Interested in learning more about security?

SANS Institute InfoSec Reading Room

Practical Cyber Security Training Techniques for New IT Support Employees

Purely technical skills can be readily acquired via classroom instruction, books, certifications and on-the-job training. Technical skill alone, however, is of limited utility when attempting to detect, assess and respond to live threats to an organization's production systems. IT support personnel - from the warehouse to the server room - need to be trained on how to perceive threats as they manifest. That requires hands-on, mentored, and nuanced instruction. This paper presents a comprehensive methodology derive...

PRACTICAL CYBER AND PHYSICAL SECURITY TRAINING EXERCISES FOR IT SUPPORT EMPLOYEES

GIAC GSLC Gold Certification

Author: Keil Hubert, keil.hubert@gmail.com
Advisor: David Shinberg

Accepted: July 2, 2013

Abstract

Purely technical skills can be readily acquired via classroom instruction, books, certifications and on-the-job training. Technical skill alone, however, is of limited utility when attempting to detect, assess and respond to live threats to an organization's production systems. IT support personnel – from the warehouse to the server room – need to be trained on how to perceive threats as they manifest. That requires hands-on, mentored, and nuanced instruction. This paper presents a comprehensive methodology derived from a decade of turning non-technical military recruits into cyber security professionals. It focuses on the creation, application and refinement of instructor-led, immersive cyber threat management scenarios coupled with guided feedback.

1. Introduction

It's ludicrous to expect a brand new, fresh faced employee to be fully productive on his or her first day in the office. Between learning where their desk is (or, perhaps, where the latrines are) and establishing their network account, the new employee is of limited practical utility in the first few days in the field. It's simple organizational dynamics: all new employees must be oriented to the workplace, be given the tools required to perform their intended task(s), and be trained in how the execution of each task is conducted differently from how it's performed in abstract theory. The network administrator must be shown the local LDAP customizations. The infrastructure tech must be shown where the communications closets are. The helpdesk tech must arrange to have remote access tools installed on her new PC. Without proper orientation and outfitting, the new employee is likely to bumble through their first jobs – making mistakes as they inadvertently violate organizational norms – thereby learning about the local version of reality by trial and error. This phenomenon is fairly well understood. It's why many organizations have formal on-boarding processes in order to ensure that the right "tribal knowledge" elements are taught early on.

For the IT department, there is an added wrinkle to this new employee orientation process: the need to teach the new hires what "normal" looks like within the IT services domain. After impressing upon new employees why security is important to the company, the first (and most critical) step in mitigating cyber security threats is to recognize when one is happening. For that to happen, all available team members must be able to act as sensors, ready to identify and sound the alarm about an emerging threat while there's still a chance to contain it. For *that* to happen, we have to teach them the art of differentiating between steady-state operations and aberrations. (Mitnick, 2002)

The most effective way to teach always-on cyber security scanning is to train your people through hands-on, fully immersive, practical exercises that include active coaching from an experienced team member. This paper presents several affordable, reasonable, and practical exercises that you can use in your organization today to accomplish this objective.

Keil Hubert, keil.hubert@gmail.com

2. Recognizing Meaningful Deviations from the Norm

2.1. Concept

For the sake of this paper, "normal" is a status awarded to a person, place, or process that the responsible community agrees when said element is operating in an unremarkable and/or desirable state. For example, Business X decides that its server room should be kept at a constant 20 degrees C (68 degrees F). So long as the server room is at (or about) that temperature, the system administrators and facilities techs agree that the room is in its desired "normal" state.

For the record, "normal" in this context does not necessarily reflect an objective, independent value; for our example server room, Business X decided on 20 C – whether they decided that arbitrarily or scientifically is largely irrelevant. Meanwhile, Business Y across the street might decide to keep their server room at 18 C while Business Z down the road is comfortable with 25 C. So long as the "normal" state meets the needs of the organization, it's fine for our purposes.

Deviations from "normal" reflect the difference from the desired state. All systems will likely deviate to some degree as a result of internal factors, external factors, or both. For our server room, the temperature inside can change due to the corridor door opening. So long as the control systems return the room to its "normal" temperature state, all is well.

The deviations that we're most interested in noticing are those that reflect an unnatural departure from the norm. If our server room temperature rose by 5 degrees and failed to return to its normal state, that might indicate an innocuous cause (like a bad sensor), a dangerous condition that doesn't reflect an active threat (like a failing air conditioner), or a threat (like Bob the Hacker propping the server room door open). The first two conditions might require a call to maintenance; the third involves a call to security.

We want all of our employees to notice all *meaningful* deviations so that the right expert will then investigate them in a timely manner to ascertain whether or not there's an active threat. In order to determine what constitutes a meaningful deviation, we first have to teach our new hires how to tell normal and not-normal apart.

Keil Hubert, keil.hubert@gmail.com

2.2. Example – Accidental Internal Denial of Service Attack

Picture a military garrison in the USA on a Friday morning. A unit was starting an early morning exercise. A half hour before the duty day officially started, the IT manager received a call from one of the techs: she had logged in to her PC, but couldn't reach any network resources. Troubleshooting showed that the PC had been assigned a non-routable IP address (192.168.X.X) that didn't match the organization's DHCP scheme. The help-desk was put on alert to look for more examples of the problem. Sure enough, within five minutes the helpdesk received seven more calls with identical manifestation.

The culprit was fairly obvious: there was a rogue DHCP server on the network that was dutifully handing out IP addresses from its own default range. As soon as the garrison's soldiers arrived at their desks, they would log into their PCs, pick up a non-routable IP and fail to authenticate against the organization's domain controllers.

The evidence was simple: they knew the base's normal IP scheme, and knew that there had been no changes to the DHCP service or production routers the night before. There were PCs in the helpdesk operating normally – ones that had been logged into two hours before the first trouble call came in. Therefore, the rogue DHCP server had probably been added to the production network between the time the IT staff came to work and the time that the affected customers did, since the affected PCs were all booting (as opposed to unlocking). The only change to the garrison's normal operational state was the execution of the local exercise – an event where units changed buildings in order to simulate deploying to a "new" base. The probability, then, was that one of the units playing in the exercise was the cause. That narrowed the search zone down by about two-thirds, as not everyone was participating in the exercise.

A tech found a consumer-grade home broadband router in the third office that he visited. Once the misbehaving device was disconnected, the helpdesk used the paging system to order everyone to reboot. The owner of the device had not intended to cause trouble; his team "deployed" with an Ethernet hub. When his old one broke, he went to the Base Exchange to replace it. Not knowing the difference between a hub, a switch and a router, he bought the device that looked the most like his old one: a blue-colored box with several ports on it. Whoops …

Keil Hubert, keil.hubert@gmail.com

2.3. Why This Matters

The first manifestation of the problem in the above example was noticed by a junior IT support employee. The tech recognized that what he was seeing was not only abnormal, but that it warranted escalation and investigation. The team formed initial theories based on how far the problem diverged from their normal state. This is *exactly* the kind of response that we want from IT employees – and, eventually, from our users.

The key to locating the source of the problem was the techs' understanding of what "normal" looked like in the organization. They knew what a normal cubicle farm should look like when standard equipment was plugged in and working. That's why it only took a cursory sweep of the users' work areas for a tech to spot a single, paperback-sized device that was visibly out of place.

The employees had been trained by the principles and techniques presented in this paper, in addition to all of their formal training, academic qualifications, and on-the-job experience.

3. Training Methodology Principles

The methodology presented here is derived from many years of teaching practical skills to military men and women. Many of the techniques that I learned from grizzled old sergeants are as true for civilians as they are for soldiers and just as true for techies as they are for riflemen. Soldiers are people, and people are largely consistent in the sense that we are all easily bored, easily confused by vague language, and often resent being lectured when we don't first understand why the content is important. Replace the word "soldier" with the more inclusive word "people" and the meaning still holds true, as in this quote:

"Whenever individual training programs fail to get the job done, it's usually for the same reasons. They lack variety; do not challenge [people] physically or mentally; are poorly planned, prepared and presented; or do not put [people] in a scenario that reinforces the skill. [People] need to understand and experience the purpose for their training." (Pendry, 1999)

Keil Hubert, keil.hubert@gmail.com

This approach is built on the principles that training must be interactive, guided, meaningful, and directly relevant to the employee's operational environment. Abstract theory is fine for teaching general principles; proficiency requires orienting a tech to the actual places they inhabit. Make your instruction positive, challenging, and (most of all) grounded in real places, real examples, and real threat indicators.

Optimal instruction incorporates successful attacks or incidents from your organization's history. Second best is instruction based upon incidents that happened recently, preferably to a similar organization. Least effective are theoretical or fantastic threats; there's little point in preparing for a volcano eruption in Kansas. Lessons built around attacks against equipment or facilities that you don't have are not only likely to be valueless – they are probably going to be counter-productive as well.

3.1. Training By Doing

Inculcation is the process of the teaching of or reinforcing of a skill by actually performing the skill several times in the operational environment where the skill is intended to be applied. It's understanding that's instilled through action.

Some employees can learn a lot by reading about a topic. Other employees extract a great deal of information from instructor-led classroom training. A small number of employees actually learn from computer-based training modules. In all three cases, these delivery methods are best suited for teaching dry, detached theory: how things work in the sterile laboratory envisioned by the content creator. When the theory meets gritty reality, theory often comes up short due to unforeseen or un-factored complicating factor.

There are exceptions, to be sure. An exhaustive written reference can cover a staggering range of situations. A talented instructor can read students, evaluate their understanding and shift approaches to better convey the material to each student.

That said, the inculcation principle flips the standard tech training model on its head. Instead of taking the employee *out* of their environment to go learn the skill in order to try and bring it back to the office, our intent is to teach a skill *in* the actual space and context where the skill will be used, taking advantage of all the environmental factors that might apply. As an added bonus, teaching a skill in the actual office is often far cheaper than shipping an employee off to a conference.

Keil Hubert, keil.hubert@gmail.com

Additionally, the focus on teaching the skill in the operational environment allows you to re-teach the skill multiple times. Each iteration of the lesson reinforces the employee's understanding of what the actual environment looks like in its "normal" state. *That* element, you teach, is a deviation from *all of this*. The constant reinforcement of what constitutes "normal" is as much a value to the employee as is learning how to recognize departures from the norm.

This approach also has the advantage of ferreting out false-positives. When you immerse the employee in the operational environment and they "alert" to an indicator that is not an actual problem, you can reset the employee's understanding on the spot.

3.2. Coaching – Training By Reorienting

Recalibration. If immersion is the engine driving this training program, coaching plays the dual roles of steering and transmission. If someone is not (yet) competent in a new skill, dropping them into it blind to fumble around and find their way is *tremendously* useful for familiarization … but not for actual proficiency. That is where the trainer has to share in the experience: to teach what's important (and what's not) in the exercise, to clear up misconceptions, and to reset the employee's understanding of priorities.

When you build your scenario, select the venue, define the objectives, set the stage and finally drop in the student. You have to be near enough to the student to perceive and evaluate their technique, and to notice when they lost the plot. This is something the instructor must do himself/herself; it cannot truly be delegated to anyone unless they co-developed the scenario and know exactly what's in your head. Other observers' feedback is critically important (see section 3.3) but cannot replace your understanding of the solution that you wished to teach.

Active coaching is analogous to training a new pilot to fly. The instructor pilot knows everything that is expected and knows what is likely to happen. The student takes on as much responsibility for driving the scenario as they're allowed. While the student "flies" (within the limits of their ability), the instructor carefully monitors the student's progress, introducing complications, variations, and questions designed to increase the student's understanding of what they are experiencing.

Keil Hubert, keil.hubert@gmail.com

The intent is to perceive the environment as it is, and then assess how the student perceives it. Determine if they are identifying and evaluating the indicators the way that they were intended. For example, if the indicator that you want them to see is a warning light on the front of a racked server, position yourself to evaluate whether the warning light is actually in their field of view. Are they looking at it? Do they actually *see* it? If they do, does it trigger a response? Is their response a correct response?

As the event progresses, you interject as-needed to call out the elements that you want understood, and then explain why they are important. Teach the **why** along with the easier **what**. Continue until the student has the breakthrough and grasps the **why**, and then applies is to pursue a reasonable solution.

3.3. After-Action Reviews – Training By Deconstructing

At the end of most computer-based training modules that I have experienced, the last screen or slide is a recap of the content that was (supposedly) covered during the lesson. That never made sense … if you learned the content, being told that you had learned it was valueless. If you had not learned the content, being told that you *had* was often infuriating. Most of the post-course, human-led critiques that I have attended have been similar, because they never actually addressed the efficacy of the training.

The military has a habit of conducting post-event analysis somewhat differently. A person's focus is greatly enhanced when mistakes can get them killed or maimed. These are called "After Action Reviews" (AAR). The idea is to end every training event with a no-holds-barred, free-form discussion about how and why the exercise was built, how the participants did, what they might have done differently, and how the problem under review might actually manifest.

"In conducting a critique, your main job is to do everything possible to get the [people] involved. … In covering each of the points that are to be emphasized, do not continually repeat 'You should have done this,' or 'You should have done that.' It is far better to pose questions that involve the [people]. 'When you arrived … what action was taken?' 'What do you think of that now …?' (Collins, 1978)

General Collins' admonition to young officers is exactly where we need to be with cyber security training. The idea is to take the event apart, moment by moment, and determine what the student perceived, believed, and acted upon. It is not enough for the student to come to the right technical solution by the end of the scenario; they could very well have come to it randomly, or via deeply flawed thinking. The deconstruction step is where you validate whether they actually *understood* what they perceived and whether their logic was sound. If anything is not properly aligned, the time to correct it is immediately – on the spot – while everything is still fresh.

The observers have just as much a role to play in the review. Simply by the virtue of occupying a different physical space, an observer can sometimes perceive something that you missed. Their experience might grant them insight that you lack. Most important, though, are their questions – they may be able to tease out critical concepts – themselves.

"By a series of questions and probing, draw the [people] who were involved in the action into the discussion. They all have ideas. More important, eliciting their contributions is essential to the learning process. Once they begin to debate with one another you will know you are conducting a successful critique." (Collins, 1978)

The AAR is every bit an inculcating event as the training scenario itself. By encouraging all participants to speak freely, without fear of retribution and without regard to rank/authority/position, the act of talking frankly about the exercise subtly trains the employee to be bold, frank, and professional in their interaction with their teammates. This is the kind of productive dialogue that you want employees to internalize as a standard operating procedure: when an employee encounters a real problem on the job, you don't want them to be intimidated into silence, inaction, or half-hearted activity out of anxiety over how their warning or activity might be received. Speaking confidently, with the understanding that they will be heard out should be thoroughly imprinted in every team member.

Finally, there's a bonus to conducting a review about actual security incidents as well; you can capture lessons-learned to build new scenarios. Re-create elements of the actual incident and teach your employees which early indicators they could have seen.

Keil Hubert, keil.hubert@gmail.com

3.4. Unannounced Exercises – Training Under Pressure

If you ever interview with me for one of my positions, expect to have an unannounced exercise sprung on you during the discussion. (Hubert, 2012) "You cannot know who a man really is until you put him under stress." I cannot cite who taught me this aphorism, but it has influenced the way I hire people for many years. In a job interview, everyone involved is expected to put up a shiny façade – an idealized caricature of oneself, meant to impress. The problem is that the person that impresses you at the interview often is not the same person who comes to work for you after the hire. That is why I like to jolt applicants; to surprise them such that we can see behind their façade and learn a bit about who they really are.

A practical exercise can be made into a more stressful event by placing arbitrary constraints on it: giving the student only minutes to isolate and solve the problem. Or have the reporting actor play the role of an irrationally angry executive. Drop the lights. Turn off the air conditioning. Added difficulty makes for a more memorable – and more revealing – training event.

The same principle holds true for "stealthed" training. The same scenarios that you walk through at a measured pace with a group, can be introduced (usually with actors) under the guise of an actual trouble call or customer encounter without anyone being aware that training is occurring. Surprise injects also help to mitigate the Hawthorne Effect wherein people may change their behavior when they know they're being evaluated. (Hoopes, 2003)

Unannounced training tends to fall under the same approach as penetration testing: select an objective (e.g., "will my staff recognize a spear phishing attack?"), train an actor in what keywords to convey (e.g., "I can't open this attachment that I received from the CEO"), then monitor the scenario from *both* ends of the encounter (i.e., observe the actor, and arrange to have another observer surreptitiously monitor responder). End the encounter when the objective has been met or has clearly failed, then provide useful feedback for the employee immediately – with the actor participating in the discussion.

Use stealthed exercises sparingly; just enough to test the waters. You do not want to desensitize your responders by "crying wolf." Pressure is good; resentment is not.

Keil Hubert, keil.hubert@gmail.com

3.5. Repeat Exercises – Training Through Repetition

The exercises listed in this paper aren't meant to be one-time events. Run each exercise many times. Every time that you run a given exercise, be sure to change the conditions, timing, details and approach to ensure that your employees are *constantly* challenged to reconsider their assumptions and biases.

4. Practical Training Exercises

Specific training scenarios can be broken down by work location, but that is an arbitrary division. Just as cyber threats can strike anywhere in your global enterprise at any time, your employees have to be able to contend with whatever happens, whenever and wherever it happens. That said, you have to start somewhere. In the interests of minimizing costs and maximizing participation, I prefer to begin inside the IT plant, then spiral out onto the support work centers, and finish outside the physical facility.

That's my approach; you can attack your situation based on your organization's and teams' unique circumstances. My recommendation is that you orient your newest employees to the most critical locations (or functions) in your organization first, and then move down the priority scale as best you can.

4.1. The Server Room

Whether your servers reside under the sysadmin's desk or across multiple floors of a skyscraper, the location of the physical servers is both an extremely tempting target for an aggressor, and a potential treasure trove of indicators for your IT team. The exercises that follow were developed to work in a small to medium sized company where the majority of processors and storage were housed in a discrete physical location, usually with its own environmental and security arrangements. Your mileage may vary; adjust as needed to suit your unique environment.

4.1.1. HVAC failure

Server rooms have to be kept cold. Part of environmental normalcy is being able to feel what the temperature (and, sometimes, the humidity) of the server room should be. Get the facilities management team to deliberately raise the temperature just high enough (say, +5 degrees) to register, but not high enough to damage the equipment. Perform a

walk-through with the employee. Do they notice the temperature (and/or humidity) differential? Do they understand the ramifications of a climbing room temperature? Do they check the thermostat? Do they know where to find or *how* to read the thermostat? Do they call the right department to report the error? Do they check the room's vents and exit doors for physical security breaches? Can they articulate a recovery plan (e.g., controlled shutdown, activating cooling carts)?

4.1.2. Alert lights or sounds

Many dedicated servers have alert capabilities built into them. Some have LED lights on their front façade. Some have LCD panels that can scroll useful text and some devices just shriek. Storage devices and large power backup units can do much the same. The intent is to set one object in the room into an alert condition, and then see if the employee notices it during the walk through. Seeing the alarm (or hearing it) is the critical first step. Once discovered, do they recognize it as a problem? Do they assess the affected equipment – front *and* back? Do they call the right operator to report the error? Can they find the maintenance tag or identifying data needed to convey which piece of kit is affected? Can they devise a fix action that will not cause more harm than it solves?

4.1.3. Unauthorized patch

This is a cheap and easy visual challenge. Get a reasonably long patch cable. Connect one end into the back of a production device (on an unused Ethernet port) and run the other end away from the production racks to a spot where an attacker might have connected a laptop. If you maintain strict cable management standards, complete with color specifications, tie wraps, and ladder racks, this kind of variance will stand out. Conversely, if your server room looks like a snarl of random cables, you might have to put some extra effort into creating a situation that someone will actually notice. The key is to make it appear that someone directly accessed something that they should not have. Walk the employee through the server room. Do they spot the out-of-place cable? Does it occur to them that it should not be there? Do they sound the alarm? Do they identify which asset the rogue cable is plugged in to? Do they alert security to seal the complex? Do they methodically search the room for other physical evidence? Do they search the sever room to see if the intruder is *still physically present*?

Keil Hubert, keil.hubert@gmail.com

4.1.4. Violated server cabinet

This is similar to the patch exercise, but should be a bit more blatant. If you keep your server cabinets closed (or closed and locked!), have one standing wide open. Pull a server that's mounted on rails halfway out of the cabinet. Walk the employee through the server room. The same questions that apply to the patch exercise apply here, with the following additions: Do they articulate that fingerprints can be lifted from the surfaces? Do they photograph the scene *in situ*?

Variations of this exercise can be done by pulling hard drive modules fully or partially out of a server or storage device. A drive or two sitting on the floor in front of a cabinet should be extremely suspicious. Another variation involves plugging an external hard drive into the cabinet with a long FireWire or USB cable.

4.1.5. Violated raised floor or drop ceiling

This is another visual check. For the floor version, partially lift a section of raised floor near the server racks or cable management area. I prefer to remove it from the grid, and then lay it over the opening at a 50-60 degree angle so that it is not immediately obvious. To increase the difficulty factor, remove a square in an area that is not directly visible from the places where techs normally congregate. Add some snipped Ethernet cable ends or severed cable ties near the hole for good measure. When the employee walks through, do they notice the breach? Do they look inside to see what might have happened under the opening? Do they search the surrounding area for other disturbances?

The ceiling variation is easier (and safer!) to pull off, but is less likely to be noticed; people rarely look up. Just nudge a ceiling tile out of place – preferably exposing half of the grid square. For added effect, place a ladder nearby. It does not have to be set up or necessarily near the breach. The same questions tend to apply to the ceiling breach as they do to the floor breach.

4.1.6. Evidence of habitation

This exercise is extremely difficult to pull off if your implementation of a "server room" is an office that people regularly occupy; this exercise is designed to be carried out in a restricted area, preferably one where people enter only when necessary and stay only long enough to accomplish a specific task.

Keil Hubert, keil.hubert@gmail.com

The idea is to leave one or more items that should not be present out in plain view. Great props are a briefcase, a beverage container, or even a cigarette (bonus points if it is still lit when the walk through happens). See if your employee notices each out-of-place item and works out what its presence could mean. What works best depends on your environment; if you forbid all food and/or drinks in the space, a half-consumed latte on the floor beside a highly-sensitive server rack should trigger suspicion.

If, on the other hand, your company allows people to take anything they like into your server room, then you'll have to get creative when it comes to objects that should appear "out of place." Try placing a digital camera near the servers after you've taken close-up photos of the cables or shots of the KVM monitor. Or leave a notepad on a table, open to a page where you've hand-written sensitive data (like server names, user IDs, or your IP scheme). These clues suggest that someone was in the server room gathering intelligence on your equipment.

Questions are mostly the same for other breaches. Do they notice? What does it mean? An exceptional student will cleverly figure out a way to check if the food or beverage is still hot or cold without degrading any fingerprint evidence on the container!

4.2. The Communications Closet

In companies that occupy more than one story of a building, physical networking components collapse back to a single location on each floor. If the server room is on the 5th floor, the 6th floor will have a closet or small office that hosts all the network switches, public address amplifiers, cabling punch-downs, patch panels and so on to serve the users on that floor. These spaces are usually un-staffed and may be unmonitored; the server room gets the attention while the cable plant is considered out-of-sight, out-of-mind. For an attacker, this makes the communications (comms) closets highly attractive. The IT staff should know where they all are and what they look like during normal operations.

4.2.1. Server Room Indicators

All of the exercises that you would hold in the server room may also apply in a comms closet, especially the Unauthorized Patch and Evidence of Habitation exercises. Given the relatively smaller size of a comms closet over a full-blown data center, your indicators (e.g., an out-of-place patch cable hanging free from a racked Ethernet switch)

might be more readily apparent. The same questions apply: What do you see? Is it out of place? What could it mean? Is a threat is indicated, what should the immediate response be? What other indicators might be present to prove or disprove your assessment? How long ago did the violation occur? What might the bad guy have been after in there?

4.2.2. Evidence of Vermin

Not all threats to the enterprise come from humans. Buildings attract vermin. Rats love to chew on cables, but they're often not caught in the act. Employees who are accustomed to working in offices rather than in crawl spaces and up in the plenum may have difficulty learning this threat. These are also slightly tricky exercises to pull off; you do not want to use stimulants that will actually *attract* real vermin. Use benign liquids like highlighter ink on "discarded" paper to simulate rodent urine on the floor of a closet. Heat the clue to discolor both ink and paper. Piles of small charcoal bits can simulate rodent feces. To show evidence of a "chewed on" cable, worry the cable's plastic sheathing crudely with a stripper or a set of pliers. Use non-production cables, to be safe.

Ask questions that are both simple and nuanced. Does the employee notice the indicator? Do they recognize what it represents? What mitigation measures do they advocate? Thinking more broadly, can they extrapolate the problem's manifestation to areas outside of the comms closet? That is, if the evidence suggests that rodents have penetrated the closet, can they articulate how and where the vermin might be attacking infrastructure in the ceiling, between floors, etc.? Can they work out how the cable plant might be a "rodent expressway" between floors?

There's an additional element to watch for with this kind of exercise: some people will get squeamish at the thought of coming into contact with critters. Some are repulsed by insects, others by rodents. If an employee recoils in disgust at the input, file that away for later – the squeamish employee might be the wrong choice to dispatch to contain such a situation when it manifests for real.

4.2.3. Storage Surprises

There has been an emerging trend in government construction to reduce the amount of dedicated "storage" spaces in buildings. (AFMAN 32-1084, 2012). According to our organization's senior civil engineer, this change in government policy reflects a

trend occurring in private sector construction. The guiding concept is that people and businesses accumulate stuff; with fewer storage spaces available, people will try to store things wherever they feel they can get away with it. Comms closets are ideal hideaways in many offices, since they're locked rooms that people do not frequent. In many organizations, comms closets aren't supposed to be used for anything other than IT equipment. Therefore the discovery that someone is using one of your closets to sequester their boxes of copier paper indicates that you may have a physical security problem – how did a non-IT person gain access to an IT-restricted space?

This is a simple exercise to run, *if* your organization mandates that comms closets are to be kept sacrosanct. Put a few objects just inside the door. These should be actual, realistic products that are common to the work center(s) located right outside the closet. Reams of copier paper, stacks of toner cartridges, and janitorial supplies all make for logical and innocuous plants. Does your employee notice that the object(s)? Do they understand that they should not be there? Do they make the leap that the closet's security has been compromised? Can they figure out where the offending material might have originated? What do they *do* with it – leave it? Chuck it in the hall? Confiscate it?

4.3. The Cubicle Farm

The cubicle farm is often where the actual production work gets done, day in and day out. Most every business has some variation of the administrative bay. Most have cubicles, some do not. What makes these spaces critically important is that *this is where the users are*. That fact cannot be overstated. If you are going to suffer an insider threat event (e.g., a data theft, a network compromise, etc.), it is going to happen where the insider lives. That is why IT support personnel must get accustomed to the areas where employees work and live. They need to learn how people keep their workspaces and perform their tasks so that they can recognize when something is out of place.

For organizations that perform their own misconduct investigations (especially, the forensic analysis of digital evidence), understanding *how* people work is often the key to finding the evidence. For example, based on where a user sits, where would they tend to place flash drives, external hard drives, optical discs, paper files, etc.? This can be critical when defining the scope of the area under investigation. (Casey: 2006)

For organizations that do not conduct internal investigations, this is still a critical space to train in. Everyone in the IT department is a potential resource for the rest of the company. When an angry user has a problem and they meet a member of IT, they often want help on the spot, even if the person that they collar has nothing to do with the team responsible for the problem. All support employees need to learn how, where, when, and why the company's workers do their jobs. It makes troubleshooting easier, and it makes it easier to recognize when something is out of place.

4.3.1. Missing Components

In the server room and the comms closet, we focused heavily on learning to perceive indicators that were actually there (e.g., warning lights, strange cables). In the common workspace, it is just as important to notice what is supposed to be there and is not. A missing component can suggest both benign actions (e.g., a rearranged workspace) and hostile action (e.g., stolen PCs). The key is to learn how to spot the negative spaces where a physical object recently sat. If you're a fan of TV forensics thrillers, you may be more familiar with the term "voids."

The way to start this exercise is to orient the student to a standard employee work-space (assuming you have a typical equipment build). For example, if every employee is issued a desktop, a monitor, a keyboard, a mouse, and a desk telephone, go through with the employees how these are set up. How much space do they take up? How far away can the PC sit from the monitor and input devices? If you have IT employees who routinely install PCs for employees, learn what their stylistic preferences are (e.g., do they always place the PC to the left of the monitor? Do they run the video cable through the access port in the desk?). Once you know what a "normal" workspace looks like, challenge your employees to figure out what a violated or dysfunctional workspace might look like.

Easy exercises do not take much effort: remove a PC entirely while leaving the monitor, keyboard and mouse hooked up. Does the employee notice that a PC component is missing? Do they know where to look first to validate that all the components are present? Make the exercise more difficult by leaving the components in place, but disconnect one or more of the cables. Does the employee crawl under the desk in order to validate that everything is actually plugged in correctly?

Keil Hubert, keil.hubert@gmail.com

In more advanced versions of the exercise, remove a peripheral component – external hard drives work best for this – while leaving the power components and data cables in place. When the employee evaluates the workspace, do they recognize that a power cable and Serial/Parallel/USB/FireWire/Thunderbolt cable sitting free on an empty patch of desk represents a missing data storage element?

These exercises can become diabolical if you remove tiny or obscure objects. The intent is not to confound your student, however; it is to recognize what is supposed to be present. That is why it's critical to remove *actual* objects from *actual* workspaces.

In all variations of the exercise, the questions are essentially the same. Do they notice the loss? Do they think to identify the owner of the space to ask what happened? Do they alert the right office about a potential theft of breach? Do they (if germane to your environment) think to seal the area or search through bags/briefcases/boxes?

4.3.2. Rogue Components

The last section was about things that should be present not being there; this is exactly the opposite problem. Even when cyber criminals and spies are removed from the equation, workers can cause network integrity breaches via unauthorized modifications to the workplace. People are creative; when they believe that they have a problem, they try out solutions – often without realizing that their actions are violating a policy or have exposed the company to risk. The key to this kind of exercise is to teach what a normal workspace looks like, then add something that should not be there. See if your people notice, and if they understand what kind of threat is represented.

Start with common objects. Most people carry smart phones, and phones run low on battery power at the most annoying times. If a user has a PC with a free USB port and a USB charging cable, you can guarantee that one user will connect their phone to their PC. If this is disallowed by company security policy, there is always one employee who does not grasp the threat – or just does not feel that the rules apply to them. Therefore, place a phone on a desk where a user would casually set it down and connect it.

External hard drives are another easy indicator. When plugged into a port on the back of a desktop PC (especially if the cabling is well-managed), it suggests that the

offender leaves the drive in place over time so that the front ports are left free for temporary connections. Conversely, if a drive is found plugged into the front panel, it suggests a recent, temporary connection. If these devices aren't supposed to be used in the workplace, all drives should stand out. If external drives *are* allowed, use an obviously personal drive labeled with a name or decorated with kids' decals. In some high security processing areas, the mere presence of a storage device sitting disconnected on a desk might be threat indicator. The exercise can also be done with USB flash drives.

Switches, routers and Wi-Fi base stations are common unauthorized components in a cubicle farm. When there are not enough ports in the furniture, some enterprising soul will bring a cheap device in from home to create more ports on the fly Place these in inconspicuous areas, like under desk surfaces, for a more challenging exercise.

In all of these cases, the objective is to determine if the employee recognizes that something is amiss. Do they respond to the object, or ignore it? Once identified, can they articulate the type of threat that it represents? Do they know the organization's process for securing the offending object (e.g., should it be left in place? Removed immediately)? Can they articulate how the device might be used to commit wrongdoing? Does the presence of the device suggest another rogue element elsewhere in the facility?

4.3.3. Rogue Networks

This is an extremely useful variant on the Rogue Component scenario. If a user (or adversary) has extended the wired network by plugging a Wi-Fi base station into a physical port, there may be evidence of it in the form of a new network ID appearing that wireless devices can select, or look for the manufacturer component of the MAC address with a script that queries the CAM table. You do not have to actually connect a rogue device to your network to run this exercise; many base stations can be set up to broadcast a network ID regardless of whether they have a working upstream connection. Place a base station somewhere in the office, then task the employee to help a user connect a PC to a legitimate wireless network. Do they notice that there is a strange network available? Do they work out what that means? Can they hunt down the offending base station and secure it?

This exercise also lends itself to cellular base stations, like Mi-Fi hot spots. Set one on a user's desk or on top of a cubicle run, turn it on, and see if your employee can discover and contain the unauthorized device. In advanced versions of the exercise, place a Mi-Fi device in a semi-public area, like the building's lobby, in a conference room or in a shared break area.

4.3.4. Unsecured Sensitive Content

This exercise is a variation of the Rogue Component scenario, only it involves content rather than equipment. Depending on how your organization handles paper, this can take many forms. An easy version involves printed pages or binders stamped "secret" left out on a desk. A difficult one would be a sticky note affixed to a monitor containing content that should not be visible. Very difficult variations might be account passwords written down and hidden under a keyboard or mouse pad.

For this exercise to really work, the employee has to understand what should and should not be visible in a public place. Government agencies and defense-related companies tend to be better than most generic companies at defining their classified, protected and sensitive information. Virtually every business has *some* information that shouldn't be exposed to outsiders. This is a parallel exercise, in that it teaches the new employee what constitutes the organization's protected information as much as it is an exercise in learning to see what's actually in front of them. Repetition of this exercise should train the employee to actually read the content posted in and around other work places in order to determine if sensitive content is being inadvertently exposed.

Note that it's helpful to get the cooperation of the worker whose cubicle you are using for the exercise. Have your co-conspirator create the suspect content themselves – using the own handwriting for scrawled content, or their own e-mail account when printing e-mails, etc. Then have the employee place the suspect content in their own work area as if they were actually using it – little measures like this help the item to blend into the background, thereby making it both harder to spot and also a more realistic training aid. The idea is to have the offending object be a needle in a haystack; make the student put some effort into the search.

Keil Hubert, keil.hubert@gmail.com

4.4. The Small Team Office

An enclosed office that two or more employees work in represents a peculiar operating environment. It is similar to the cubicle farm, in that the people sharing the office are not assured of individual privacy, and therefore are likely to be somewhat circumspect. Unlike a cubicle farm, it can be secured – which makes it similar to the comms closet in terms of its attractiveness for storing pilferable material. Since small team offices share attributes of both previously discussed environments, you can productively run several of the exercises from the previous entries.

The more people that work in the office, the higher the probability that the office will be left unsecured so that workers can come and go as they please.

4.4.1. Storage Surprises

The small team office is actually more likely to accumulate stuff than a comms closet because of the increased traffic. A comms closet is accessed only for infrastructure work, whereas a team office is likely accessed all day every workday. Therefore, any available free space in the team office is likely to get used relatively quickly. That being said, objects that clearly do not belong in a comms closet (e.g., cartons of copier paper) may be perfectly appropriate in an administrative space. The key to crafting an effective out-of-place object exercise is to understand what kind of work goes on in the space. Research the space beforehand. Talk to the occupants. It is great practice to bring them into the game as actors in your exercise.

A strong variant on the storage surprise exercise uses inappropriate personal effects. “Inappropriate” may differ depending on company policy; the more conservative the work environment, the more likely it is that any item that’s not clearly “work related” will be considered forbidden. Sports equipment (e.g., a bag of golf clubs) is likely to be frowned upon, but does not constitute a cyber threat in and of itself – it can, however, be an indicator of an employee’s mindset. If an employee is able to rationalize violating one rule, then they are likely predisposed to violate others. This nuanced exercise allowed our employee to analyze the artifacts associated with an actor in order to evaluate that actor’s security mindedness.

Keil Hubert, keil.hubert@gmail.com

4.4.2. Cubicle Farm Exercises

The Missing Components and Rogue Components exercises should resemble the same ones performed in the cubicle farm. Look for what should be there (but is not) and what is there that should not be. Note that an enclosed office offers additional physical space for workers to store objects – in some cases, all the way to the ceiling.

Additionally, a small office that hosts multiple employees likely hosts multiple PCs and phones as well. If the space wasn't engineered from the outset to accommodate all the gear that is being used, then odds are good that the current occupants adjusted the infrastructure to "get the job done." Keep an eye out for small hubs and switches, spliced patch cables, and patch cables run from another office (either through the drop ceiling or under the door). Kludged connections may indicate resentment with IT support.

4.4.3. Unsecured Sensitive Content

This exercise is actually more likely to be a problem in a room with a door than in a cubicle farm. The presence of the lockable door can give workers a sense of safety; the illusion that their data is protected *even when the door is neither locked nor closed*. Play to that knowledge, and liberally salt the exercise scene with sensitive information objects. Bins, carts and stacks full of records might look like legitimate work in progress. Blueprints or networking diagrams posted to the wall are good too, especially if they can be seen from the hallway through the open door. Whiteboards are an exceptional resource for the adversary who gains basic access to the building. If sensitive information is left on the board, a bad guy walking down the hall can snap a photo of the content without ever entering the room.

Similarly, people who feel that their offices are reasonably secure are highly likely to become lax with printed copy that needs to be shredded. Drop some highly sensitive content into the office's recycle bins and/or waste bins. Teach your employees to always cast an eye to these containers when they're within range. The room's occupants might have had the best of intentions and were inclined to shred everything later … but if something sensitive can be snatched or read, it constitutes a risk.

4.4.4. Prototypes and Demos

Another differentiator for small team offices is that the space may well be devoted to an actual team. If the securable room is considered "private" space for a group, the inhabitants may be lax about leaving half-finished projects accessible within the office. If your company has anything to do with technology, introduce a desktop PC or a small server to the space that's clearly in use: strip the case off, and rig it to bypass the company's normal security controls (e.g., automated screen savers, smart-card logins). Does your employee recognize that the project PC constitutes a different kind of risk than normal company PCs thanks to its unimplemented or disabled security controls?

4.4.4. Unsecured Pilferable Property

It is human nature to ask a peer to watch over a valuable object (e.g., tablet, mobile phone, wallet, smart card) while you run a short errand. You trust your peer to keep your gear secure … and your peer can forget, get distracted, or wander off.

Set up this exercise in an office that appears actively lived in. Leave a PC authenticated to the production network and unlocked, but with no operator present. If your company uses smart cards for network access, leave one visible on a work surface. Leave a tablet, wallet or even a credit card lying out on a table where it can be quickly scooped. Does your employee notice the object(s)? Do they secure it (them)? Do they lock the unguarded PC? Do they ask about for the owner or operator?

For an advanced version of this exercise, take a consenting employee's wallet and remove about half of the contents – say, the ID cards, or the cash and credit cards – and then leave it discarded on the floor near the door. Does your employee recognize that the wallet has likely been burgled? Do they sound an alarm before the "thief" can escape?

4.5. The Private Office

Private offices usually signify "power," which is why the "corner office" perq is still treasured in many companies. The employee who gets a private office clearly has greater clout than all the workers on the floor who have to share workspace. If the private office features a "gate guard" out front (e.g., a secretary, receptionist or dedicated assistant who stands between the private office and the masses), then the office likely features a treasure trove of sensitive content secured within.

Keil Hubert, keil.hubert@gmail.com

4.5.1. Actively Haunted Spaces

In addition to presenting a potentially rich target, the private office is desirable for an attacker because of the privacy factor: if an infiltrator can work out when the sole occupant will be out of the facility, their private office then becomes an ideal staging area inside the physical perimeter to operate from with small risk of being discovered. Activity in a space where no activity should be taking place should be a clear indicator that someone is up to something.

Simulate this phenomenon by placing an actor inside the office that you want investigated and have them act like they are actually exfiltrating data. As your employee walks by, do they hear the sound of typing or movement? Do they notice that the lights are on? Do they challenge the occupant? Do they call security to trap the miscreant? Do they validate that the office should be vacant with someone who should know?

This exercise can get confusing quickly if you fail to plan for confrontation. For these actor-driven exercises, craft a back story for the actor, and give them a branching script so that the encounter with the employee can be a realistic as possible. For example, the actor pretends to be a contractor that's committing corporate espionage by using the unoccupied office to hack into the network. When confronted, the actor has an excuse for why he is in the room ("I needed to take this call in private"), why the lights are out with the blinds are drawn ("I didn't want to disturb anything"), and why the office PC is in use ("It was like that when I got here"). For advanced training, coach your actors on how to convey evasiveness, fear and desperation … just be sure to decisively **end the exercise** before either the employee *or* the actor cross a line that your company won't tolerate.

Actor-driven exercises are immensely valuable if you can immediately deconstruct the event *from the actor's perspective*. Explain all of the clues and proper responses to them, then have the actor share his/her perspective on the employee's reactions. Where they swift enough to stop the infiltrator from covering up evidence of their activities? Did they accidentally compromise the scene? Was their challenge credible? Did the actor feel that he/she could escape? Confrontation is unsettling; many people are not comfortable with face-to-face challenges. That said, it's a skill that can be taught and fear of confrontation can be overcome with practice.

Keil Hubert, keil.hubert@gmail.com

4.5.2. Formerly Haunted Spaces

A variation on the haunted space scenario is to arrange the private office to look like it was recently penetrated, but that the infiltrator has left the office. Opening cabinet doors and desk drawers can indicate that the office was riffled through or ransacked. Pull a desktop PC (fully or partially) out from its normal space or partially disassemble the PC case to indicate that an attacker used the PC. Leave sensitive information out in the form of a stack of hardcopies on the printer, MFC or copier. In order to simulate a attack that is currently underway, have the office PC unlocked and authenticated, attach an external hard drive or flash drive to it, and have a massive file copying onto the drive as the employee reaches the office to be investigated. If you have windows that can open safely, leave one propped open … the bad guy may have just left.

4.5.3. Inappropriate Content

A completely different form of cyber compromise is highly likely to occur in private offices, because the occupant feels safe in their "private" space, they believe they can access inappropriate content without getting caught. "Inappropriate" content can range from pornographic imagery to sports scores depending on your company's allowable use policy. Adjust your scenario accordingly. (Lawrence, 2002)

Simple exercises involve having something that your company considers inappropriate up on the PC screen when your employee walks through on another task. Send the employee in to troubleshoot a desk telephone problem, but have your complicit actor leave something visible in a window on the PC's display. For safety's sake, I submit that a simulated image is probably prudent so that you do not violate your own policy. One faculty taught this technique using popular cartoon characters holding signs that said "simulated nudity." Your intent is to see if your employee notices the stimulant. Do they react to it? Do they force the offender to move away from the PC so that the evidence can be preserved? Do they alert the proper resource to take control of the scene?

Audio variants on this work well – instead of putting a (simulated) inappropriate image on a PC, tablet or phone, have one of the devices in the office (e.g., a smart phone sitting face-down on the desk) start playing an audio track that would seem to indicate that the device is currently playing prurient video content.

Keil Hubert, keil.hubert@gmail.com

An advanced variant on this exercise is to have your actor pretend to be furtive; as soon as the employee makes himself/herself known, have the actor immediately clear their screen, or close their laptop screen, or disable their monitor. These actions indicate that the actor has something that they wish to hide in a hurry. See if your employee picks up on the atypical behavior. Can they articulate that the actor may be trying to hide evidence of improper conduct? Do they report the behavior? Do they challenge the employee about it? Do they inspect the (potentially) offending device? Do they secure it?

Content exercises like this can become messy quickly; make sure to clear the scenario with legal beforehand so that a simulated event does not become a *real* event!

4.6. The Break Area

A private office promotes the illusion that the owner is entitled to some measure of privacy. Similarly, break areas can often be perceived as non-work or semi-private spaces where normal work rules might not apply. You might not be allowed to read a novel at your desk, for example, but no one would think it inappropriate if you did so while you ate your lunch in the office cafeteria. This perceived separation of work versus not-necessarily-work spaces can cause some employees to relax their behavior and act differently in the break room than they normally would in the production setting.

Additionally, break areas are often communal settings. You may well recognize everyone else that works in your assigned cubicle farm, but if you do not know every employee in the company on-sight, then the appearance of an unknown person in the common break area may not trigger suspicion. Further, the instinctive drive to avoid rudeness and to seek some small escape from the workplace might numb employees to potential threat indicators in a common area. This gives adversaries the enviable ability to hide in plain sight.

4.6.1. Loiterers

Your environment is unique, but the odds are good that your organization has established some norms regarding break area loitering. Learning to spot suspicious behavior involves understanding what's out of place, and that requires your employees to know the rules and expectations of taking breaks and meals. How long does your employer allow you to be away from the grind for lunch? Or for a coffee break? Seeing

someone you don't know in a common area, perhaps with a coffee and a laptop, is hardly remarkable. Seeing them there for more than hour, though, might be strange. How about all afternoon? Before or after the majority of people arrive from work?

Add this event to a separate string of exercises. Assign the employee to make the rounds of the building, looking for indicators. Have a pre-arranged actor take up a fixed position in the break area with a laptop, tablet or smart phone and feign working. Preferably, this should be someone no one in the facility recognizes. Will your employee remember the actor's face and realize that something may be amiss?

4.6.2. Social Engineering Encounters

Social spaces – where people who have never met might be called on to mingle – open up the possibility of an outsider gaining sensitive information through casual interaction. The "outsider" can be a spouse, vendor, friend, contractor, new hire … anyone, really. This is why employees need to learn how and why to be circumspect in their speech, even when they're psychologically "at work" (and, therefore, "safe"). Kevin Mitnick was able to charm any information that he needed out of darned near anyone simply by being polite, inoffensive, warm and persistent. (Mitnick, 2002)

Pseudo-public spaces where insiders and outsiders can mingle make for a perfect exercise field for practicing social engineering attacks. Get an actor that no one knows and give them a plausible reason to be visiting the complex. They showed up early for an install job, or they are a client waiting on a meeting to start. Let them loose in the break area with a pleasant nature and a list of objectives: the names and phone numbers of all the key managers; the local IP addressing scheme; the skinny on the newest product in the development pipeline; or whatever you feel you would not like to have leaked. Set your actor loose and watch … the odds are *very* good that they will be back in a few hours with all the data you did not want them to have.

As for evaluating your employees, did they even realize that they were being probed for sensitive information? Did they unwittingly reveal any? Did they report the contact? Did they detain or otherwise isolate the contact? Can they articulate the attacker's methodology and, thereby, interpret his or her objectives?

These exercises hinge on people being generally decent folks; people *want* to be liked, and usually want to be appreciated. When you reveal that some friendly strangers might actually be adversaries, there is potential for behavioral overcompensation. You do not want to inadvertently make your employees hostile towards customers. You do, however, want to teach them to temper their natural desire to be helpful and friendly with some practical circumspection. Reinforce the lessons learned in the AAR by practicing verbal disarming and social evasion techniques.

Variant exercises can – and should! – be conducted regularly over the phone, via instant messaging, and via e-mail.

4.7. The Receiving Dock

You may not have a dedicated warehouse depending on the size, location and nature of your organization. The odds are good that you probably do have a regular place where packages and shipments are delivered. You also probably have a go-to place where in-bound packages are stored if the intended receiver is not available. Hopefully, this go-to place is not inside a comms closet (see above).

These exercises are oriented towards organizations that feature a discrete physical location where content is shipped and/or received. Many office parks have a shared loading dock on the ground floor that all the businesses in the complex share. Many retail locations have a dedicated freight area on one side of the building. Some high-security organizations even maintain a separate, isolated complex that's set away from the rest of the campus. Whatever you have, this is a common point of interaction with random outsiders … which means it is a potential threat zone.

4.7.1. Rogue Packages

Locations dedicated to receiving material are accustomed to seeing new objects come and go on a frequent basis. Adversaries take advantage of this in several ways, and we can train our employees to recognize the various attack methods.

Send an unannounced, unsolicited package from off-site to a generic address (e.g., "To: the IT Department"). Scammers use this method to send cheap goods (like re-filled toner cartridges) with an accompanying or following invoice. If the receiver opens or

uses the unsolicited goods, the sender demands that the new "customer" pay for the goods. Use this technique to send a part or component with a fake invoice. Does the employee blindly accept it? Do they break any seals or put the item into production? Do they inquire through proper channels to see if the shipment was legitimate or expected? Do they follow up with the sender data on the invoice or shipping label to validate the shipment? Do they secure the unsolicited material? Do they alert the appropriate element in the company to a potential fraud event? Note that this attack type can be a one-off robbery, or an attempt to compromise a company credit card. Once a payment method is validated, the criminals might set up a "recurring" service, where they regularly charge the business for unsolicited products. Or they will just steal the card number.

A very useful variant on this exercise involves sending a batch of flash drives along with some marketing swag (e.g., fliers, decals) to the employee that you wish to train, addressed to a generic department. At the very least, before you ship out the package, load the drives with a placebo "malware" payload (which can be as simple as a text file with the word "virus" in the name). If you wish to be prickly, have the only file on the drive be titled "Report immediately to [your name]'s office." However you rig the exercise, does the employee connect the simulated infected drive into a work PC?

4.7.2. Rogue Components and Networks

Similar to the Cubicle Farm example, a public space like a loading dock can be an excellent place to introduce items intended to compromise or bypass network security (e.g., a Wi-Fi base station). In a busy public area, it may take very little time or effort to stealthily introduce a rogue device. In a shared space, the problem is greatly complicated, because it can be difficult to determine which organization might have placed the object. When in doubt, people tend to hesitate. Attackers use this to their advantage.

Coordinate your exercise **in advance** with the relevant offices (e.g., the loading dock staff, security) so that the people who normally work in the office do not respond to the inputs before your employee does.

An easy exercise is to plug a Wi-Fi base station into an exposed Ethernet jack in a reasonably visible location (for security's sake, use a nonfunctional patch cable). Send your employee down to the dock to sign for a reasonably bulky delivery. Do they notice

the out-of-place object? Do they ask about it? Do they inspect it? Do they disable or secure it? Do they at least *unplug* it? For added realism, configure the base station as a wireless bridge rather than a home-type router, so that the employee can work out that the device was meant to extend the network compromise outside of the physical facility. Does the employee work out the connotations?

You can also run a variant of the "infected flash drive" exercise from the loading dock. Simply drop your device in a place where it can be found and see if the employee picks it up. Do they take it back inside the organization's perimeter and mount it?

4.7.3. Exfiltrated Data in Physical Form

Massive amounts of data can be stolen via portable hard drives, CDs, etc. If an attacker does not want to risk getting caught carrying storage items out of the facility, they can always have them shipped. For this exercise, pack an external hard drives (or internal drive module from a server) into a moderately damaged shipping box. Ensure that the contents can be perceived from outside the damaged box. Put a shipping label on the box that purports to be from a real department address, but ships *to* an employee's home address, or to a competitor. Send your employee to see your accomplice at the loading dock, using the excuse that an out-bound package got accidentally damaged and may need to be re-packed. Will the employee notice the contents? Will they find it strange to be sending a drive outside the organization via postal service or a commercial courier? Do they re-pack the object in a new box, or do they secure it? Do they interpret from the label that this may be a data exfiltration attempt? Do they alert the security team? Do they advise the loading dock personnel to look out for other such shipments?

5. Words of Warning

All of these exercises were designed to address real-world threats in the actual operational environment. If done well, these are extremely cheap and very effective ways to teach your new IT support employees how to skeptically perceive their workplace in order to recognize and respond quickly to potential cyber threats. Be aware, however, that there *is* a legitimate risk of doing as much (if not more) harm to the employee as good if you are not careful. Be aware of these potential undesired effects:

Keil Hubert, keil.hubert@gmail.com

5.1. Complacency Blindness

The more you train your people, the better they perform the tasks that you trained. The more they practice their skills, the more proficient they become. Success builds confidence. Unfortunately, this confidence raises the very real possibility that a well-trained and thoroughly seasoned employee will become overconfident.

Once an employee gets comfortable with their operating environment and learns where to scan for warning lights, they tend to put less effort into the tasks. After all, *they know this!* Up until the point where they don't …

In David McRaney's book "You Are Not So Smart," he devoted entire chapters to the human fallacies of "confirmation bias" and "attention." He summarized the former as: "Your opinions are the result of years of paying attention to information that confirmed what you believed, while *ignoring information that challenged your preconceived notions*." [emphasis added] Similarly, he defined the later as "You are only aware of a small amount of the total information your eyes take in, and even less is processed by your conscious mind and remembered." (McRaney, 2012)

For our purposes, these two heuristics combine to efficiently undermine the competence of all of our IT employees. During those first few weeks and months, everything in the company is effectively brand new. Every scenario you present is revelatory. The first time that you walk a new tech into the server room, it is overwhelming … so many new sights and sounds to take in. It is little wonder that new employees have no idea which tiny blinking indicator to pay attention to amidst the vast sea of lights. Once they are taught, however, their eyes know exactly where to go – and which inputs to ignore.

Over time, this leads the employee to discard any perceptive input *other than what they had expected.* If you tell them to go see "what is wrong" in the server room, they know which LEDs should blink red, what the room thermostat should say, what the UPS status display should read, etc. They don't actually go in and sweep the room with an open mind; they will usually look right at a problem and skip right over the actual input because it wasn't within the scope of what they were looking for.

Keil Hubert, keil.hubert@gmail.com

5.2. Flawed Realities

The intent of this training methodology is to help your new employees learn what "normal" is within the workplace so that they are primed to notice and react to deviations from the norm. Unfortunately, it is very possible that an employee will accidentally internalize a flawed or skewed vision of the environment – and, once learned, will continue to operate on that flawed assumption for as long as their mental model is not actively challenged.

This is why it is critical to deconstruct an employee's thought process, reasoning and perceptions as close to an event as possible. Do not ask **if** they saw a warning light; ask what it was that they saw. Do not lead them to the answer. People are very good at interpreting what it is that you want them to tell you. For a young employee, the desire to get good marks may inspire them to parrot whatever they think it will take to end the exercise on a positive note. That kind of evasion will not help them learn

An effective way to probe an employee's mental model is to task them to serve as the instructor for a different employee for the task you want to evaluate. Watch how they perform the task, paying particular attention to what elements of the scenario they emphasize and which they deemphasize. You may discover that the "successful" method that the employee had learned was riddled with misinformed information, or was based on flawed assumptions.

Optimally, you want to correct people's flawed understandings as swiftly as you practically can before their thinking gets rigid and they begin to resist change.

5.3. Obsolete Realities

The fraternal twin to the flawed reality problem is that our understanding of "normal" must evolve change as the environment evolves. Unfortunately, people will usually continue to apply their internalized mental models *long* after they cease being accurate. This problem is exacerbated when dealing with entrenched technical people. In IT, skills rust very quickly as technology changes. It's critical to train employees to work with what's actually in front of them, instead of what they're familiar with.

Keil Hubert, keil.hubert@gmail.com

Depending on your budget and culture, you may keep a desktop PC in service for a year … or for five. The standard user equipment package regularly changes. Offices get rearranged as business units reorganize. The server room changes configurations as fast as the budget will allow. Servers get installed, servers get virtualized, racks get rebuilt … The only real constancy in the IT world is change. Some people cannot keep up. In that respect, you have an obligation to re-run many orientation exercises as physical locations or systems configurations change. Consider it a recalibration; your employees knew the old build, now they have to re-learn the new build as if it truly were brand new.

Simple enough, except … there is a more sinister version of the obsolete reality problem that we need to deal with. This is called the "anchoring effect," and it has a special place in the IT world. (McRaney: 2012) In essence, your first encounter with a new situation will continue to influence your understanding of it and attitudes towards it in future encounters, even when the situation changes and our understanding of it should change as well. We see this quite often in early implementations of new products and services. As IT people, we have to fight buggy, incomplete, flawed and troublesome products. By the time we get one deployed to the users, the solution may well have been improved or configured to actually work as intended. That first encounter will linger in our unconscious, though; when we re-engage with that same buggy piece of crud, we react to it based on what we first experienced … not what it actually is.

To mitigate this problem, exercises that take place in pre-production or brand new locations need to be re-run after the new operating environment has stabilized. Make it a point in the exercise AARs to deconstruct how things had been and what has changed. Draw attention to the differences in order recalibrate the employees' mental models.

6. The Influence of Organizational Culture

Security awareness training may be difficult to implement if your organization's culture features defensive or paranoid parochialism. Your employees cannot learn what "normal" looks like in a particular office if they're not allowed *in* the office. Similarly, many of the responses that these exercises aim to teach involve directly confronting problems, witnesses, and supporting agencies. If that is forbidden, why bother?

Keil Hubert, keil.hubert@gmail.com

The problem gets its own chapter because it's highly likely to cause you grief. People being what they are, they come up with official and unofficial sets of rules for getting along whenever people come together in collections. Your large, international company may have codified standards for all employees … but your country's main office will have slightly different ones, as will your local campus and even your floor or office. Even small companies can have different interpretations of the general rules of conduct between different production groups. Expectations for any group of people are collectively agreed to, based on factors unique to the members that make up the group. What works for the salespeople on the 4th floor (e.g., casual horseplay in the cubicle farm, beers over lunch) might be forbidden by the executives on the top floor. (Schein: 2004)

Additionally, the dynamic of any given group changes over time as members leave and get replaced. A team led by a staunchly conservative team leader may grow to function under certain unwritten rules of personal conduct; once that leader is out of the office, however, those rules may change as the repressed and resentful team members "blow off steam."

Finally, the rules that people *claim* to obey might not be obeyed in practice – or, at least, no practiced when no one is watching. This happens quite a bit in organizations with strict cyber security expectations. Your company policy may require you to lock your workstation every time you get up from your chair, but employees will grow tired of complying if they feel the rule is burdensome or is irrelevant to their lives.

You, as the leader responsible for training your people, have to be aware of these factors. Before engineering a training encounter, you will need to watch the people in the operating environment go about their lives. Be as stealthy and unobtrusive possible; think of it as how an anthropologist might observe life in a previously undiscovered remote village, and you will be on the right track. Listen to what you're told, but contrast what you are told with what you actually observe. Note the variations so that you can teach them to your people.

Finally, you actually have an opportunity to teach your non-IT employees about cyber security as they watch you go about training your own people. As often as you can, allow actors and bystanders to participate in discussions and AARs. Over time, you will inculcate the same cyber concepts in your users that you inculcate in your own staff.

Keil Hubert, keil.hubert@gmail.com

7. Conclusion

This paper illustrates a pragmatic methodology for instilling comprehensive cyber security awareness in new employees through full-immersion training conducted in your live operational environment. It's built on twenty years of experience in teaching corporate and military technologists on a constrained budget. I have learned how to make the most of my existing resources to train my people. Now that you have had an introduction to the concepts and example exercises, it should be clear that there's very little stopping you from introducing a similar program in your own outfit.

This kind of immersive training is not intended to be a substitute for formal technical education; your people will always require foundation level knowledge in order to work in IT. This training approach attempts to bridge the theoretical, perfect-world knowledge gained in formal instruction with the gritty, messy application of theory where work is actually performed. As you learn more about your people during the execution of this program, you will likely discover some serious gaps in employees' knowledge bases. That is alright: you *need* to know your people well in order to lead them effectively. Discovering their weaknesses should be a cause for celebration, not embarrassment – ignorance is often easily curable, and education builds a stronger contributor.

The heart of the entire program is to train your new employees to orient themselves to their operational environment, and to learn how places, people and equipment should appear when things are normal. Your role as the coach is to help the new employee gain an accurate understanding of normal; you correct them when they draw flawed conclusions and teach them where, when, how, and (most importantly) *why* to seek out variations from normal operations.

This is a collaborative effort between supervisor and worker, between experienced tech and new hire, between tech and user. It ignores pride in favor of productive, honest communication. Finally, it's meant to be an encouraging, constructive process.

Because this methodology is based on using your actual people, places and gear to train, the only factor limiting you is your own creative streak. Dive in! Try it, deconstruct how the exercise went, learn from your mistakes and then do better next time.

Keil Hubert, keil.hubert@gmail.com

8. References

Air Force Manual 32-1084, *Facility Requirements*, 20 April 2012. Retrieved July 02, 2013, from Son of citation machine Web site from: http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afman32-1084/afman32-1084.pdf

Casey, Eoghan. *Handbook of Computer Crime Investigation: Forensic Tools and Technology*. London, UK: Elsevier Academic Press

Collins, Arthur S, Jr. *Common Sense Training: A Working Philosophy for Leaders*. Novato, CA: Presidio Press

Hoopes, James. *False Prophets: The Gurus Who Created Modern Management and Why Their Ideas Are Bad For Business Today*, Cambridge, MA: Perseus Publishing

Howard, Rick. *Cyber Fraud: Tactics, Techniques and Procedures*. Boca Raton, FL: Auerbach Publications

Hubert, Keil. Retrieved July 02, 2013, from Son of citation machine Web site from: http://biztechreport.co.uk/2012/08/separating-the-l33t-from-the-chaff/

Hubert, Keil. Retrieved July 02, 2013, from Son of citation machine Web site from: http://biztechreport.co.uk/2012/08/practical-interviewing-techniques-part-1/

Hubert, Keil. Retrieved July 02, 2013, from Son of citation machine Web site from: http://biztechreport.co.uk/2012/09/practical-interviewing-techniques-part-2/

Hubert, Keil. Retrieved July 02, 2013, from Son of citation machine Web site from: http://biztechreport.co.uk/2012/09/practical-interviewing-techniques-part-3/

Lawrence, Patti. *Acceptable Use: Whose Responsibility Is It?* Retrieved July 02, 2013, from Son of citation machine Web site from: http://www.sans.org/reading_room/whitepapers/acceptable/acceptable-use-responsibility-it_3

Long, Johnny. *No-Tech Hacking: A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing*. Burlington, MA: Syngress Publishing Inc.

Keil Hubert, keil.hubert@gmail.com

McRaney, David. *You Are Not So Smart: Why You Have Too Many Friends on Facebook, Why Your Memory Is Mostly Fiction, and 46 Other Ways You're Deluding Yourself.* New York, NY: Penguin Group.

Mandia, Kevin; Prosise, Chris & Pere, Matt. *Incident Response & Computer Forensics*. Emeryville, CA: McGraw-Hill/Osborne

Mitnick, Kevin D. *The Art of Deception,* Indianapolis, IN: Wiley Publishing Inc.

Pendry, J. D.. *The Three Meter Zone*. New York, NY: Random House

Schein, Edgar H. *Organizational Culture and Leadership*, San Francisco, CA: Jossey-Bass

Keil Hubert, keil.hubert@gmail.com

Last Updated: June 22nd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Paris 2017	OnlineFR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced