A Ransomware Decision Game
Whitepaper

Philipp Leo[1]
Cyber Risk Expert
leo@leomuhly.com

Fabian Muhly[1,2]
Researcher in Criminology
muhly@leomuhly.com

[1]Leo & Muhly Cyber Advisory, Wettswil, Switzerland
[2]School of Criminal Sciences, University of Lausanne, Batochime, Lausanne, Switzerland

Abstract
Ransomware is a continuously growing cyber threat in particular for public and private organizations. With the emergence of cryptocurrencies as means of making non-traceable financial transactions those entities have become especially prone to these malicious attacks. To achieve resilience against these attacks, effective and sophisticated deterrence and mitigation measures have to be set in place by all organizations universally. As this is far from reality and as ransomware threats develop as well, accountable staff of organizations need to be trained on the decision choice portfolio associated with a ransomware incident that goes beyond the obvious binary decision of whether to pay or not to pay a ransom. We propose a serious game that helps players understand the decision dilemmas they will face during an attack and that will educate players about decision alternatives that aim for minimizing the damage the organization induced by such an attack. In an entertaining way, our game intends to transfer explicit knowledge about decision scenarios into tacit knowledge for knowledge internalization. This whitepaper presents the general ideas of such a game.

Keywords
Ransomware, Serious Gaming, Senior Decision Makers, Decision Tree, Tacit Knowledge

Introduction
Ransomware is malicious code that encrypts computer systems or files on them. The perpetrators blackmail their victims by making it clear that the system or data will be released only after a ransom is paid. You will know immediately if your computer system is infected with ransomware. If you are denied access to your computer and files, you very likely have become a victim of cyber criminals who have taken your computer and data into custody and encrypted it. They will tell you their demands and promise to unlock your computer or decrypt your files after paying a ransom in a cryptocurrency. The spread of ransomware is little different from that of other malware. It often enters the computer when visiting manipulated websites through a link in a spam email or a message via a social network. Sometimes, the perpetrators also send emails that are supposed to contain an invoice or a payment reminder. In reality, however, malicious code is hidden in the attached file (Thomas, 2018). According to a report of Coveware (2021), more than 50% of ransomware attacks start in this fashion. Blackmailing users in this way is not a new invention. The first documented ransomware is the "PC Cyborg" (Bates, 1990). Evolutionary biologist and Harvard graduate Joseph Popp sent over 20,000 infected floppy disks by mail to participants of the World Health Organization's World AIDS Conference in 1989 (Richardson and North, 2017). Instead of the supposed conference documentation, it contained ransomware he had developed. After inserting the diskette, the malware replaced a system configuration file and, after ninety reboots, it began encrypting the hard drive. To get the data back, victims were supposed to send $189 USD to a company in Panama (Tailor and Patel, 2017).

What caused trouble back then, spreads anxiety and fear today. Ransomware has currently become one of the biggest cyber threats and ransomware attacks are supposed to have grown exponentially in recent years (Beaman et al., 2021). According to a study by Sophos (2021), financial losses expressed in remediation costs were $1.85 million USD on average per incident across countries. Since ransomware attacks usually hit users unexpectedly, there is often a sense

© Leo & Muhly Cyber Advisory

of helplessness after an attack. However, it is important to limit the impact of an attack immediately by acting skilfully and thoughtfully. Unfortunately, a proper education about ransomware attacks and their rationales is currently not readily available and particularly not for those that have to take decisions during a ransomware incident, namely the senior management, board of directors or crisis management team. For sure, there are various approaches and initiatives that discuss ransomware mitigation, detection and prevention strategies (Silva et al., 2019; Oz et al., 2021) or technical and behavioural trainings against ransomware attacks (Bello and Maurushat, 2020), but to the best of our knowledge there are no approaches that educate people about decision alternatives during a ransomware attack. It is true that once you fell prey for the malware, you will inevitably experience losses. However, during a ransomware event there are far more decisions to take than a mere unidimensional – paying or not paying the ransom – state of mind might suggest on the first sight. We believe that there is a huge benefit in utilizing a serious gaming approach to educate people about decision scenarios in the regard of ransomware incidents. Our game intends to educate people about different decision considerations during a ransomware attack and by this enables them to take decisions that would increase the likelihood of limiting financial losses. In this paper we present our thoughts for such a serious game in terms of the pedagogical knowledge transfer and the design of the game.

Knowledge Transfer and Serious Games

There are often limits to classical knowledge transfer. The desire for a simple handling of knowledge is expressed above all in the search for simple instruments. According to Nonaka's and Takeuchi's knowledge spiral model (1995), knowledge can take different forms. They draw on Polanyi's (1966) distinction between explicit and tacit knowledge. Nonaka and Takeuchi's model identifies four types of knowledge transformation: socialization, externalization, combination and internalization.

When it comes to reacting correctly in an extraordinary situation, such as a ransomware attack, it is about transforming explicit knowledge into tacit knowledge. Games and especially serious games are a powerful tool for internalization. In the 1970s Clark Abt (1970) defined the term of serious games as games that are primarily designed for training and educational purposes and not primarily for amusement. He explicitly mentions that such games are beneficial for decision makers of different domains. Serious games are often perceived to be digital computer games and are assumed to be limited to the digital sphere (Zyda, 2005; Rudman, 2019), but do not have to incorporate technology. On the contrary, it is even beneficial to play serious games in a tabletop format to foster the socialization dimension of knowledge transformation. Based on prior research (Muhly et al., 2021) we see playing and experiencing games together within a group as a particularly effective way to transfer explicit knowledge to tacit knowledge.

Serious game characteristics

- Serious games often require making decisions and thus learning valuable skills for situations that actually occur.
- These games facilitate interaction and dialogue with other people and thus cultural, social and generational barriers can be overcome.
- Users learn new concepts and skills through play.
- Interactive environments can be designed in a simplified and practical manner.
- Learning processes are more successful because the user can recall knowledge learned through play more easily.
- Serious games promote important skills such as observation, motivation, dealing with criticism, strategic thinking and interpersonal skills.
- The interactive character and playful components of serious games arouse the learner's commitment and contribute to entertaining learning.
- When cooperation is fostered using games, learners are more satisfied with their work, feel a sense of belonging to the team, and are committed to achieving goals.

© Leo & Muhly Cyber Advisory

Design of the Game

The design of our «Ransomware Decision Game» is based on the considerations above. Instead of limiting ourselves to frontal knowledge transfer, our methodology is based on a playful approach. The game is designed to serve a small group of participants or a plenary with a group size that would be difficult to handle with a tabletop game set only. Therefore, there are no restrictions to group size or logistical requirements, such as room size or number of tables. The game is led by game masters who centrally administer the game. At the beginning, a realistic initial situation of a ransomware attack is described. Based on these descriptions, different options for action arise. The group must decide on an alternative course of action. This is determined by a voting process. For the voting process we use the Mentimeter platform.[1] Each decision has consequences that lead to new alternative courses of action. Using actual examples, the consequences of their collective decision are presented to the group. Iteratively, the group experiences a possible course of a ransomware attack. The game is based on a sequential decision tree.

In brief, the structure of the game is as follows:

1. Introductory presentation: Prior to the game a brief case-study presentation of real-life ransomware attacks hooks up the participants and stresses the problem.
2. Familiarization: The game starts with the presentation of a fictitious ransomware incident scenario and a familiarization with the game material.
3. Game iterations: The game follows an iterative procedure with different courses of action. Participants decide for a specific course of action by voting.
4. Debriefing: The overall decision tree including all paths of action is presented and discussed with the participants in a reflective approach by comparing the course of action followed during the game and the alternative outcomes given the decision tree.

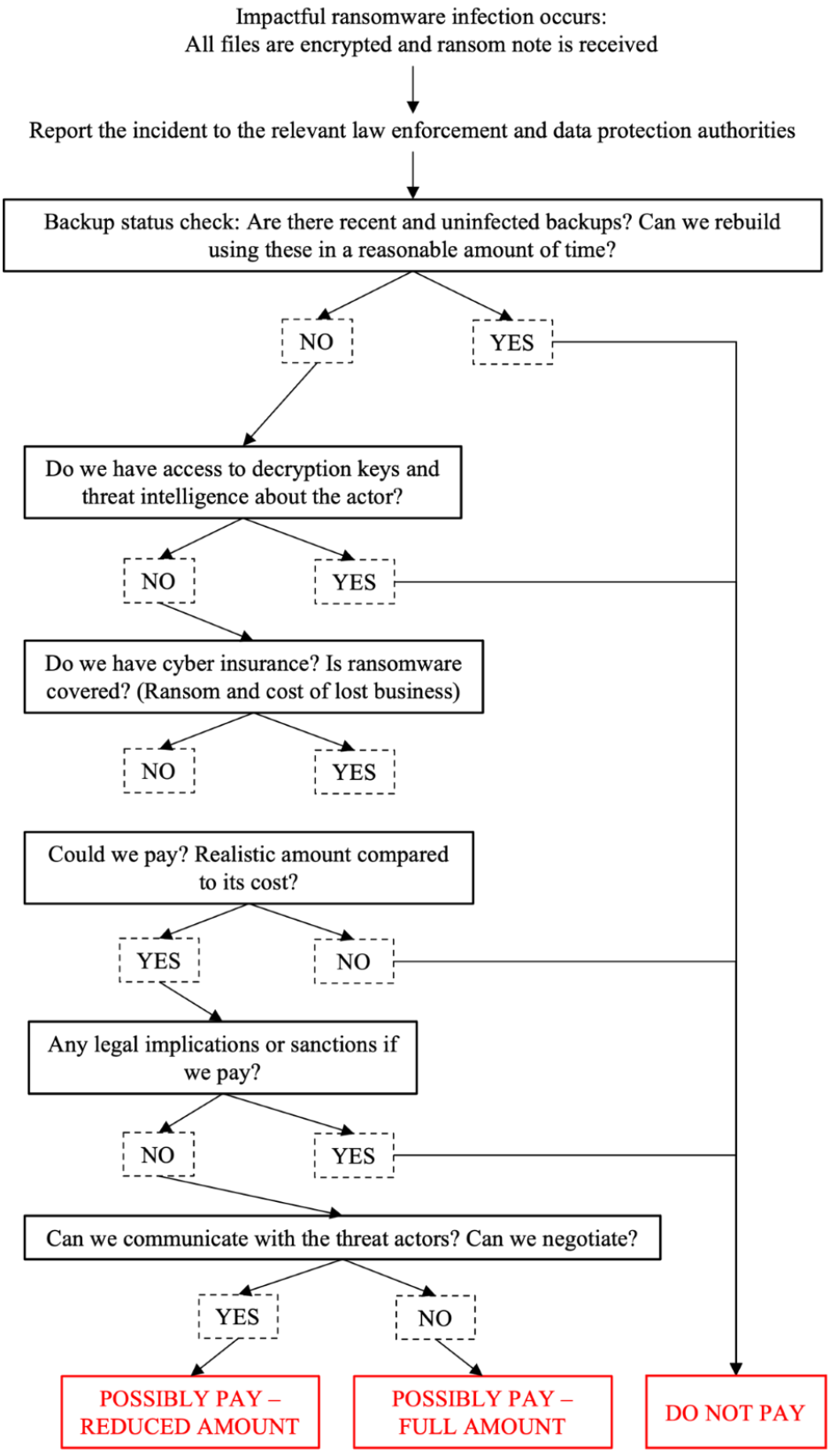
The overall game characteristics are as follows:

1. The game is led by one or multiple game masters.
2. The game can be administered in small groups with a game master per game table or in the plenary.
3. The game material is either available as a tabletop for small groups or as a mobile application for plenary purposes and single independent player mode.
4. Participants obtain the role of a senior management, board of director or crisis management personnel.
5. Participants are requested to take decisions during a fictitious ransomware attack along a predefined decision tree.
6. The decision tree is not known to the participants in advance.
7. In each iteration participants are given a predefined amount of time for taking their decision of the next course of action.
8. Depending on the mode of instruction, participants do either reflect on their own, in a team or in the group about the desired decision of action and vote for it.

[1] Mentimeter.com

© Leo & Muhly Cyber Advisory

Figure 1: Ransomware attack decision tree (preliminary, generic version)



© Leo & Muhly Cyber Advisory

Outlook

Ransomware in all its forms and variants poses a considerable threat. In this regard, it is all the more important to keep an eye on the threat it poses to organizations and society. Decision-makers need to be prepared for all eventualities as best as possible. It is therefore essential to have up-to-date knowledge about ransomware. This enables responsible personnel, like senior management, board of directors and crisis management staff to act consciously and thoughtfully during cyber incidents, such as a ransomware attack. Our serious game creates favourable conditions to be able to react appropriately in case of a ransomware attack. In future, we will convert these ideas into an executable tabletop game. Once this has been set, we will administer our ransomware decision game with senior decision makers. We intend to utilize the game as **A**wareness creation among the participants about the different decision scenarios that follow a ransomware incident. Aspirations of testing the game's potential in effectively inducing a more resilient ransomware incident **B**ehaviour and **C**ulture among senior decision-makers is without doubt harder to evaluate. It would imply that we take track of the game participants and follow up with them when being hit by such kind of malware. This induces a substantial amount of uncertainty and dependency to the research. However, aspirations to simulate ransomware attacks and evaluate the game in an experimental design might be worth thinking of.

References

Abt, C.C. (1970). Serious Games. University Press of America.

Bates, J. (1990). Trojan horse: AIDS information introductory diskette version 2.0. Virus Bulletin (1990).

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, 111, 102490.

Coveware (2021). Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020#vectors.

Muhly, F., Leo, P., & Caneppele, S. (2021 forthcoming). A Serious Game For Social Engineering Awareness Creation. *Journal of Cybersecurity Education, Research and Practice*: Vol. 2022 : No. 1 , Article 1. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss1/1.

Nonaka, I., & Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. Oxford University Press.

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2021). A survey on ransomware: Evolution, taxonomy, and defense solutions. arXiv preprint arXiv:2102.06249.

Polyani, M. (1966). The tacit dimension. London: Routldege & Keagan Paul.

Richardson, R., & North, M. (2017). Ransomware : Evolution , Mitigation and Prevention, 13(1), 10-21.

Rudman, S.A. (2019). Serious games to study the influence of wildlife devaluation strategies on hunter behaviour. A thesis submitted to the Victoria University of Wellington in fulfilment of the requirements for the degree of Master of Science. Victoria University of Wellington, 2019.

Silva, J. A. H., López, L. I. B., Caraguay, Á. L. V., & Hernández-Álvarez, M. (2019). A survey on situational awareness of ransomware attacks—detection and prevention parameters. Remote Sensing, 11(10).

© Leo & Muhly Cyber Advisory

Sophos (2021). The State of Ransomware 2021. https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

Tailor, J. P., & Patel, A. D. (2017). A comprehensive survey: ransomware attacks prevention, monitoring and damage control. *Int. J. Res. Sci. Innov*, *4*(15), 116-121.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management, 12(3), 1-23.

Zyda, M (2005). From Visual Simulation to Virtual Reality to Games. Computer, September 2005, pp. 25–32.

© Leo & Muhly Cyber Advisory