Reinforce Teamwork and Creativity for Cybersecurity in a Classroom Setting: A Team Activity for Building a Strong Cyber Defense using K'Nex®

Abstract

Can students learn about teamwork, creativity and cybersecurity at the same time? Yes, they can when Management and Organizational Behavior faculty team up with colleagues in Information Technology (IT) and Cybersecurity to implement a game-format as one of their pedagogies. We have adopted this team building activity successfully in a variety of courses for undergraduate and graduate IT and business students. For our undergraduates, we use this team activity to reinforce theoretical material previously covered in lecture format. For our graduate students, we use this approach to introduce students to each other at the beginning of the program in orientation.

Keywords: Teamwork, Creativity, Cybersecurity

Introduction

Defending a company from cyberattacks is a team effort and its effectiveness is partly based on the strength of the defense as well as the ability to be prepared for attacks that may happen in the future. However, we find that many of our students have misconceptions that cybersecurity is only about technical knowledge and skills. Students often assume a career in cybersecurity is often "geeky" and primarily entails "working solo." Contrary to this misconception, the cybersecurity profession demands diversified talents and skills including problem solving ability, interpersonal communication skills, and language facility (Liu & Murphy, 2017). Further, pedagogies that allow students to actively participate will motivate and engage them to achieve superior learning outcomes (Beard and Wilson, 2006).

To address the above misconceptions and contextualize the ten "Cyber Ops First Principles," faculty members from the Information Technology and Cybersecurity Department along with faculty from Management and Organizational Behavior Department have collaborated and designed a team activity which serves as an analogy for building cyber defenses.

Exercise Overview

The team activity utilized the K'Nex construction system consisting of interlocking plastic parts including rods, connectors and wheels. K'Nex can be pieced together to form a wide variety of structures. The K'Nex building system was designed to aid in the teaching of science, technology, engineering and math topics and it is therefore well suited to a cybersecurity application.

The team activity includes two major parts. The first part focuses on "building a tower" to meet certain given criteria; while the second part is dedicated to reflection and a discussion of how “Cyber Ops First Principles” are embodied in the students’ tower designs. Prior to engaging in this activity, the instructors had already introduced the cybersecurity first principles to the students. Further, the inherent nature of this activity adds tremendous value for reinforcing iterative and incremental design concepts.

Each team of 4 students was given an identical set of K’Nex building materials in a large envelope. The activity instructions are documented as follows:

Team Activity Building a Strong Cyber Defense

Part I: Designing and Building Your Tower

Each team is asked to construct a tower based on the materials in the envelope. The height of the tower and its stability reflect the strength of your cyber defenses and the appearance (aesthetics) of your tower represents the elegance of your solution and its ability to keep up with the constant changes in the field. Different colors represent different cybersecurity techniques, for defense-in-depth you need multiple colors,

The evaluation criteria are summarized in the following chart:

Evaluation Criteria	**Percentage**
Height	40%
Stability	30%
Appearance	20%
Colors	10%

This task requires technical capability, coordination, teamwork, and creativity for successful completion.

Process:

1. Planning the design: each team have 30 minutes to get to know your team of 4 or 5, to understand the skills that they bring to the table, and to plan the design of your tower by looking at the components in the envelope. At the end of the design phases each team must return all components to the envelope. “Pre-fabricated” pieces of the tower may not be assembled during the planning phase. The tower must be self-supporting and not lean on another structure, person, wall, etc.
2. An instructor or teaching assistant will inspect the envelope to ensure the pieces are as they were when each team received the envelope.
3. Construction: each team will have 4 minutes to build your tower from the components in the envelope. This is a team project so it is important to emphasize that each team member should have some role in the construction effort.
4. Evaluation: The instructor will inspect each tower, with the main evaluation being shown in the above chart. One or two members of the team will explain the design of the tower to the instructor and how it meets the criteria for height and aesthetics. This should be a persuasive presentation and show your team’s commitment to the design.
5. Having reviewed all the structures and learned from them, the team will be asked to construct the tower again using the lessons learned
    a. Planning and redesign: 15 minutes
    b. Construction: 3 minutes
    c. Re-evaluation

Part II: Discussion and Reflection

A panel of four judges evaluated each team's tower against the criteria independently. Then the individual judges' scores were collected and aggregated, Once the winning team was selected, all of the students engaged in a discussion of management topics including aspects of motivation, leadership, team work, task organization, and the practical matters of what worked and what did not work. After the discussion of management and group dynamics, the instructor recapped the First Principles of Cybersecurity and asked the students to reflect on how these principles apply in the K'Nex tower building activity.

"Cyber Ops Frist Principles" are the foundation upon which security mechanisms are reliably built and security policies can be reliably implemented. The students are asked to use these First Principles to examine the design of real-world security mechanisms. The First Principles of Cybersecurity include:

- **Abstraction:** summarizing or explaining in a way that people can easily understand
- **Domain Separation**: separating the areas where resources are and people work prevents accidents and loss of data or private information
- **Information Hiding:** any attempt to prevent people from being able to see information
- **Layering**: a contemporary cybersecurity mechanism to use multiple layers of defenses for protecting information
- **Least Privilege:** limiting what people can do with your information and resources
- **Minimization:** the goal is to simplify and decrease the number of ways the software can be exploited

- **Modularity:** The concept is like building blocks. Each block (or module) can be put in or taken out from a bigger project. Each module has its own separate function that is interchangeable with other modules.
- **Process Isolation:** a process occurs when task is executed. Keeping processes separate prevents the failure of one process from negatively impacting another
- **Resource Encapsulation:** A resource can be hardware such as memory, disk drives, or a display screen. It can also be system objects such as semaphores, a linked list, or shared memory. Processes (or programs) need resources to run. Resources have to be separated and used in the way they were intended.
- **Simplicity of Design:** the less complicated something is, the less likely it is to have problems. It is also easier to troubleshoot and fix.

Based on the class discussion following the K'Nex building activity, we found that some First Principles are more intuitive and easy to relate to than others. For example, modularity was the principle most students could explain and implement with ease in their team activity due to the "plug and play" nature of the K'Nex materials they used to build towers. Simplicity of Design is another principle that the students can easily articulate and understand when reflecting on their team's tower design. However, some principles, such as information hiding and minimization, are more challenging to implement in this team activity.

Feedback from the student participants was predominantly positive. This team activity promoted collaboration and interaction among students while also helping students a gain better understanding of Cyber Ops First Principles and their application in the real world. Perhaps most importantly, students became aware of the reality that cybersecurity requires much more diversified expertise and skills beyond simply "hacking".

Session Description

The session will begin with a <u>15-minute </u>overview by the presenters. This overview will cover 3 themes. First, we will describe how we modified the Tinker Toy exercise as described by McNeely (1994) as well as Coff and Hatfield (2003) by switching the building material from Tinker Toys to K'nex. Second, we will share the basis for using a management exercise with Information Technology (IT) and Cybersecurity students based on the previous work of Galliano et al. (2017), LeClair et al. (2013), and Liu and Murphy (2017). Finally, we will discuss how this exercise can be used with either a large group in an orientation activity, or in class. We will also share our experience using this exercise with both undergraduate and graduate students.

Then we will form teams with the participants in the session and distribute K'Nex for building along with building instructions (this will take 5 minutes). The activity will be run as described above with 30 minutes allotted to get to know your team and plan your tower design, followed by a 4-minute building period and then 10 minutes for evaluation. (Please note we will not run the second half of the activity with planning and redesign, construction, and re-evaluation.) This active section of our session will total <u>50 minutes.</u>

The final 25 minutes of our session will be devoted to debriefing the exercise, reviewing the learning outcomes and allowing for participants to ask questions of the presenters. If time allows, we will share personal experiences from our various classes. We will also ask out colleagues to identify various forms of incentives that might be tied to this assignment.

References

Beard, C. & Wilson, J. (2006) Experiential Learning: A best practice handbook for educators and trainers. Second edition. Kogan Page Limited. London and Philadelphia.

Coff, R.W. & Hatfield, D.E. (2003) Tinkering in Class: Using the Tinker Toy Exercise to Teach Frist Mover Advantages and the Resource-Based View. Journal of Strategic Management Education 1(1): 1-15.

Galliano, J. S., Webb, J. O., Fonseca-Lind, S. & Hargiss, K. M. (2017). Improved Matching of Cybersecurity Professionals' Skills to Job-Related Competencies: An Exploratory Study.

LeClair, J., Abraham, S., & Shih, L. (2013). *An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce*. Paper presented at the Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference, Kennesaw GA, USA.

Liu, X., & Murphy, D. (2017). Are They Ready? Integrating Workforce Readiness into a Four-Year College IT/IS Curriculum. *The Proceedings of 20th SAIS (Southern Association for Information Systems Conference)*. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1007&context=sais2017

McNeely, B.L. (1994) Using the Tinker Toy Exercise to Teach the Four Functions of Management. Journal of Management Education 18(4): 468-472.