Cybersecurity Incident Response

Tabletop Exercises Using the Lego Serious Play Method

It is foolish to wait until an enterprise is in the midst of a data breach to test its cybersecurity incident response plan (CSIRP). How likely is it that the enterprise will know that a cyberattack is underway and be able to react appropriately? Are the enterprise's current policies and procedures sufficient to effectively detect, respond to and mitigate sophisticated cybersecurity incidents?

The use of tabletop exercises (TTEs) can help answer these and other questions. TTEs are designed to prepare for real cybersecurity incidents. By conducting TTEs, an incident response team increases its confidence in the validity of the enterprise's CSIRP and the team's ability to execute it.[1]

The Lego Serious Play (LSP) method can support, improve and strengthen the design, execution and outcomes of the TTEs an enterprise uses to assess the capabilities, effectiveness and maturity of its CSIRP. TTEs help determine whether the current CSIRP is able to detect, respond to and mitigate incidents in a timely and successful manner. They can also ascertain whether the right people are in place, whether they are aware of and committed to their duties during a real cybersecurity incident, and whether they can execute the procedures correctly.

Although TTEs are based on recommended methodologies, such as the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-84,[2] the need to improve TTEs to prevent failures and overcome challenges has been recognized. Cybersecurity professionals need to acknowledge these shortcomings and explore new mechanisms to manage them. The LSP method has proved to be one mechanism that enriches and improves cybersecurity incident response TTEs and reduces the risk of failure.

The Value of Tabletop Exercises

A TTE presents a realistic cybersecurity incident scenario to which an enterprise must respond. Participants in the exercise describe how they would react during the incident, what tools they would use and what procedures they would follow. At the end of the exercise, the enterprise can determine where its incident response plans and policies are working well, where there is room for improvement, and how it can refine its CSIRP

Fabian Garzón, CISM, CRISC, GCIH
Has two decades of experience in the IT and information security consultancy services working in various roles including product management, IT security operations engineer, cybersecurity incident management, Payment Card Industry Data Security Standard (PCI DSS) implementation, cyberrisk management and, now, chief technology officer at Hackergame, Colombia. He can be reached at *fabian@hackergame.com* or *www.linkedin.com/in/r-fabian-gg/*.

Gustavo Garzón, CISM, CRISC, PMP
Has more than 15 years of experience in technology and digital security areas as a consultant and team leader implementing information technology projects in Latin America and now is the founder and chief executive officer at Hackergame. He was a member of the development team for *A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)*. He can be reached at *gustavo@hackergame.com* or *www.linkedin.com/in/gustavogarzonr*.

> INCREASINGLY, CLIENTS, INSURERS, AUDITORS AND REGULATORS REQUIRE EVIDENCE OF PREPAREDNESS, AND THE RESULTS OF A TTE CAN SATISFY THESE REQUIREMENTS.

moving forward. Increasingly, clients, insurers, auditors and regulators require evidence of preparedness, and the results of a TTE can satisfy these requirements.

A variety of standards, regulations and guides related to cybersecurity incident response recommends the testing of CSIRPs. **Figure 1** provides a sampling of standards from NIST,[3, 4] the Payment Card Industry Security Standards Council (PCI SSC),[5] the SANS Institute,[6] the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)[7] and ISACA®.[8]

The US Department of Homeland Security's Ready Campaign,[9] designed to educate and empower US citizens to prepare for, respond to and mitigate emergencies, summarizes the benefits and outcomes of exercises to test response plans. They include the following:

- Identify planning and procedural deficiencies.
- Clarify roles and responsibilities.
- Obtain participant feedback and recommendations for program improvement.
- Measure improvement compared to performance objectives.
- Improve coordination between internal and external teams, enterprises and entities.
- Increase awareness and understanding of hazards and the potential impact of hazards.
- Assess the capabilities of existing resources and identify needed resources.

Methodology for Planning and Performing Tabletop Exercises

TTEs must follow some widely accepted methodology or guide. NIST SP 800-84, for example, focuses on TTEs and functional exercises.[10] It can help enterprises design, develop, conduct and evaluate testing, training and exercise events in an effort to assist personnel in preparing for adverse situations involving IT.

TTEs are discussion-based exercises. Personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular crisis situation. A facilitator presents a scenario and asks the participants questions related to the scenario, which initiates a discussion of roles, responsibilities, coordination and decision making. **Figure 2** outlines the NIST SP 800-84 methodology for conducting a TTE.

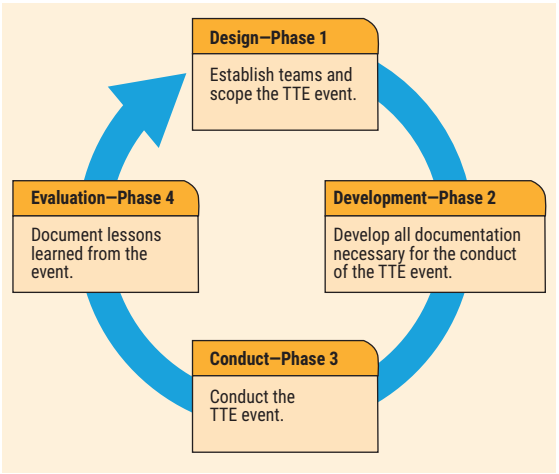
Failures and Challenges of Tabletop Exercises

TTEs are not exempt from weaknesses and discouraging results.[11] Disengaged staff, low attendance, inattention during the exercise and other failures have been identified. They include the following:

Figure 1—Cybersecurity Incident Response Guidelines

Standard	Requirement/Recommendation
NIST SP 800-53	Requires US federal agencies to conduct exercises or tests for their incident response capabilities at least annually
NIST SP 800-61	Requires that the incident response policy, plan and procedures be tested to validate their accuracy and usefulness
PCI Data Security Standard (DSS) 3.2	Requires the implementation of an incident response plan, including a review and test of the plan at least annually
SANS Institute	Recommends drills at regular intervals to ensure that all individuals on the incident response team can perform their duties during an incident
ISO/IEC 27035	Recommends periodic tests of the information security incident management scheme
ISACA®	Recommends comprehensive exercises that involve all key factors: communications, coordination, resource availability and response

Figure 2—NIST SP 800-84 TTE Methodology



- **Lack of clear and achievable objectives**—Do not overcomplicate the objectives of the TTE, and make sure they are achievable.
- **Irrelevance**—The value of a TTE is the opportunity to discuss individual interests (related to areas or roles) and to explore new and unforeseen issues.
- **Tedium**—TTEs are a means to expand the scope of an enterprise's human, process and technology assets. For some individuals, the prospect of a TTE meeting may not be exciting, so it is important to make the exercises interesting.
- **Boring scenarios**—The TTE scenario should ensure that all the participants are engaged. Maintaining their interest in the conversation throughout the session can be difficult, but it can be accomplished by including issues that are specific to the participants' areas of responsibility.
- **Lack of visual appeal**—Pictures, short videos, manipulated images, simulated news and social media messages can create realism and keep participants engaged. Failure to present a visually stimulating experience will result in less interaction and more disengagement.
- **Exercises that are too challenging or not challenging enough**—Achieving the right balance can be difficult. If scenarios go too far, participants may be overwhelmed by the various problems presented to them. This can lead to a reduction in active participation during the TTE. The same is true for a scenario that is too easy to handle and does not test the team.
- **Distractions**—If TTE participants divide their attention between their electronic devices and the exercise—multitasking—neither activity gets the benefit of the brain's full resources, and participants are likely to miss important details of the cybersecurity scenario.[12]

This list of failures and challenges is not all-inclusive, but these shortcomings have been highlighted because LSP addresses them directly.

Game-Based Learning and Gamification

Because many of the failures of TTEs are related to interest, interaction, engagement and participation, creative solutions are needed, and this is where game-based learning and gamification can help. An example of game-based learning applied to TTEs is Backdoors & Breaches, an incident response card game that is simple in concept, easy to play and fun.[13]

Gamification is the craft of deriving fun and engaging elements found typically in games and thoughtfully applying them to real-world or productive activities. Game mechanics such as points, challenges, leaderboards, rules and incentives make game-play enjoyable. Gamification applies these mechanics to motivate the audience to achieve higher and more meaningful levels of engagement.[14]

Many enterprises have experimented with gamification to improve end-user awareness. The results have been remarkable.[15] Games have the ability to disarm people, negating their natural aversion to meetings because games make them fun, and most games are associated with the chance to win. Although using games to increase people's engagement with work may seem counterintuitive, game playing appears to be paying off in the areas of cybersecurity awareness, incident response exercises and cybersecurity skills development.

Lego Serious Play Method

In the search for innovative and proven methods of game-based learning that can be used without any restrictions in the development and execution of TTEs and can mitigate the failures described previously, LSP is an obvious choice. In simple terms, LSP is a systematic method that enables people to use Lego bricks to solve problems, explore ideas and achieve objectives.[16] Lego bricks are combined with animals,

> "LSP...IS A CREATIVE APPROACH TO ENHANCING INNOVATION AND IMPROVING BUSINESS PERFORMANCE, WITH THE FOCUS ON UNLEASHING PLAY."

miniature figures and an extensive selection of special elements such as wheels, tires, windows, trees, sticks, globes, spiral tubes, ladders and fences. **Figure 3** shows models built with Lego pieces during an LSP exercise.

If participants' hands are occupied with Lego pieces, one failure of TTEs—distraction—is already diminished. But LSP is much more than building models. It is a creative approach to enhancing innovation and improving business performance, with the focus on unleashing play. Based on the merging of play with organizational development, systems thinking and strategy development, LSP can lead to improved meetings, faster innovation processes, team growth and better communication.[17]

The purpose of LSP is to change "lean backward meetings" to "lean forward meetings,"[18] where the result is more participation, more insights, more engagement, and, ultimately, more commitment and faster implementation. In several TTEs executed with LSP in Latin America in 2019, the traditional failures of TTEs were reduced. The following are some of the positive outcomes:

- Everyone involved in the TTE has an interest or stake in the agenda.
- Everyone commits to and honors decisions reached after the TTE.
- Team understanding is increased, and team frustration is decreased.
- Participants do not consider the exercises a waste of time.
- All participants share a common understanding and frame of reference (CSIRP in place).
- Conversations flow without the fear of treading on personal feelings.
- Cybersecurity incident response can be complex and multifaceted. TTEs using LSP help participants grasp the bigger picture, find connections, and explore options and potential solutions.
- Participants acquire the skills to communicate more effectively when a cybersecurity incident happens and approach their work with increased confidence and commitment.
- There is a level playing field for discussion.
- Excuses and lack of initiative are less common after the TTE.

Figure 3—Lego Models

What are the practical applications of the LSP method? Many case studies have been documented.[19] Effective team building; shared vision, values and behaviors; and the development of workshops are some of the practical examples. Depending on the challenge (the incident scenario in the TTE), the LSP method has seven application techniques (**figure 4**), all of which are built on four core phases (**figure 5**).[20]

Figure 4—Applications Techniques of LSP

Applications Techniques
Building individual models
Building shared models
Creating a landscape
Making connections
Building a system
Playing emergence and decisions
Extracting simple guiding principles

Figure 5—Basic Phases of LSP

Basic Phases
1. Facilitator poses the questions
2. Individuals build a model
3. Individuals share their stories
4. Questions and reflections

Enterprises are strongly encouraged to adapt scenarios to use in their own incident response exercises. For TTEs executed with LSP, sample scenarios can be found in the Center for Internet Security (CIS) guide[21] or appendix A of NIST SP 800-61.[22] If an enterprise wants to simulate incidents using cloud-based services, Amazon Web Services (AWS) provides sample scenarios.[23]

During TTEs applying the LSP method in Colombia's financial enterprises, it was observed that participants with shared Lego models demonstrated a team understanding of a cyberattack, its impact and the step-by-step incident response.[24,25] They had a shared vision of the response strategy and how to mitigate the simulated cybersecurity incident. Participants can make physical connections between various Lego models to demonstrate how they are related; this helps them solve problems involving cross-functional relationships within the enterprise (e.g., legal, IT, human resources, public relations) and decreases the resistance to performing cross-functional TTEs. Modifying Lego models is analogous to manipulating elements in a system, network or process in a simulated incident scenario. The participants explore "what if" questions (injecting new elements into cybersecurity scenarios) and how these elements can impact the results of their response. By observing connections among Lego model systems and by playing "what if," participants are able to identify the underlying truths that will guide them through real cybersecurity incidents in the future.

Conclusion

A number of efforts can advance an enterprise's CSIRP, including the development of TTEs that are fun, engaging and interactive. Lego Serious Play can be an important tool in a cybersecurity incident response TTE.

When planning a TTE, remember that people tend to be more engaged when the subject matter is pertinent, fun, appealing and challenging. It is important to test the CSIRP and the incident response team as often as possible with different scenarios, different exercises and different mechanisms.

LSP is not just for incident response TTEs. Once cybersecurity professionals understand and have practiced and tested the LSP method, they can use it for other types of workshops, including security awareness, skill building, team building, cybersecurity program goal setting, cybersecurity behavior modification and cultural activities within the community, enterprise, workplace and home.

Endnotes

1 Markey, S.; "Testing Your Computer Security Incident Response Plan," *ISACA® Journal*, vol. 2, 2012, *www.isaca.org/Journal/archives*

2 National Institute of Standards and Technology (NIST), "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," Special Publication (SP) 800-84, USA, 2006, *https://csrc.nist.gov/publications/detail/sp/800-84/final*

Enjoying this article?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

3 National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations," SP 800-53, rev. 4, USA, 2013, *https://nvd.nist.gov/800-53*

4 National Institute of Standards and Technology, "Computer Security Incident Handling Guide," SP 800-61, rev. 2, USA, 2012, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

5 Payment Card Industry Security Standards Council (PCI SSC), Payment Card Industry Data Security Standard (PCI DSS) 3.2.1, 2018, *www.pcisecuritystandards.org/document_library*

6 SANS Institute, "Incident Handler's Handbook," 2012, *www.sans.org/reading-room/whitepapers/incident/paper/33901*

7 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27035-2:2016, "Security Techniques—Information Security Incident Management—Part 2," Switzerland, 2016, *https://www.iso.org/standard/62071.html*

8 ISACA®, *Responding to Targeted Cyberattacks*, USA, 2013

9 US Department of Homeland Security, Ready Campaign, 21 January 2016, *www.ready.gov/business/testing/exercises*

10 *Op cit* NIST, 2006

11 Murray, M.; R. Lelewski; "Common Tabletop Exercise Failures," 31st Annual FIRST Conference, 2019, *www.first.org/conference/2019/program#pTop-Common-Tabletop-Exercise-Failures*

12 Etailinsights, "Why Multitasking Doesn't Actually Increase Productivity," 2014, *www.etailinsights.com/blog/multitasking-productivity*

13 Porup, J. M.; "Backdoors and Breaches: Incident Response Card Game Makes Tabletop Exercises Fun," *CSO Online*, 2020, *www.csoonline.com/article/3509467/backdoors-and-breaches-incident-response-card-game-makes-tabletop-exercises-fun.html*

14 Chou, Y.; *Actionable Gamification—Beyond Points, Badges, and Leaderboard,* Octalysis Media, USA, 2017

15 Bedell, C.; "Play On: How Gamification Can Improve Employee Cybersecurity Compliance," *Infosecurity Professional Magazine*, July/August 2019

16 Blair, S.; M. Rillo; "Serious Work: How to Facilitate Meetings and Workshops Using the Lego Serious Play Method," 2016, *https://b-ok.cc/book/3403461/887f78*

17 Kristiansen, P.; R. Rasmussen; *Building a Better Business Using the Lego® Serious Play® Method*, Wiley, USA, 2014

18 Association of Master Trainers, "The Lego® Serious Play® Method," Serious Play, 2019, *seriousplay.training/lego-serious-play/*

19 *Op cit* Blair, Rillo

20 Rillo, M.; "History: Copyright of Lego Serious Play Methodology Process Elements," Serious Play Pro, 3 August 2018, *seriousplaypro.com/2018/08/03/copyright-of-application-techniques-and-4-core-steps-of-the-lego-serious-play-process*

21 Center for Internet Security (CIS), "Six Tabletop Exercises Prepare Cybersecurity Team," 2018, *www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/*

22 *Op cit* NIST, 2012

23 Amazon Web Services (AWS), "AWS Security Incident Response Guide," 2019, *https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf*

24 HackerGame, "Taller de ciberseguridad con Lego® Serious Play®—Cómo afrontar una Crisis Digital en tu empresa," YouTube, 15 August 2019, *www.youtube.com/watch?v=ikQR0ILU9YY*

25 HackerGame, "Taller de ciberseguridad con Lego® Serious Play®—Cómo hacer que tus inversiones sean seguras," YouTube, 15 August 2019, *www.youtube.com/watch?v=zHsRln_kH6k*