**SEI Webcast**

*How Do We Teach Cybersecurity?*

**by Rotem Guttman and Josh Hammerstein**

**Shane McGraw:** Hello. Welcome to today's SEI webcast, "How Do We Teach Cybersecurity?" My name is Shane McGraw, Outreach Team Lead here at the Software Engineer Institute, and I'd like to thank you for attending. We want to make our discussion today as interactive as possible, so we will address questions throughout today's talk, and you can submit those questions in the YouTube chat area, and we will get to as many as we can. Our featured speakers today are Rotem Guttman, and will be moderated by Josh Hammerstein. Rotem is a Senior Cybersecurity Researcher here at the SEI. Josh is the Technical Manager for Research and Prototypes in our Cyber Workforce Development Directorate. Now I'd like to turn it over to Josh. Josh, good afternoon. All yours.

**Josh Hammerstein:** Thanks, Shane. As mentioned, my name is Josh Hammerstein, and I'm the Technical Manager for Research and Prototypes within the Cyber Workforce Development Directorate here at the SEI, and one of the things that we focus on is creating new and innovative ways for people to learn and to develop hands-on cyber skills. You're going to hear from Rotem Guttman today, who's going to be sharing lessons learned that we've learned over the past decade on how to create motivating training that engages learners and retains their focus. With that, I'll kick it off to Rotem.

**Rotem Guttman:** Thank you, Josh. So hi. I'm Rotem Guttman, a Senior Cybersecurity Researcher with the Software Engineering Institute's CERT Division in the Cyber Workforce Development Directorate. I'm also an adjunct faculty member at the Information Networking Institute over on the academic side of campus. My research areas focus on education and training, ludological techniques, augmented and virtual reality, cyber kinetics and more, but really, my passion has always been addressing the pipeline problem, namely the lack of cybersecurity professionals. This year alone, there's a projected worldwide shortage of three and a half million cybersecurity professionals, so basically, we need to train up every man, woman and child in state of Connecticut and we'd still be a couple of thousand jobs short. So clearly, a problem of this scale isn't going to solve itself. Here at CERT, we've been tackling this problem for more than 20 years. At first, we provided repeatable instruction on removable media, and then as bandwidth become-- became more widely available, we moved on to streaming recorded content and eventually capturing live instruction. This would become a hallmark of our methodology for years. After all, live instruction was considered the gold standard. So the question we were focused on was, "How do we make the remote experience as good as sitting in a classroom with a live instructor?" Over the years, we began implementing what we now call a learning management system, as well as various assistive features and a wide variety of content that made it simple for users to find the material that they needed quickly and jump right into the classroom setting with hands-on labs, exercises, everything else that you'd expect from the classroom. These features, taken together, allowed us to complete the traditional learning cycle. Students would sit through a lecture as they built their knowledge. They'd participate in labs to build their skills. They'd join in exercises to gain the experience that they needed, and they'd be evaluated to demonstrate their proficiency before starting the cycle again. But ask yourself this. Who are the top performers in your organization today? Who are the rock stars in your cybersecurity workforce? Are they the ones that have taken the most classes or are they the ones that dive into every problem themselves, not waiting for a class to even be offered before they're ripping through the barely written documentation on some new tool or technique? How do we build that into our training audience? How do we nurture the attitude that allows the spirit of self-education to grow? The answer is by creating immersive learning experiences. By creating a living world. By crafting an experience that responds to and rewards the students' curiosity. That way we can teach them to teach themselves. The key here is to know your audience and meet them where they are. Give them challenges that are too hard without enough support and you'll discourage them. Too easy and they'll get bored. Now, you may already be familiar with what I'm talking about. In positive psychology terms this is what we would call a flow state or as it's more commonly called, being in the zone. One of the hallmarks of this state is losing track of time as you're completely absorbed in the task, and this is where immersive learning experiences can truly shine, drawing in students for a lot longer than they expected. With the right design, your training audience won't just train for longer but also more often. By focusing on what motivates your audience in particular, you can draw them in time and time again to continue consuming your training content. Now, we've used a wide variety of techniques in determining what motivates a particular audience. One good option, where it's possible to administer it, is to utilize the Reiss Motivation Profile. By looking at what common motivators exist across your training audience, you can craft an experience that speaks to what uniquely motivates them, be it showcasing their achievements publicly to satisfy their need for status or creating a tight-knit community to satisfy their need for social contact. The key is to provide a motivator that speaks to your unique audience. When you can get both of these elements right, your students will voluntarily spend their own time, nights, weekends, lunch breaks, whatever time they have available, to continue their training. That's how you can stretch your training dollar as far as it can possibly go.

**Josh Hammerstein:** Hey, Rotem, we got a question from the audience. So someone's asked if you'd give some more detail about this profile that we're seeing. You know, what exactly does it mean?

**Rotem Guttman:** Okay. So this-- actually, full disclosure, this is my Reiss profile. I wouldn't share anybody else's, and what it's showing here is essentially the way the RMP works is it's divided into a set of unique motivators that are common across all of humanity but are unique to you in how much you want them. So, you know, I clearly value beauty a lot less than the majority of the population, and so what you want to do is take these surveys, give them to a representative sample of your training audience and then see what trends tend to appear. So if you're training a bunch of soldiers, you'll often see that a lot of them value honor very highly, moreso than your-- the average people, and so that's something you can target. When you see those trends emerge, when you see them showing up time and again in your audience, you can then craft your training to provide a sense of honor for succeeding in it, to really focus on what's going to speak to that individual audience.  There's other things that you can utilize.  If there's a sense of status that's important for them then maybe you want to give badges that are publicly visible.  You know, one of the things that I tend to kind of rant against is applying these strategies-- badges and leaderboards are great examples-- applying them without knowing your audience, because if you have an audience that doesn't care about status, you can put all the badges you want around it, they're not going to care, and so you really have to match the techniques that you use to the audience that you have.  Is that good, Josh?

**Josh Hammerstein:** Yeah.  Yeah.

**Rotem Guttman:** Okay.

**Josh Hammerstein:** Definitely.

**Rotem Guttman:** Okay.  So that's enough with theory.  Let's look at some concrete examples.  The first immersive training that we created was for an industry consortium that was focused on both intel and technical aspects of cyber attack and defense.  So the first thing we did is observe the previous iteration of the training for this consortium, and while the technical content was excellent, two problems stood out, defensiveness and lack of engagement.  You see, this training audience was already in the role that they were being trained for, and the results of this training were available to their supervisors.  So when we tried to give feedback, no matter how carefully worded, they didn't hear, "Hey, there might be a better way to do that."  What they heard was, "You're bad at your job and we're going to tell your boss."  So of course, rather than internalize their mistakes and learn to improve, they push back.  The most common thing that we'd hear were comments like, "Well, it isn't that way at the office," or, "That's not how it would've happened," and at first, we took these comments at face value.  We were always striving to make the environment more and more accurate.  I'll tell you, we kept doing this where it got to the point that I had a participant tell me, "Well, the background is a different color than at the office, so I would've noticed that alert at the office, but here it sort of blended in so I missed it."  Yeah, I mean, there's only so much we can do to make the training environment match the work environment when we have participants coming in from companies all around the world.  So clearly, we had to take a different approach.  The second problem was a lack of engagement.  Sure, at the start of the day the participants were raring to go, but that motivation quickly wanes when you're confronted by what seems to be an endless collection of PowerPoint slides.  By the third day of the training, participants were averaging 17 minutes between requests for a break.  So, you know, every couple of minutes a hand would go up.  They'd be like, "Hey, can we go to the bathroom?"  "Hey, can we go get some food?"  "Hey, can--" you know, whatever the reason was, the participants were tired and their motivation was gone, and so something had to change.  So we did the same thing that Hollywood does when they need to get your attention.  We threatened to destroy the world. <laughs> Now, imagine for yourself that you're used to getting an email inviting you every once in a while to a three-day training event, and instead of that, this is what lands in your in-box.

<video plays>

**Rotem Guttman:** So needless to say, enrollment went up.  Class was filled to capacity.  Once here, we engaged our audience by creating a living world which they could effect.  We gave them an objective and allowed them to explore the world in order to solve it, and in doing so, created a learning experience that was naturally self-paced.  Let's take a look at the instruction our audience got to this experience once they arrived.

<video plays>

**Rotem Guttman:** Welcome.  You've been selected as the newest agents for the A.R.M.O.R. Cyber Heroes Initiative.  You'll be joining teams tasked with responding to global cyber threats as they emerge.  Over the course of the next few days, you will receive extensive briefings on A.R.M.O.R. policies and proc-- just a moment.  Yes?  Yes.  I'm with them right now.  All right.  Yeah, bring it here. <pauses> Agents, change of plans.  It appears your skills are needed immediately.  There'll be time later for going over your benefits package.  This video was just posted to 5Chan [ph?] and I'm assigning your teams to investigate it.

**Dr. Diabolicov:** Governments of the world, this message not for you.  For too many years one world power has stifled, exploited their people.  Today, <background music> I give the people the opportunity to press a Reset button on humanity.  I have placed vials of weaponized smallpox in several key locations around the globe.  I leave it to the people to decide if the smallpox will be released.  Linked in this post is a tool that will allow any individual to place their vote to reset civilization and preserve it.  If I suspect any interference on the part of any government, I will immediately trigger the smallpox's release.  You have two days to make your decision.  I leave it in the hands of the people.

<video ends>

**Rotem Guttman:** So what we did here was by using a semi-fantastic setting, we diffused the defensiveness.  How ridiculous would it be, you know, to say, "Well, this isn't how it would be at the office," when you're playing a superhero?  That natural suspension of disbelief associated with the exercise extended to the training content itself, and the engaging nature of the evolving scenario kept the students hooked and looking for more.  In fact, this was so <laughs> successful it almost shot us in the foot. You see, it observed how food motivated the students who were in the previous iterations as they kept asking for food breaks, so we provided three newspapers with their lunch break. The New York Times, the Pittsburgh Post-Gazette, and an Endgame paper that we printed up that was filled with stories and intel artifacts that we figured they'd notice when they went to get the food. What we hadn't guessed is that when we, you know, announced that the lunch buffet was open, that nobody would get up to eat. The students had arranged themselves into three teams and they were all so engrossed and so busy, no one got up to eat. So we eventually said, you know, "The food's going to get cleared away soon. Please go and eat," and so they only sent one representative from each team to bring back plates for everyone else so they could keep working. After the first two came back with plates of food and nothing else, we started getting worried, until finally the third one came running in carrying the entire stack of newspapers and basically waving them saying, "Hey, look at this." But that, that's the engagement that we're looking for. Exactly that type of engagement with our training audience.

**Josh Hammerstein:** Rotem, another question from the audience.

**Rotem Guttman:** Oh, yeah.

**Josh Hammerstein:** Can you go into more detail about the scenario involved for the participants?

**Rotem Guttman:** Sure. Okay. So for that particular scenario-- we actually did several seasons of that scenario, but for that original one, we actually had this full storyline that went back all the way to the 1980s, and we basically plotted out what happened with this individual, this guy that's calling himself Dr. Diabolicov. Who he actually was, where he used to work, why he got, you know, why he went nuts, basically, you know, why he's threatening to destroy the world, and then all the different interconnects there. We had intel artifac-- several hundred intel artifacts about every mover and shaker there, from OSNs to, you know, fictitious signals, intelligence and so forth, so that our participants could actually do a full workup and figure out who's doing what, who's involved, what their motivations are, and then even within the scenario we had people acting against interests. So there was somebody involved in the scenario who wasn't a true believer but was actually taking advantage of it and had bought a bunch of stock in companies that make smallpox vaccine so they could make a bunch of money when the entire world had it. And, you know, so we kind of built that scenario while at the same time the technical side, they were reverse engineering this voting tool that he had created, trying to figure out where the votes were going. Once they figured that out, they, you know, went to go seize those machines and realized, "These are just compromised machines that are actually proxying the votes and they go back to a bunch of command and control servers that had to actually discover where they were located and, you know, it just-- a scenario that kept evolving day after day as they would get new intelligence, while at the same time we were creating new intelligence artifact on the fly based on their requests, their RFIs that they would be submitting to our team that was waiting on the back end.

**Josh Hammerstein:** Rotem, we got another question from the audience.

**Rotem Guttman:** Sure.

**Josh Hammerstein:** This question comes from Sydni. Question is, "Is there a place where I can create an escape room challenge for training?"

**Rotem Guttman:** An escape room challenge for training. So we've actually done some escape room stuff. If you don't mind, I'll defer that question until a little later in the presentation and then I'll go into little more detail, because we do have some content that I think would be useful for you that you can adapt that I'll actually talk about in a couple more slides.

**Josh Hammerstein:** Okay. And then we have time for one more question before you move on.

**Rotem Guttman:** Sure.

**Josh Hammerstein:** This one comes from Sarah. What were the traits that the participants valued the most to drive this type of training?

**Rotem Guttman:** It really, it really depends on your training audience. So when you're talking about-- in this particular training, because they were in this consortium and their supervisors had access to the data, they really cared about status and acceptance were two things that they cared about. They didn't want to stand out from their peers. They wanted to be seen as a team player and they also wanted to get that recognition of being good at their jobs, and so that's something that we really had to built into that of giving them the chances to both be a team member, and that's why we built it in such a way that they self-organize into these groups, while at the same time being able to show off what they're discovering, and so we actually created in several points there where they had to give briefings, you know, of fictitious supervisors, and so that was part of the exercise for them is how they're briefing that, and that was all made available to their actual supervisor. Any other questions?

**Josh Hammerstein:** No, that's it for now.

**Rotem Guttman:** Okay. So let's see. Where were we? Okay. So with this early success, we extended this approach beyond the purely cyber domain. Extending our training into the field of combined arms, we developed a system that allowed effects to propagate between the cyber and the kinetic domains, and so by supporting a live mission, cyber operators were kept engaged throughout the training period as the constant feeling of suspense drove them to continue with the mission until it was complete, either successfully or otherwise. So let's take a quick look at that system.

<video plays>

**Male Voiceover:** CERT Advanced Cyber Kinetic TTP Simulation system is designed to seamlessly integrate a cyber simulation environment with kinetic operations conducted within a virtual battlefield simulator. Here we can see on the left an OP4 Cyber Operator disabling a drone system within the STEP interface. On the right, we see the drone operator's view within the battle simulator. As the link is disabled, the drone operator system ceases to function. In this particular scenario, enemy forces are holding a high-value target as a hostage. To support the hostage rescue mission, cyber operators compromise the enemy's security camera system and determine where she is being held, as well as enemy troop positions. Now that the hostage's location has been confirmed, special operators move in to rescue the hostage under the cover of darkness. Unfortunately, their progress is stymied by search lights installed around the enemy facility. To support the kinetic operations, cyber operators must disable power to the facility's lighting systems. Here we see a cyber operator leveraging an attack within our STEP environment to do just that. As the system is turned off, the effect propagates into the battlefield simulator and allows our troops to neutralize the enemy forces and move into the facility and rescue the hostage. All infrastructure systems within the blue forebase [ph?] and the outcore facility are fully replicated within the STEP environment, allowing them to be attacked just as they would in the real world. By combining the cyber and kinetic domains, the ACTS [ph?] system allows operators in both fields to gain an understanding of the capabilities granted and restraints imposed upon the operations by their counterparts. Additionally, combined arms training and mission rehearsal can now be accomplished without resorting to white carding effects. The increased motivation provided by ACTS-enabled training cannot be ignored. Engagement by the training audience is greatly increased as they feel they are supporting a live mission and can connect emotionally with the task at hand. CERT Advanced Cyber Kinetic TTP Simulation System.

<video ends>

**Josh Hammerstein:** So Rotem, we got a couple more questions. This first one comes from Taz, which I think you'll want to defer on because you'll address it later. But this one question asks-- this pertains to the previous cyberheroes. Have any of these techniques been applied in a traditional undergraduate setting, perhaps spread over a semester-long course?

**Rotem Guttman:** That's literally my next slide. It's a graduate setting, not an undergrad setting, but equally applicable, and actually, we're planning for next semester to apply it to a undergrad course as well in the business world, so I'll defer, because that's literally the next thing I'm going to talk about.

**Josh Hammerstein:** And this next question comes from Peter. "Is any of this training available in FedVTE?"

**Rotem Guttman:** I don't know what the status is of FedVTE or what parts of this are available there. I would have to check, but if they send an email to info@sei.cmu.edu, it'll get routed to me and I'll be able to get back to them on that. Okay.

**Josh Hammerstein:** All right.

**Rotem Guttman:** So I'm going to move on to the-- I'm going to go back to that first question right now, actually, because interesting story. I don't know if anybody heard, but COVID happened, and so everything got shut down and, you know, we were all struggling to adjust and as I mentioned at the start, I'm also the instructor for CMU's Cyber Forensics and Incident Response capstone course, and since on the academic side we were facing those same challenges, I wanted to highlight this course here to show you that even if you aren't an industry consortium or a government agency, these techniques can be applied. So exactly what that question was asking. So together with another SEI employee, Will Nichols, and using only free and open-source tools and a pile of spare computer parts literally fished out of the trash and running out of his basement, we completely redesigned the course over the summer to allow for fully remote and asynchronous instruction. This let us support students spread across a wide variety of time zones, from the West Coast to the Middle East, all while still providing an immersive and student-driven experience. So let's take a look at the part of the content that waited for those students when they first logged into the class.

<video plays>

**Rotem Guttman:** --from the glorious nation of Ambrosia. I'm sure you've heard a lot about our beautiful country already, but I'm here to announce that Ambrosia is open for visitors. With over 11 kilometers of beaches to explore, you'll be able to relax on the sand, kick back and enjoy your vacation in peace and quiet. Don't believe the rumors. We've had more than 10 years without civil unrest, and not a sing-- ah, what? That doesn't count. That was barely a riot. They didn't even have-- <beeps> with over three years of peace and quiet as our compassionate government provides for-- ah, now-- wha-- wai-- where did we even get this director? I want him taken out behind the chemical shed and sho-- <beeps> our peaceful atmosphere has been uninterrupted for as long as anyone can remember. Why, just ask any citizen on the street <mumbles> <inaudible 00:23:36>. So come on over on any one of our three magnificent, modern and luxurious ferryboats and see for your-- what? Sunk? How? Oh. A wave? In the ocean? Chance in a milli-- <beeps> so come on over on either of our magnificent, luxurious cargo ferries and see for yourself. The island of Ambrosia. A vacation here is truly a taste of the fun.

<video ends>

**Rotem Guttman:** So we created this Banana Republic. <laughs> Literally their primary export was bananas in this fictitious island nation and we created a cast of characters all involved, you know, in their own activities, often with conflicting agendas and a myriad of storylines, from cabinet members cheating on their spouses to employees embezzling money or selling state secrets. The students were organized into investigative teams by time zone and availability and tasked with conducting their own formal forensic investigations into an event that occurred on this island. They were then required to have weekly meetings with their supervisors, us, as they worked to create a full formal forensic investigation report. Ultimately this culminated in a series of mock hearings that were held in class, remotely, to determine the guilt or innocence of those accused of wrongdoer-- of wrongdoing during the investigations, and an actual panel of real industry representatives, including CTOs and CEOs of relevant technical organizations, were invited in and they participated as guest judges. In this manner, the immersive experience itself provided not only the training content, as my co-instructor and I filled the role of, you know, supervisors mentoring their direct reports, but also it provided the evaluations, as the formal incident reports the students produced formed the basis of the hearings, and the hearings themselves were graded by the guest judges based on the students' performance. These artifacts provided all of the evaluation needed to determine the students' performance by looking at the quality of the work they produced under real working conditions and not, you know, some artificial, two-hour evaluation during finals week. Josh, does that answer the question from using this in a class setting?

**Josh Hammerstein:** It does. There was a follow-up question though from Jewels here. It says, "Will this class continue to be offered in this manner post-COVID?"

**Rotem Guttman:** Oh, okay. So yes, it's-- it actually-- it worked so well, we've gotten excellent feedback from the students, that we're actually going to continue offering this class as classes resume and as students come back on campus, and we're actually looking at further extending the class, bringing in additional content, and I actually had a conversation today about using these techniques in an undergraduate class as well and possibly even having the, you know, the classes feed into one another. So we might have some combined classroom experiences as well. I think one of the real keys is letting the students feel like they're immersed in a real world, that they're participating in an environment, because getting that suspension of disbelief is so critical to letting them really immerse themselves in the learning.  Are there any other questions?

**Josh Hammerstein:** No, not right now.

**Rotem Guttman:** Okay.  So in that case, I'm going to go to the complete opposite end of the spectrum, going from, you know, students at the start of their careers to cyber operators, you know, the best cyber operators across the entire federal workforce.  So in this case I'm talking about the President's Cup Cybersecurity Competition, and I'll say this is probably the crowning achievement of these techniques thus far, at least for me.  So okay.  Executive Order 13870 gets signed and part of that order creates the President's Cup Cyber Security Competition, and so, you know, they're looking to find and reward the best cybersecurity talent in the entire federal workforce, both individuals and teams.  The Department of Homeland Security gets tasked with this, specifically CISA, and so here in this new competition, you know, it's the first of its kind.  Nobody's ever done anything like this before on this scale, and you're talking, you know, the entire federal workforce being invited to compete in this, and we're trying to find the one best team out of that group.  Now, thankfully CISA was willing to take, I mean, well, a risk and try something new and innovative to accomplish this goal.  So what we created with CISA was what eventually became the finals client, an environment that allowed us to put teams into an immersive environment and test their ability to operate as a team, not just a collection of individuals, and again, going with that thread of motivation being key, let's look at the teaser that was put out there as we invited competitors and spectators to join the event.

<video begins but cuts off>

**Rotem Guttman:** So again, in this experience, we used the best of what we'd learned in a semi-fantastic setting.  Just unreal enough to suspend disbelief but still identical to reality in how all of the technology operates.  In this case, we had to get the participants acquainted with three abstractions.  First, the fake organization they were supposed to be part of, the Disaster Relief Task Force.  Second, the avatar that they would be using to navigate within the game world, their RADs, or remote access droids.  And third, the MOTHs, or multiple object tethering hardware which served as the connection that they'd be using to bridge the gap between the digital world they were navigating and the cyber objects that they were connected to.  So in order to do this, again, we provided in-game briefing materials, both actual physical packets with essentially an instruction manual that they were given, as well as this video that was the first thing that they were introduced to as they accessed the environment.

**Recorded voice**:  Welcome to the disaster relief taskforce, DRTF, application.  A winter superstorm has hit the east coast, damaging important infrastructure.  Due to freezing temperatures and blizzard conditions, people's lives are at risk and we've been authorized to provide any support we can. Using this interface, your team will work with local agencies to mitigate the superstorm's effects and prevent further damage. Your taskforce has been assigned to a city. We have a briefing prepared for you with details regarding the latest operational instructions for our remote access droid, RAD 9000. Your mission tasks can be accessed from the DRTF application, alongside local news coverage, taskforce updates and weather changes. Until conditions improve, your RADs are the only way to access the hardest hit areas. It's up to you to accomplish as many tasks as you can as quickly as possible. Welcome to the disaster relief taskforce orientation. As a new employee, you will need to remember these three easy steps. Step one, telepresence with the RAD. This is a remote access droid or a RAD, the device that you will use to move around locations otherwise out of reach. You will choose a RAD to log into at the beginning of each module. Please note, the RADs are sometimes located in different rooms with different areas they can access. You can exit RADs at any time by pressing escape. Step two, cyber access with a MOTH. To access computing devices in these remote locations, your RADs are equipped with MOTH devices, or multiple object tethering hardware. You may access the console of any device that you or another DRTF team member has deployed an active MOTH to, via the MOTH net, a list of all MOTHs that have been deployed, which can be accessed by pressing M in any module. However, the MOTH net is limited to MOTHs in your current module and cannot access MOTHs in the other modules. Step three, complete your mission. Once a MOTH is deployed, you will be able to access the machine at any time through the MOTH net and execute your missions. Thank you for listening.

**Rotem Guttman:** So we created this amazing simulation of a city getting crippled by a winter superstorm, and we checked the long term forecasts, because the one thing we didn't want to have is, have a real disaster occur at the same time that we're conducting the event. Well, again, Covid happened and the competition was delayed due to Covid. So of course, a week before the actual competition, that big storm hit Texas. So if anything we learned from that, it's don't ever assume anything at all about the weather. But beyond just the weather, each of the challenges we designed for the competition ended up having a real world event happen between when we designed the challenge and when we conducted the competition, from a datacenter suffering an outage while being inaccessible to personnel, to a hospital getting hit with malware. But by creating realistic scenarios, CISA was able to not only capture the participants' attention, but also raise awareness of actual cyber threats in front of the livestream audience. And so this is-- I want to pause here for a second because we did have a question earlier about resources. And so one of the things that we've done is, we've actually created a virtual appliance that packages up all of the infrastructure for this competition that we can make available. Shoot an email, info@sei.cmu.edu. I'll make sure that you get a link for where to download that appliance, but it's a nice turnkey way of being able to deploy all of this and be able to modify it however you need to. So somebody had mentioned making an escape room actually, so here I'm showing the 2020 competition, but actually, the 2019 competition was an escape room. So we had competitors locked in a building that was going to blow up in eight hours, and they had to work through a bunch of cyber challenges in order to escape that room.  And so actually, one of the things that you're seeing here in the video that's playing right now is the competitors actually moving around in that environment, driving their RADs around, accessing different things.  I think we're about to see them moving a van to a different location.  And actually, what wifi networks you can get onto is going to change, depending on what you do there.  So you can really make as immersive of an experience as you'd like there, and when you download the virtual appliance, you have everything that you need in order to start tinkering with it yourself.  Josh, were there any other questions?

**Josh Hammerstein:**  Yeah, we got two questions. One related to this.  Sarah asks, "Can we get access to these challenges to try them out ourselves?"

**Rotem Guttman:**  Yes.  So again, that virtual appliance comes with everything you need in order to kick the tires, as is, for the way that it was crafted, then you can modify it.  But if you just want to try the challenge as stock, run the virtual appliance, connect and go.

**Josh Hammerstein:**  And then we have another question from Anousha. I think this is related to your class.

**Rotem Guttman:**  Okay.

**Josh Hammerstein:**  "How do you gauge performance when offering a course with gamification? Are there multiple ways of trainees/students cracking the case?"

**Rotem Guttman:**  Okay, so yes.  First of all, absolutely.  One of the things that I try to do with all of the training that we craft is, don't prescribe a path to solution. Make sure that at least one path exists.  Have an intended path, sure, but don't require that path to be followed.  And so what you want to make sure that your grading criteria are on achievements, on objectives, not on "have to get there".  And so if your students find an alternate solution, you want to reward that, not penalize that.  So whereas when I was in grad school, I remember there was an exercise that I took that I was very disappointed that we had to secure a network. And one of the things that we did was we picked up that whole network and moved it. We just changed the entire addressing space, and then the day before we were supposed to get evaluated, the TA told me, like, "No, you've got to put all that back, otherwise, you know, everything's going to break and you'll get a zero."  It's like, why?  Whereas so, Josh, do you happen to remember? We had that one team during the President's Cup that solved one of the challenges.  Do you remember how long it took them?

**Josh Hammerstein:** I can't.

**Rotem Guttman:** I remember that they actually solved the challenge in, I think it was like, less than 15 minutes, and it was a challenge that the actual developer of the challenge couldn't solve in less than half an hour. And so you want to reward that kind of performance, and so the metrics that you want to make, you want to make sure that they are aligned to what you're actually asking them to do. So I'll take the example of the class that I developed. I'm asking them to conduct a forensic investigation and then provide a report. Well, the report that they had to create, with actual grading criteria on it, I pulled out those directly out of the federal rules of civil procedure. So that report they created, that would be admissible in court. You could take that to court today and submit it as evidence and it probably wouldn't get excluded by opposing counsel. And so you know, I've asked them to meet this high criteria, provided them all the resources they need in order to be able to do it. But now, how they conduct their investigation, the steps they go through to do that investigation, I'm going to evaluate them by looking at that report that they've created. But the next step of that class was actually, the team's now got assigned and split off, so that for each individual person that got investigated, one team was prosecuting and the other team was defending. And so they were actually reading each other's reports and raising issues with it. "Oh, I don't like the-- the procedure you've followed here, we don’t think is forensically sound," or, you know, "The procedure that you followed there, we weren't able to replicate with the information that you gave." And so now, they're actually helping with the grading themselves without even really realizing it, because they're going through those reports and determining, okay, what are the weaknesses, what are the flaws? Then all of that comes up at the hearing. Well now, one of the learning objectives of that course is their ability to verbally present their findings and defend them. And so at the hearing, they're doing live cross examinations of one another, so that they're actually discussing this. And in the meantime, you know, I'm recording everything, and that gives me all the artefacts I need in order to assess them. No, some of the teams, you know, one of the teams this last semester developed their own custom tool chain for doing a portion of the forensic analysis. Great. There's no way I could have predicted that they would do that, but it sped up their procedures. They documented it well enough to where it was repeatable and they provided the tool chain. Great. Everything that they would need to do. They got extra credit for that, you know. As long as you build your scenario where you inject fantastic elements. Sure, this is a banana republic, but you ensure that the technology is aligned with what you're trying to train. Then anything they do is going to operate the way that it should. I'll give even another example. During the 2019 President's Cup, we had this SCADA system, where the last thing they were going to do to escape was actually mix some volatile chemicals in a tank that would explode, blow a hole in the wall and they'd climb out to get out of the building. And so we had left documentation on there so they could reprogram the SCADA controller, reboot it, and when it would come up, it would pull the new programming, mix the chemicals and go. Well, one of the teams, you know, they weren't able to get that working for one reason or another. What they did is, they actually used a mod bowl [ph?] to send direct messages to that SCADA control and tell it, "just mix the chemicals". Well, we hadn't thought of that, so we hadn't programmed for that. But because what we were evaluating on was the actual state of the tanks, the SCADA control was like, "Okay, I'll mix the chemicals". It went, hit the SCADA simulator that we were using, mixed the chemicals and our grading script, so it was like, oh, chemicals are mixed. Blow the hole in the wall. And so they got out. Everything worked great and they ended up actually winning the President's Cup. And so as long as you make sure, really, the evaluation criteria are what you care about them achieving, then how they go about achieving that, certainly you can give them extra credit for that. Ask them to document it, sure, but don't evaluate based on that as your core grading criteria. Big lesson learned from there. Any other questions, Josh?

**Josh Hammerstein:** Yeah. We've got Yuleni asking, "Are there any resources that are available for creating realistic cybersecurity lab simulations that are similar to SEI cyber leak forward, that college professors can leverage for their classes?"

**Rotem Guttman:** So again, I'm going to point to that virtual appliance, but beyond that, I'll say, I'm always happy to help. Again, info@sei.cmu.edu. You know, say your looking to contact Rotem. They'll route it to me, but I will be more than happy to point you at whatever resources are appropriate for your individual classroom. At its core, the best advice I can give is, have good learning objectives. So for example, with my class, that was the first thing. We spent several days on that. What exactly are the learning objectives that we want to achieve in this course? And then we built the content based on that, so that everything that we're asking the students to do, every challenge they would be confronted with, mapped directly back to one of those learning objectives.

**Josh Hammerstein:** All right. Why don't we go ahead and move on. We've got a couple more questions, but we can hold off on them for now.

**Rotem Guttman:** Okay. So finally, the last group of things I'd like to showcase are some of our more experimental creations that I've developed over the past few years. Now, as I mentioned at the start, we have this huge shortage of skilled cyber professionals in the pipeline. Studies have shown that the vast majority of students decide on a career before high school graduation, yet at the same time, for most high school students, no one's even mentioned the idea of a career in cybersecurity. So how can we spark interest in something that students aren't even familiar with? So to reach a younger audience, we have to simplify these concepts down to a manner that they can understand, and we have to gamify the experience to make it engaging. And we have to integrate with educators to really bring it into the classroom. So that's where Three Envelopes comes in. It's a cybersecurity and risk management boardgame that requires no prior knowledge of programming or networks. It introduces a variety of cybersecurity career options, you know, natively, through the gameplay itself. So let's take a quick look at the game. At its start, each player, or team of players-- because you can play this either individually or in small teams-- they get a company to run.  The example on screen right now is an example of a company in the tech sector, but there's boards for all sorts of businesses.  Entertainment industry, critical infrastructure, you name it.  And so as you see, the board is divided into three zones: operations, business development and IT.  At the top, some helpful text reminds the players of how their business starts the game.  How much money they start with, what their finances look like, et cetera.  And then they also get a player aid board. There's one that matches each business.  And this is designed expressly to lower the cognitive load on the players, as it allows the players to handle all the calculations, all the tracking of numbers, for the game, simply by placing little wooden cubes on the board and moving them around.  So each business has their board that's associated with it, and you'll see, there's a couple of shaded in squares.  That's just the starting positions for the little cubes.  So you can see, every business's security posture is tracked in four areas: technical controls, physical security, policies and procedures and security awareness.  By providing this board to aid in the tracking, we free up the players to focus on the content and the theme of the game, the material that we really want them to absorb.  So as the players play the game, they receive a set of cards.  Each round, they have to choose if they'd like to invest in one of the cards, you know, basically buy that card, or if they'd rather focus on building capital, you know, just focusing on their core business, or heaven forbid, be forced to shut down their operations, basically skip a turn, in order to remediate their networks.  So each turn, the players choose one card from the options that they've been randomly dealt, and the remaining options are passed on to the player next to them. This is a drafting game, essentially, for anybody that's familiar with that type of boardgame. So each card presents a different cybersecurity policy or a piece of equipment, or a type of employee, and each card explains, at a high level, what that policy, equipment or employee does.  The process of choosing cards repeats as the cards go around the table, until only two cards are left.  Of these two, they choose one card and discard the other one, so nobody's forced to pick from, you know, here's your choice of one card.  And this way, the players can strategize about what cards to pick, while influencing which cards to allow their opponents to choose from.  And they get into great arguments here.  There's nothing that's more rewarding for me as an educator than to hear, you know, two seventh graders arguing over the merits of hiring security guards or investing in an intrusion defense, you know, an IDS system.  And so, as they make these choices, they basically build their company. Then at the end of each round, once, you know, they've made those choices, a number of event cards are dealt.  Now each event affects all of the companies at the same time, but how the company's affected by the event is determined by the cards that they've chosen to buy during that round.  So some cards present, you know, certain events or affect the company's overall security-- sorry.  Some cards prevent certain events or affect the company's overall security posture, changing the outcome of the event for that particular company.   So, you know, you might have purchased DDoS protection, and been able to just ignore the threat and cyber extortion that you're seeing on screen here.  But your neighbor might be forced to choose between forking over the ransom or losing some of their profits this round.  And so then the game play repeats in this manner for three rounds. And at the end of the third round, whichever companies have made some actual profit win, but of course, the company that makes the most profit wins the most. Before I move onto the next thing, you had mentioned there were some questions, Josh, before. Do we want to catch up on any of those, or?

**Josh Hammerstein:** Yeah. So one question related to this. Aaron's asking, "Do you have any data on how effective this game is in actually getting students into the pipeline?"

**Rotem Guttman:** So the best I can offer is anecdata, you know. I will say, having run this at several local middle schools, that I know of at least three professionals that are now in the pipeline. One's graduated from Stanford. Two others are currently still in school, but three professionals that got interested in a career in cybersecurity just from playing this game and then the conversations that we had afterwards. And so I can definitely say that it is absolutely motivating in presenting this to students as a career that they can pursue. One of them actually has-- I gave him a copy of the card when he graduated, so he has the career he's gone into, he has the associated card with him that he kept. I'm not cheap. It's a sentimental graduate gift. Were there any other questions?

**Josh Hammerstein:** Yeah, there's one question from Deepak for Three Envelopes. "What instructions or background do you give to the players?"

**Rotem Guttman:** So there's three ways that the game can be played. In its first modality it's just, you know, here's a box with a game. Here, play it, enjoy it. It doesn't need to be given in a classroom setting. They can, you know, just provide it to the kids, just because you want your kids to be aware of these things. Great. I've given it away before. But in the classroom modality, it's actually designed to be administered twice where, in the first time, it's just, here's the game play instructions. Let's play a game. The students love it because they feel like they're getting time off from class. They get to just kind of have an extra recess. Then after they've played the game, that's kind of the introduction without them realizing it. Then there's a module that we do with the students that teaches them very basic risk management concepts. How likely is something to happen? How damaging would it be if it happened? How do we analyze these? And then they actually get given a copy of every card in the deck, every event in the deck, and they're allowed to create a business plan. So you put them in small groups, and then they go through and they say, "Okay, there's three copies of the phishing attack email event, and so it's really likely that we're going to see that, but there's only one copy of the Zero Day Exploit card event happening, so that's less likely. So we're going to--" you know. Then they look at all of the things that they can purchase. How many copies of that are in the deck? How much do they cost to purchase? What's the benefit that we get? What do they actually affect on our security posture, or in events that they can address? And then based on all that, they can calculate out, okay, what are my priorities? What should I pick?  And then once they have the business plan, which is, you know, the thing that they submit that they get graded on-- that's their assignment-- then they get to play the game again in class, but now they have their business plan with them, sitting with them, and so when they're making those choices, they're making informed choices.  Now they're playing a lot more intelligently, and they'll see that in the gameplay, that they'll suddenly be a lot more successful than they were, when they played the game the first time.  And that way, it both reinforces for them, like, hey, doing risk analysis has benefits.  This is something useful to me, not just in this game, but in general.  And then beyond that, it also teaches them how to value these different concepts.  Does that kind of answer the question?

**Josh Hammerstein:**  Yeah, I believe so.

**Rotem Guttman:**  Okay, so in that case, I'll move on.  I see we're getting pretty short on time, so I want to make sure we get through some demos of our initial explorations into virtual and augmented reality.  So what we did is, we connected our cyber simulation capability from our cyber range with this virtual environment, so we can really immerse the training audience in the environment.  Take a look.

**Josh Hammerstein:**  So, Will, we've been getting some reports of strange behavior on this file server.  I already dumped the logs from the firewall and from the gateway router, and I'm seeing a lot of activity from the user subnet.  So can you go poke around over there and see what's going on, and I'll take a look at the file server in the meantime?

**Rotem Guttman:**  Yeah, absolutely.  I'll check it out.

**Josh Hammerstein:**  Thanks.  All right.  Let's head back over.  There's a Coley [ph?] client that's been flashed to user 3 machine.

**Rotem Guttman:**  Oh, okay, show me.

**Josh Hammerstein:**  Yeah.  Take a look at user three.

**Rotem Guttman:**  This one?  Ooh, let's see what they've been up to.  Ooh, that's  not good.  Okay, we're definitely going to have to take a closer look at this. Man, today sucked at work.  Well, get something to eat.  Mm, pizza.  Get something to drink.  And now just sit down, relax and enjoy the evening.  So what was I doing here?  So, you know, that's the content that I had to share.  I'm going to stick around and answer any questions that are here, but I just wanted to say that I hope you found the talk useful and if you have any questions, you want more information, you want input on  how to craft these experiences for your individual classroom, please contact me.  Send an email to info@sei.cmu.edu and ask for Rotem.

And I promise every-- you know, this is my passion-- every one of you that needs help with this, I'll do my best to help you individually and help you craft something for your individual classroom. Because beyond anything else that I've learned in the last decade of doing this, it's that having a customized experience, something that talks to your individual audience, will pay dividends far and beyond what you're going to get from some generalized solution that might not really match what your students are looking for. So with that, Josh, are there any remaining questions?

**Josh Hammerstein:** Yeah, we've got a few. We got one that was asked earlier from Deepak, that actually I can answer myself. But the question is, "Any recommendation for a set of challenges that students can individually do on their own with answers and hints, if they cannot?"

**Rotem Guttman:** Oh yeah, absolutely.

**Josh Hammerstein:** Yeah. So the President's Cup, as Rotem mentioned, 2019 challenges, a number of them are open source and on GitHub, so if you just do a simple Google search and just search President's Cup 2019--

**Rotem Guttman:** Oh, Josh, actually, hold on. You reminded me. I have a slide for that.

**Josh Hammerstein:** Even better.

**Rotem Guttman:** You teed me up well there. So whoever asked that question, thank you.

**Josh Hammerstein:** So do you want to explain what that is?

**Rotem Guttman:** Yeah, so that's a QR code. You can scan that with your phone right now or copy the link below. That should link you to our workforce development page. We have GitHub repositories for not just the challenges but a wide variety of tools that our team has created for creating these cyber infrastructure, these cyber environments for automating user behaviors, all sorts of stuff, beyond just what I've talked about today. There's a lot of great tools there, to kind of dig into.

**Josh Hammerstein:** Just to add to that. I don't know if the President's Cup, if the link to those challenges are on there. If they're not, you can just simply go to Google and Google President's Cup 2019 GitHub, and the challenges will show up. We've got one more question here from a couple of folks. This is regarding, I believe, your Three Envelopes game.

**Rotem Guttman:** Okay.

**Josh Hammerstein:** "How can we get access to this game?"

**Rotem Guttman:** Again, your best bet-- it's not publicly available yet. That's dealing with printers and publishers and so forth. But if you shoot me an email, I can work with you to get it in your hands. I would love to get more data on how well it runs, so I'm more than happy to give it out for play tests. All I ask is, you know, give feedback on how it's working for you.

**Josh Hammerstein:** With that, I don't see any other questions.

**Rotem Guttman:** All right, well thank you. I hope everybody has enjoyed this as much as I have. I love being able to connect with the community so again, please reach out.

**Shane McGraw:** Rotem and Josh, great discussion today. Thank you both for sharing your expertise.

**Rotem Guttman:** Thank you.

**Josh Hammerstein:** Thanks.

**Shane McGraw:** And again, we'd like to thank you all for attending today. Upon exiting, please hit the like button below the video window and share the archive if you found value. Also, you can subscribe to the SEI YouTube channel by clicking on the SEI seal in the lower right corner of the video window. Lastly, join us for our next livestream, which will be May 19th, and our topic will be software supply chain concerns for dev sec op programs. Registration information will be available soon and emailed out. Again, any questions from today for Rotem or Josh, you can send those to info@sei.cmu.edu. Thanks, everyone. Have a great day.

**DM21-0425**