The Importance of Gamification in Cybersecurity

CIRCADENCE®
TECHNOLOGY POWERED BY TOMORROW

HEADQUARTERS
1011 Walnut Street
Suite 400
Boulder, CO 80302

ADVANCED RESEARCH &
DEVELOPMENT FACILITY
398 E. Main St.
CDF Building - 2nd Floor
Tupelo, MS 38804

CENTER FOR CYBER
AUTONOMY
2305 Historic Decatur Rd.
Suite 100
San Diego, CA 92106

WASHINGTON, D.C.
SALES OFFICE
6715 Whittier Ave. - 3rd Floor
McLean, VA 22101

t. 303.413.8800
info@circadence.com

www.circadence.com

A Sobering Scenario

Late at night, the Chief Information Security Officer of a large organization receives a frantic call from the Security Operations Center. Several dozen active exfiltration events had been detected throughout the network, and the internal Information Assurance (IA) teams were in complete panic, not knowing how to execute properly a full triage plan.

The attacker(s) had penetrated the most sensitive areas of the organization's network, stealing terabytes of highly sensitive data. The existing Intrusion Detection System had proven ineffective, and the deluge of stored historical data showed little signs of anomalies. The exfiltration events were discovered by a combination of pure luck, a vigilant and competent Cybersecurity vendor and the attackers' sloppy tradecraft towards the very end of the exfiltration.

Further investigation by a very costly external team of forensics experts showed that the attackers had compromised wireless network printers, where the printers' WiFi and Bluetooth transceivers were left enabled with the manufacturer default settings. By printing documents containing carefully-crafted exploits, users had unwittingly modified the printers' firmware, turning them into attack vectors. So why did the organization's internal Cybersecurity and IA experts fail in the prevention, detection and mitigation of attacks against their organization's most critical assets?

Root Cause Analysis determined that the organization's Information Security procedures, although mature, were ineffective. Despite being placed through conventional training programs, and having obtained nearly every industry certification in Cybersecurity, the IA team lacked the critical thinking skills and practical training required to counter the threat actors in real-life scenarios. After completing each training program at the cost of several thousand dollars each, the company had no cost-effective means of keeping the trainees' skillset current, particularly against evolving threats. Moreover, the training material itself was not very effective to begin with: Students were bombarded with PowerPoint slides in a series of 5-day sessions, with little time and opportunity to practice the theory during the courses. The little they did absorb was quickly forgotten shortly thereafter.

> *"So why did the organization's internal Cybersecurity and IA experts fail in the prevention, detection and mitigation of attacks against their organization's most critical assets?"*

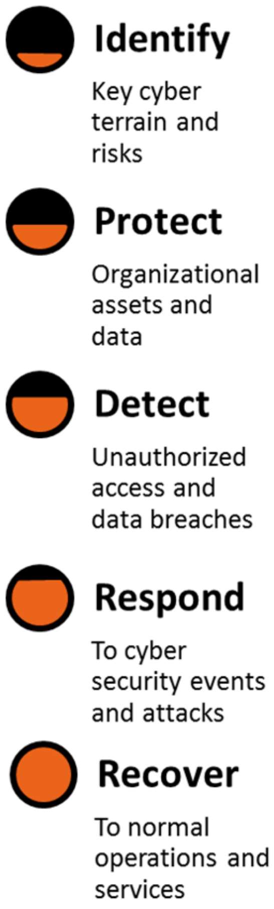
Identify
Key cyber terrain and risks
Protect
Organizational assets and data
Detect
Unauthorized access and data breaches
Respond
To cyber security events and attacks
Recover
To normal operations and services

Figure 1. National Institute of Standards and Technology (NIST) Cybersecurity Framework Benchmark

Why Gamify Learning?

Students in science, engineering and mathematics classes taught via a traditional lecture format are 1.5 times more likely to fail than students in classes with active learning, a recent study shows (1). Additionally, teaching approaches that turn students into active participants show exam improvement by 6%. Although there is no concise definition, active learning includes calling on individuals or groups randomly or having students work in groups to discuss or solve an issue (1). The results of this study merely scratch the surface for the potential learning impact of game-based learning, or gamification, which is likened to active learning on steroids.

In recent years, gamification has become a buzzword in education, training and business marketing. It has been applied to build teams, train personnel, improve health or to earn airline mileage rewards. Gartner Inc. defines gamification as the use of game mechanics and experience design to digitally engage and motivate people to achieve their goals (2).

> *"…teaching approaches that turn students into active participants show exam improvement by 6%"*

One example of successful gamification in the training sector was the game *Monkey Wrench Conspiracy*. In 1999, the company Games2train, recognizing the impact of gamified training, released the training game to teach industrial engineers how to use new 3-D design software – selling over one million copies (3). To succeed in the game, the players/trainees utilized the 3-D design software to design everything for their missions to rescue a space station from alien hijackers (4). What was unique about this game was that the players were motivated to train on a sophisticated real-world tool while having fun.

A vital component of games is immediate audio/visual feedback. This feedback confirms the player's action and grants them the outcome of that action (5). An article researching the Monkey Wrench Conspiracy and discovery-based learning describes the context of a game as motivating and that, "the game provides a safe environment for the learners to solve problem and make mistakes without fear of failure. They can ask questions by clicking on new terms. The game models problem solving in a way that involves users' multiple senses. The game provides constant feedback and hands-on practice. In addition, the game situates the learners in an environment where they are challenged to complete game tasks to further advance in the game." Ultimately, the overall approach of the training game is similar to simulated learning, which applies to solving relevant, real-world problems (4).

Project Ares Addresses the Training Gap in Cybersecurity

Navy SEALs spend much more time training compared to the amount of time they are actually on mission, which includes a significant amount of team building and team-based training. Cybersecurity teams need to start utilizing the same training approach – they can't wait for a breach or Cyber-attack to learn from the experience, and they need to know how to work together to defend their mission systems, which include networks, applications and data.

Currently, Cybersecurity teams predominantly utilize two training methods: Lecture-based learning, or high-fidelity simulation. Outside of traditional academic settings, lecture-based learning is often received within the context of a conference or an industry training program. The relevancy of the content in these settings is fleeting as threats are constantly expanding and evolving – so a Cybersecurity professional would need to be in constant attendance in order to stay current, which is unrealistic. Moreover, finding qualified instructors, developing training material, and keeping both the material and the instructors up-do-date and relevant is a daunting task: Good instructors practice Cybersecurity on daily basis, which makes their availability to teach extremely limited and their hourly-rates very high. Additionally, high-quality classroom instructions are simply not scalable: Trainees require highly-individualized training at different learning paces, sometimes requiring one-on-one instructor access throughout the course that may need to last weeks or months.

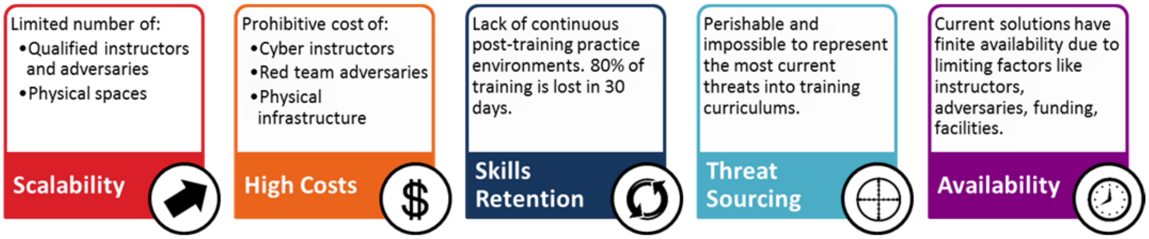
Limited number of:
•Qualified instructors and adversaries
•Physical spaces
Scalability
Prohibitive cost of:
•Cyber instructors
•Red team adversaries
•Physical infrastructure
High Costs
$
Lack of continuous post-training practice environments. 80% of training is lost in 30 days.
Skills Retention
Perishable and impossible to represent the most current threats into training curriculums.
Threat Sourcing
Current solutions have finite availability due to limiting factors like instructors, adversaries, funding, facilities.
Availability

Figure 2. Shortfalls in the traditional Cybersecurity training model

On the other end of the spectrum, Cybersecurity teams may deploy high fidelity exercises where a team of anywhere from 20-90 people come in over several days to a replica of a target network and conduct Blue/White/Red team simulations. Albeit extremely relevant, useful and educational, these high fidelity simulations require significant manpower, time and financial resources that limit the ability to execute them with any frequency – and may be cost prohibitive for a Cybersecurity team.

Figure 3. Circadence's solution to the Cybersecurity training gap - a gamified training platform, Project Ares

Project Ares™ is Circadence®'s answer to address the gap between lecture-based and high fidelity learning for Cybersecurity professionals, via a gamified training platform that is scalable, cost-effective, and very flexible to customize, modify and update. Despite a number of studio and indie releases of games in the Cyber genre, the game-based training market remains relatively nascent and shows tremendous potential for a blockbuster that can disrupt the legacy training models.

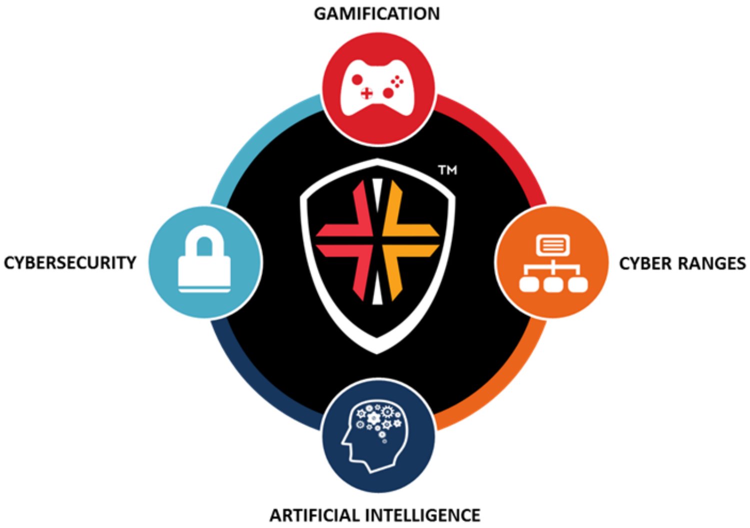

Figure 4. Project Ares provides a nexus of Cybersecurity, gamification, cyber ranges and artificial intelligence

Project Ares provides Cybersecurity teams the real-time opportunity to practice skills and hone tactics via its next generation training platform. Project Ares deploys realistic, mission-specific virtual environments with real-world tools, network activity and a large library of mission scenarios, available 24/7. To keep its content relevant, Project Ares employs a modular architecture that enables the platform to quickly and easily add new missions to address rapidly changing threats.

The platform may be utilized to train individuals or teams and provides the instructor with a trainer view for progress monitoring, performance assessment, and real-time training intervention. The platform catalogues a team member's actions and skills thereby creating a record for institutional and team memory. Because it is also available online 24/7, it increases the availability and access to train individually or by team, which approaches the Navy SEAL model.

Artificial Intelligence Makes Project Ares More Useful

Not only does Project Ares provide relevant, effective gamified learning, but it also introduces an Artificial Intelligence (AI) component as a computerized advisor, umpire or opponent. The AI component provides on-demand help and instant feedback to trainees, which results in freeing up the trainer's time to help other trainees or facilitate more focused orchestration tactics.

"…embedded instructional support allows personalization of learning, enabling trainees to explore in greater detail a game's instructional content…"

The current AI-based advisor is called Athena, which is powered by IBM Watson, along with other proprietary AI systems. Athena provides in-context knowledge to trainees and trainers and has been trained on a large corpus of deep Cybersecurity information.

According to a recent article on gamification, embedded instructional support allows personalization of learning, enabling trainees to explore in greater detail a game's instructional content by providing content, either remedial or supplementary deeper explanations or related topics, when a trainee wants to know more (6).

The AI component Athena enables the trainees to focus on Ares' game content rather than its operational rules. For example, a trainee can ask Athena for help if stuck at a mission, allowing the trainee to acquire and rehearse new procedures and tradecraft, while simultaneously progressing and learning within the context of the mission.

In addition to providing in-platform help, AI provides monitoring and scoring as an umpire, and enables the trainees to play the missions against an adaptive, dynamic opponent that continually challenges the players to improve their tradecraft and hone their offensive and defensive skills.

Conclusion

Gamification has a tremendous opportunity to revolutionize the speed, efficacy and relevancy of training in the quickly-evolving landscape of the Cybersecurity sector. Game-based learning provides immediate feedback in a safe environment where trainees can solve relevant problems without consequence – ideal for Cybersecurity context. Project Ares takes gamified training to the next level by facilitating teamwork in addition to introducing an Artificial Intelligence component that provides both in-game help and increases the challenge factor on an as-needed basis. Circadence anticipates the future of Cybersecurity training to include lecture-based and high fidelity training as supplemental, and that the basis of training will be a gamified virtual platforms such as Project Ares to provide the most effective overall professional training, recertification and growth.

About Circadence

With over 20 years' experience, 34 patents and a history of cutting-edge software development, Circadence solves complex customer problems using robust, industry-leading solutions. Circadence is a recognized leader in the Federal cyber security community. Powered by a culture of innovation, intellectual property and the demands of an evolving cyber market, Circadence is using its current cyber range solution and next generation cyber security training platform to address this critical national security challenge and tremendous business opportunity.

Works Cited

1. *Active learning increases student performance in.* **Freeman, Scott, et al., et al.** 2014, PNAS, p. 28.

2. **Burke, Brian.** *Gamify.* Boston : Bibliomotion, Inc., 2014. p. 1.

3. Monkey Wrench Conspiracy Official Website. *Games2Train.* [Online] http://www.games2train.com/site/html/tutor.html.

4. *Examining the pedagogical foundations of modern educational.* **Kebritchi, Mansureh and Hirumi, Atsusi.** [ed.] C-C. Tsai, R.S. Heller and P. Twining. 2008, Computers & Education, p. 1735.

5. **Markopoulos, Angelos P., et al., et al.** *Gamification in Engineering Education and Professional Training.* Corresponding Author: amark@mail.ntua.gr.

6. **Kapp, K.M.** Choosing your level: Using games and gamification to create. [ed.] M Murphy, S Redding and J Twyman. *Handbook on Personalized Learning for States, Districts, and Schools.* 2015.