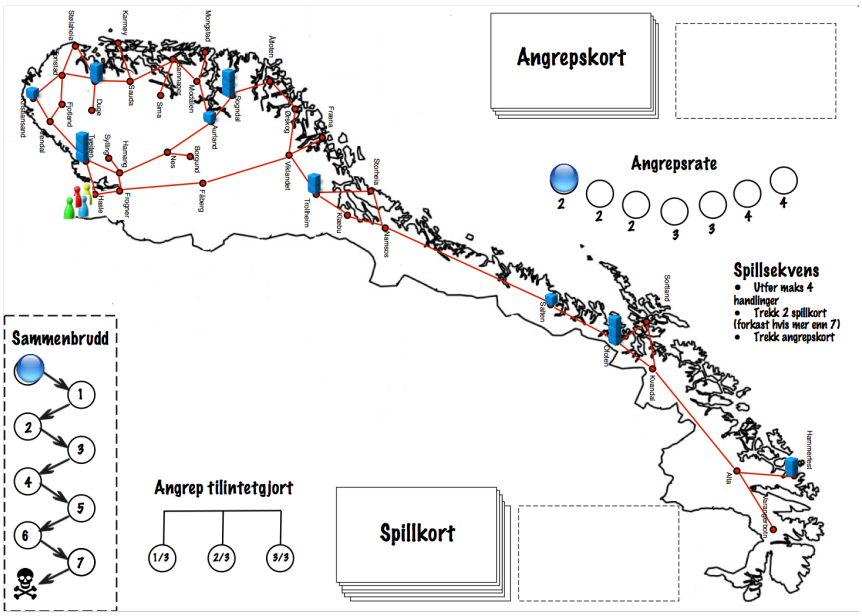


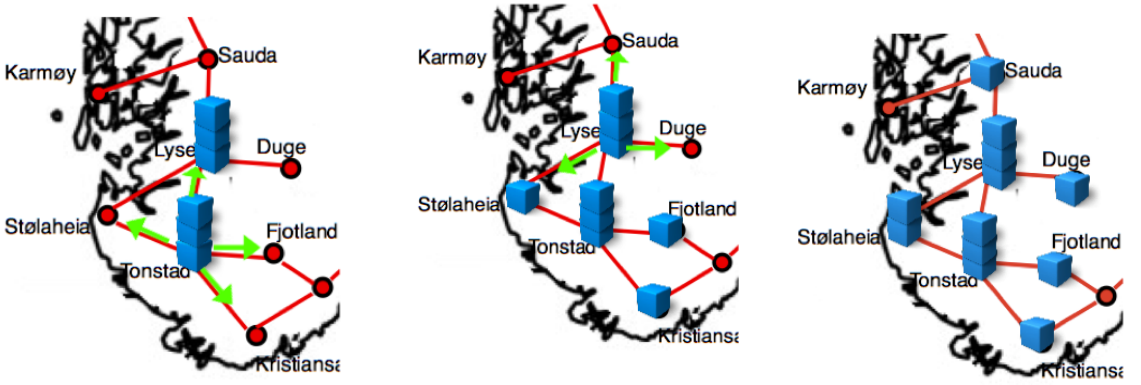
Figure 2: The board game, prepared to be played.

Actions in the Game

The play proceeds clockwise around the table with each player taking turns in order until the game ends. Each turn, the current player must 1) Take (at most) 4 actions, 2) Draw 2 Player cards to add to his hand, and 3) Draw 1 Attack!! card. The different actions that the player can choose between are:

- Drive: the player moves his pawn to an adjacent city.
- Fly: the player can 1) dismiss a card to travel to the city printed at the card, or 2) dismiss a card that has the pawn's current city printed and travel to any city, or 3) travel from a city with a Research Station to any other city with a Research Station.
- Build a Research Station: the player can dismiss a card that has the pawn's current city printed in order to build a Research Station in that city.
- Restore the system: Remove a cube from the city where the pawn is located.
- Mitigate an attack: Dismiss 5 cards that represents each of the five phases in the incident management process.
- Share knowledge. When two pawns are located in the same city, their players can exchange cards printed with that city.

A given action may be performed more than once during a turn, as long as 1 action is spent for each instance. Each player's Role will grant them special abilities that are unique to that player. Players may also pass if they have nothing else to do. Unused actions may not be saved from turn to turn.



(a) A breakdown in Tonstad

(b) The breakdown in Tonstad leads to another breakdown in Lyse

(c) The situation after the chain reaction has passed

Figure 3: An example of a breakdown causing a chain reaction in the network.

Description of the Game

In the current version of Play2Prepare **the board** represents part of the central power distribution network in Norway. The target of the current version of the game is therefore employees at Statnett, which is the organization that manages the central power distribution network in Norway. However, the board can easily be adapted to other organizations by replacing or changing parts of the network. The **attack rate** is initially set to 2, which means that 2 cards will be drawn in each round. The attack rate will increase every time an Attack!! card has been drawn. An attack will be **mitigated** when a player manages to collect 5 Player cards with different numbers (representing the five phases in the ISO/IEC 27035 information security incident management standard[5]) and deliver these to a Research Station. For each attack that is mitigated, 1/3, 2/3 and 3/3 (i.e. all) of the cubes on the board will be removed. The players will agree on which cubes they want to remove. The **Breakdown marker** starts at "0" and will increase every time there is a breakdown somewhere in the network. A breakdown occurs if a player is required to add a cube to a city that already has 3 cubes in it. When this happens, instead of adding a 4th cube, add a cube to each adjacent city. If any of these new cubes would cause the total number of cubes of that colour in an adjacent city to exceed 3, additional breakdowns may occur, causing a *chain reaction*. Note that each city may only breakdown once in each chain reaction.

Fig. 3 shows what happens when an Attack!! card with the city Tonstad is drawn when this city already has 3 cubes. Then the cities Stølaheia, Kristiansand, Fjotland and Lyse will each receive an additional cube. Since Lyse already has 3 cubes, a breakdown will happen in this city as well. The attack will therefore spread to Sauda, Duge and Stølaheia.

The Cards

There are seven different types of cards in the game. The **Attack Propagation cards** show which cities an attack spreads to. For each card that is drawn, add 1 cube to the

[5]The five phases in ISO/IEC 27035 are: 1) Plan and prepare, 2) Detection and reporting, 3) Assessment and Decision, 4) Responses, and 5) Evaluation and lessons learnt. Note that even though the plan and prepare phase is not directly part of the process of responding to an actual incident we have chosen to include all five phases in the game to create a complete mapping to the standard.

Table 1: The roles that have been defined for the current version of Play2Prepare.

Role	**Skill**
CEO	Can draw a random card and give it to another player whose pawn is in the same city as the CEO's own pawn.
IT security expert	Needs only 4 of the 5 phases in the ISO/IEC 27035 standard to mitigate an attack.
Public authority	By dismissing an arbitrary Player card, this role can 1) build a new Research Station in the city where his pawn is located, or 2) fly from a city with a Research Station to any other city.
Network operator	Can dismiss all cubes in 1 city with only 1 action.
IRT team leader	Can move other players' pawns (with their permission) as if they were his own.
Control system operator	Can prevent that new cubes (i.e. attacks) are placed (i.e. occur) in the city, or in any nearby cities, where his pawn is located.

city printed on the card. The **Player cards** are associated with one city and one of the incident management phases defined in ISO/IEC 27035 standard [9]. The Player cards have two functionalities. Either they can be used to perform an action, for example flying to the city associated with the card, or they can be collected in order to mitigate attacks. A player can mitigate an attack if he has collected 5 Player cards that cover all the 5 different phases in the standard. The **Scenario, Question and "Did You Know" cards** have technical contents as described in the previous section. A number of these cards will be shuffled into the pile of Player cards (the actual number depends on how much technical discussion one wants to include in the game). The **Attack!! cards** describe what actions shall be taken when an attack happens. The possible actions are: 1) Increase the attack rate: Move the Attack Rate Indicator up by one on the Attack Rate Track on the Board. 2) Distribute the attack: Take the bottom card from the Attack! draw pile and add 3 cubes to the city pictured on the card. Note that no city can contain more than 3 cubes. If the attack would cause the city to exceed that limit, any excess cubes are returned to the stock and an breakdown is triggered. 3) Intensify the attack: Shuffle the used Attack! cards and place them on top of the remaining Attack! cards pile. Finally, all players have been assigned a role in the game. Each role has a special skill described on the **Role card**. An important aspect of the game is to cooperate in order to use the skills associated with the roles in the best possible way. The roles that have been defined for the current version of Play2Prepare are displayed in Table 1. Note that it is of course possible to replace the name of the roles with other terms that better fit the structure of the organization(s) that are involved in the exercise, however, to ensure a good flow in the game the skills should remain the same.

Game End

Players collectively win the game immediately when 3 attacks have been mitigated. The game ends immediately in defeat for all players if any of the following conditions occur:

- The attack has spread too much: there are more than 30 cubes on the board.
- The sixth breakdown occurs (the Breakdown Marker reaches the skull symbol on the Breakdown Indicator)
- There are not enough cards in the Player card pile when a player must draw cards

The game takes approximately 1-2 hours to play.

5 Evaluation

Play2Prepare has been evaluated in three rounds during its development.

Functional Testing Without the Scenarios

In the first round the functionality of the game was tested. The main goal of this test was to identify potential improvements and to adjust the basic functionality of the game. The test was performed in two phases; an initial pre-test where the first author of this paper took the role of three different players and played the game herself in order to identify obvious shortcomings and make quick improvements, and a second phase where three volunteers (without any specific knowledge about information security or the power grid network) played the game. The scenarios were not included in the first round of the test.

The first round of the test resulted in a number of functional improvements, such as adjusting the number of cities and corresponding connections on the map of the board, the criteria for winning and losing the game the number of players in the game, the expected time to complete the game and the division of responsibilities amongst the participants.

Functional Testing Including the Scenarios

In the second round the main goal was to evaluate the feasibility of the complete exercise. The participants in this test were three university students who specializes in information security. They played the game from start to end and provided feedback on a number of different aspects, as discussed beneath.

- **The pile of Player cards.**. The game was set up with 2 Scenario, 3 Question and 3 "Did You Know" cards mixed into the pile of Player cards, which thereby consisted of 38 Player cards with city and phase, 8 cards with technical content and 4 Attack!! cards (in total 50 cards). This ratio of different types of cards turned out to be a good choice and had no obvious negative influence on the feasibility of the game.
- **The Scenario, Question and "Did You Know" cards.** The test revealed some obscurities in the initial wording in these cards (that have now been reformulated).
- **Timing.** Using the proposed set-up with 4 Attack!! cards, the test was completed in 35 minutes (the test group won the game), which is considered relatively fast. Based on how many cards that were left in the pile of Player cards we estimate the time to complete the exercise to be approximately 60 minutes in ordinary cases (when the participants may not be as lucky). Adding time for introducing the exercise and preparing the board we estimate the time for completing the game to at most 1.5 hour.
- **Flow of the game.** Finally we wanted to investigate how the introduction of the technical part (i.e. the scenarios, questions and "did you know" facts) influence the flow of the game. The technical part currently runs somewhat in parallel to the game, since the scenarios currently do not affect the actions of the board. Due to the participants' background (they were all university students with limited knowledge of how DSOs operate) we did not manage to fully test this aspect. However, our test indicated that splitting up the discussions of the different phases in a scenario may be problematic since the incident that is being discussed needs to be fresh in the participants' memories.

During the debriefing of the test, several of the participants mentioned that, even though the game appeared to be complicated when it was introduced, it turned out to be easy to grasp once they had started to play.

Feedback from the Power Industry

In the third round Play2Prepare was presented to three stakeholders from the Norwegian electric power industry; one employee at Statnett[6] and two employees at NVE[7], who are actively involved in preparedness activities in their respective organizations. They provided feedback on the technical content of the game and on the exercise as a whole.

Regarding the idea of using a board game for preparedness exercise, the stakeholders considered this to be a fun and informal way of learning and that it is efficient, since the necessary preparations will be kept minimal. They believed that such an exercise can contribute in increasing the ability to cooperate and share knowledge amongst their employees; in particular between the IT staff and the industrial control systems staff. They pointed out that discussions across different departments within an organization are always useful and that there is always a need for more training to increase their IT security preparedness. They also pointed out that the rules of the game should not be too complicated, in order to lower the threshold for start utilizing the game.

Regarding the technical content, the stakeholders suggested that some of the roles that have been pre-defined in the game needed to be changed to better fit their respective organizational structure. Also, all scenarios will not be relevant for all organizations.

The final round of the evaluation also resulted in a number of editorial changes to the text in the description of the scenarios, the questions and the "did you know" facts.

6 Concluding Remarks and Future Work

We have presented *Play2Prepare*, a board game intended to support teams in industrial control organizations performing preparedness exercises for IT security incidents. The game facilitates knowledge exchange and awareness raising through a set of scenarios to be discussed, a number of questions to be answered and a number of "did you know" facts. Even though our evaluation was brief, it indicates that this type of exercise might indeed be useful for DSOs, as part of their preparedness exercises.

The feedback from the participants in the evaluations indicated that it takes some time to understand the rules of the game and to set up the board the first time the game is to be played. If the game is to be used in a preparedness exercise program, someone with experience with the board game should support the team playing the game by acting as a facilitator. This would increase the efficiency of the exercise, ensuring that the participants do not spend unnecessary time on learning the game dynamics.

Recalling the goals that were stated in Section 3, we aimed to create a table-top exercise that 1) increases awareness, 2) enables discussions, and 3) improves the DSOs' incident response capabilities. Our evaluation indicates that we have achieved the first two goals, however, to what degree Play2Prepare will be useful as a part of the organizations' preparedness exercise progress remains to be seen. Our next step will therefore be to perform thorough evaluations in industrial control organizations with relevant personnel participating. Further, the effect of this board game compared to a traditional table top exercise should be evaluated. We are also considering re-designing and implementing Play2Prepare into a digital version, which would better support an exercise for distributed teams where the team members are located at different geographical locations.

In addition there are functional changes that could be implemented in order to improve the gaming experience. As mentioned in Section 5, the technical content of the game, (i.e.

[6] `http://www.statnett.no`

[7] NVE: The Norwegian Water Resources and Energy Directorate, `http://www.nve.no`

the scenarios, questions and "did you know" facts) currently do not influence the state on the board (i.e. the spread of the attack). In a new version of the game, the correct answers to e.g. the questions could be used to gain advantages in the game.

The current version of Play2Prepare has been designed for Norwegian DSOs. To be useful as a preparedness exercise in other countries, and in other types of organizations, both the network graph printed at the board, the language used, and the content of the scenarios must be adapted in order to fit the new context. Finally, if the game is to be played repeatedly during a number of subsequent exercises, the number of scenarios must be increased in order to make sure that each round brings up fresh topics to discuss.

References

[1] Dennis Batchelder, Joe Blackbird, David Felstead, Paul Henry, Jeff Jones, and Aneesh Kulkarni. Microsoft Security Intelligence Report. Microsoft, 2014.

[2] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 915–928, New York, NY, USA, 2013. ACM.

[3] Mark Gondree and Zachary N. J. Peterson. Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game. In *Presented as part of the 6th Workshop on Cyber Security Experimentation and Test*, Berkeley, CA, 2013. USENIX.

[4] Ingrid Graffer. It-sikkerhetsberedskapsvelser i smartgrids. Master thesis, NTNU, 2015.

[5] Tim Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good. NIST SP 800-84: Guide to Test, Training and Exercise Programs for IT Plans and Capabilities. National Institute of Standards and Technology, 2006.

[6] HealthIT.gov. Cybersecure: Your medical practice. `http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html`

[7] C Hove and M Tårnes. Information security incident management - an empirical study of current practice. Master thesis, NTNU, 2013.

[8] ICS-CERT. ICS-CERT Monitor, Oct/Nov/Dec 2013. `https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf`.

[9] ISO/IEC. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management, 2011.

[10] Maria B. Line. Why securing smart grids is not just a straightforward consultancy exercise. *Security and Communication Networks*, 7(1):160–174, 2013.

[11] Maria B. Line and Nils Brede Moe. Understanding Collaborative Challenges in IT Security Preparedness Exercises. In *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015*, pages 311–324. Springer Science and Business Media, 2015.

[12] Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard A. Kemmerer. Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared? In *21st ACM Conference on Computer and Communications Security and Co-located Workshops*, pages 13–22, November 2014.

[13] Maria Bartnes Line, Inger Anne Tøndel, and Martin Gilje Jaatun. Information security incident management: Planning for failure. In *8th International Conference on IT Security Incident Management and IT Forensics (IMF)*, pages 47–61, May 2014.

[14] Disaster Game LLC. The Disaster Game. `http://www.disastergame.com`.

[15] M Olano and et.al. Secure empire. `https://www.usenix.org/conference/3gse14/summit-program/presentation/olano`

[16] Inger Anne Tøndel, Maria B. Line, and Martin G. Jaatun. Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45:42–57, 2014.

[17] Z-Man Games. Pandemic. `http://zmangames.com`.