

AN ETHNOGRAPHIC STUDY COMPARING RESTRICTED AND OPEN ENGINEERING LABS FOR INFORMATION CONTROL

Lee J. Steen, Robert Morris University, ljst8@rmu.edu
Robert J. Skovira, Robert Morris University, skovira@rmu.edu

ABSTRACT

Advanced Rocket Research Corporation (ARRC) is an engineering company that specializes in doing research and development for the Pentagon. ARRC has open laboratories for research that any employee can access and work in. ARRC also has restricted or closed laboratories that only employees with cleared access can use. This paper takes an ethnographic study comparing each of the labs. From the study, patterns that appear will be identified and theories will be proposed when applicable. The main theories use Hofstede and Hofstede's [3] five dimensions of culture, security models, communication with the aid of a system model, and emotional knowledge to explain information control.

Keywords: Information Technology (IT), Human Factors, Information Control, Cognitive Science, and Security.

INTRODUCTION

Advanced Rocket Research Corporation (ARRC) is an engineering company that specializes in doing research and development for the Pentagon. ARRC has open laboratories for research that any employee can access and work in. ARRC also has restricted or closed laboratories that an employee must be cleared to access. The Pentagon has three main levels of security clearances for employees. In order of lowest to highest they are Classified, Secret, and Top Secret. In order to obtain a security clearance at any level, a background investigation is performed to ensure the employee is responsible, ethical, trustworthy, and crime free. The desired cleared level determines the extent to which the employee is subject to a background investigation and interview. In order to be a candidate for a security clearance, the employee has to have a "need-to-know" purpose. This is because the Pentagon requires the employee has a purpose to access some type of classified information. This usually means the employee was hired to work on material that is considered classified.

The two labs at ARRC that were monitored were an open lab and a secret lab. Whenever the words

closed or restricted are used for a lab, it refers to the secret lab. The words engineer and employee are used interchangeably also throughout the paper. The open lab is used as an electronics lab. This lab contains soldering stations for circuit card assembly (CCA) boards and a lot of other equipment. The restricted lab is a high technological advanced lab that has systems ARRC works on that are on the rockets sent out by NASA.

The observations made between the labs will appear in the following sections detailing the recordings and describe where each one fits. The open lab was much less secure than the restricted lab. When people are in the restricted lab, their sense of security and awareness is heightened. Power differentials appear more in restricted labs as people take the idea of security as personal responsibility. The restricted lab saw an increase in communication compared to the open lab. The restricted lab was also a more formal structure than the open lab. All of these factors support the theory of information control within a secure environment.

Tipton [11] identifies Access Control, Information Security and Risk Management, and Physical (Environmental) Security as three of the ten common bodies of knowledge (CBK) for the Certified Information Systems Security Professional (CISSP) exam. The CISSP is considered the gold standard for security exams in information technology world wide. This paper is easily adaptable to any of these areas.

The Labs

There were two different labs being observed, an open/unclassified lab, and a restricted/classified lab. The open lab is considered open because it is not classified and is not allowed to contain classified material in it. There is an east door opening leads to a hallway and a north door opening leads to a room full of engineering offices and cubicles.

Upon walking in the door to the open lab, the first thing that is noticeable is that the place always looks like it is in chaos. Most engineers enter from the east since it is part of a main hallway. When entering in

that door, the first thing that is seen is a large desk full of soldering equipment. The equipment is regularly spread out all over the table. The equipment includes soldering guns, soldering wire, shrink wrap, picks, tweezers, suction ducts, extra wires, wire cutters, and heat guns. Papers full of schematics are spread out and hung up at eye level above the soldering station. Wires hang down from the edge of the desk with alligator clips at the end of them. The desk shelves are wiring meshed and have other equipment such as volt-meters on them mixed in with wires and soldering equipment. In this chaos though, the engineers seem to get around pretty easy.

The open lab has chairs spread out near all of the desks. The chairs are usually pulled out from the desk and randomly placed at one side or the other. There is rarely a time when the seats are at their designated area (designated for safety reasons).

RESEARCH METHODOLOGY

The study began as an ethnographic study to research the culture of a secure engineering lab environment. As the study progressed, noticeable differences emerged from the comparison open lab also used by the engineers. The research then was focused on a main difference in the labs, how information is controlled. The question that was asked was “how is information controlled within each lab comparatively?”. The second question asked later was “what makes the restricted lab information controlled so much more tightly?”

This was a qualitative study. The proceeding sections have the names of the individuals and any given dates scrambled and changed. This does not affect the theories of the paper or its validity. Ethnographic methods were used to obtain the data.

James Spradley [9], author of *Participant Observation*, sets out an ethnographic methodology of study called the “developmental research sequence” that was used in this study. The culture of each lab was different, but just slightly. Hall [2] states that “[w]hat has been thought of as mind is actually internalized culture” (p. 192). This means it what may be seen as thought or emotions, is really part of the culture. Geertz [1] states that “[c]ulture is public because meaning is” (p.12). Since culture is public, the ethnographic study will hold because it can be observed and is not hidden or concealed.

IDENTIFIED PATTERNS AND THEORIES

This paper describes how the culture of the secure environment is affected by several different components and how each component plays a role in information control. Hofstede and Hofstede [3] identify five dimensions of culture that were investigated in the ethnography and this paper shows how each dimension affects information control and security. The paper identifies how environmental objects are used for visceral control in specific settings. Awareness and communication through emotions like fear and respect that have been heightened due to the cultural settings defining human instinct are investigated. Mental models and learned behaviors are identified and shown how they contribute to the information control. Information control through obscurity and short term obligations are identified. Frames of environments in the culture are used to show where the culture changes and where the ecology of the “infoscape” takes place. Finally, the paper identifies when conscious behavior becomes unconscious and this affects the information control.

The following sections will detail identified patterns, comparisons of the lab cultures, and theories when applicable. Stories may be given to provide examples to help clarify detail when needed.

Entering the Labs

When there are people in the open lab, it is hit or miss if they will look up and acknowledge a new presence in the room. Earlier in the morning, before 9:00AM, a person entering the room is more likely to be acknowledged upon entering the room. This is likely because engineers are expecting others to begin entering the lab because work typically starts at 8:00AM. ARRC allows flex time for the engineers, meaning they can work a schedule that best fits their lives with approval from their supervisor. That’s why some people don’t come in by 8:00AM to start work.

The restricted lab is a bit different. There is a lock outside the door that is high tech. It is not simply a combination lock, but a digital combination lock that does not allow the numbers to be displayed unless looking at it in direct line of sight from above. This makes someone trying to see the combination have a very hard time clearly identifying the numbers, if any can be seen at all. These locks can also be programmed to have special combinations, meaning the standard turn right, left, right combination may not apply. It could be right, right, left, left, left, left, right, left, and right if it needed to be. The combination to the door is only given to specific

employees who need the access. If the employee does not need access, the employee does not need to know the combination (another need to know). Surprisingly, there is not a paper that tells what employees have access and what employees do not that is openly available. There is a sheet that exists, but it is held by head of security so the list is known incase it is ever needed.

The combination lock alone is an environmental object that instills a sense of security in a person just by the look alone. Norman [5] identifies the visceral level as the first level of emotional processing by saying this is the “automatic, prewired layer” (p. 21). Norman [5] explains that as humans, the visceral level has a strong hold on emotions and plays a key role into molding the other two layers of behavior and reflective. This means that the lock’s look alone is enough to make a human understand the area is secure and important. This will raise emotions that aid in information control.

The restricted lab, upon entering is very clean. There are rarely papers laid out on the desk. If they are laid out, there is usually a person sitting right by them. This is very true for classified papers. The classified papers will never be laid out on the desk alone, even though the room is secure and allows it.

The restricted lab has all of the chairs right near the desks that they belong to and are pushed in. Rarely will the chairs be chaotically laid out. The chairs can be used at any desk in the room. In order to make sure the room stays clean and organized, there are not enough chairs in the room to fill all the desks. The purpose of not having a full room of chairs is because most of the time, the room is being occupied by different people on different projects at different times. This means only half of the computers and systems in the room will be used at any given time. Rarely will all of the systems be used at the same time.

When people occupied this lab, there was never a time observed when an individual entered the room and nobody “looked up”. Immediately upon turning the handle, people will look up to see who is coming in. They will cover papers or move computer screens to hide information, controlling access to it, until a person is identified coming in the room. Then once the person is identified and people know the person is cleared, the engineers in the lab will relax and say “hello” or at least give a nod acknowledging the person is in the room.

Comparing the introduction to the two labs, it is clear the restricted lab gives employees a heightened sense of awareness. The engineers in the restricted lab always know who is in the lab with them and who is cleared for access. By acknowledging a person that walks in, the engineer is giving a subconscious respect identifying the person coming in is equal. The person coming in acknowledges back, giving the same subconscious respect. This is identified by Hofstede and Hofstede (2005) as “power distance”, or more precisely “[p]ower distance can therefore be defined as *the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally*. *Institutions* are the basic element of society, such as the family, the school, and the community; *organizations* are the places where people work” (p. 46). Power distance is one of the five dimensions of culture defined by Hofstede and Hofstede [3]. The other four will be explained later.

Even though there is not a direct power distance between the engineers upon entering, there is a power distance between a cleared employee and a non-cleared employee. If a non-cleared employee would walk in the room, s/he would immediately be escorted out by one of the engineers in the room and security would be notified of the breach. In the open lab, no such thing would happen; there is no clear power distance between the cleared employees and the non-cleared employees.

Hofstede and Hofstede [3] label “uncertainty avoidance” as another dimension of culture. Hofstede and Hofstede [3] define uncertainty avoidance as “*the extent to which members of a culture feel threatened by ambiguous or unknown situations*” (p. 167). The main idea behind granting security clearances for access to information is a clear result of the Pentagon’s way of avoiding people that have an uncertain background. Once the background investigation is completed on an employee, the Pentagon is then more certain a person is acceptable and trustworthy. This clearly shows avoidance of uncertainty. Without being cleared, a person cannot access classified information. By controlling access to the information, the information is controlled.

Leaving the Labs

Observing a person leaving the labs also indicates that the employees in the restricted lab are more aware. Upon leaving the open lab, if employees are in there working, they may not even look up to watch people walk out. There were only a few times this

was observed. Most of the time when it was observed that an engineer acknowledged another leaving the lab, the two were working together on something, so when one got up to leave, the other watched. Even more to the point, it was observed that the people, who watched others leave, waited until the person leaving said "I'll be right back" or "see you later".

In the restricted lab, even when a person stands up, it was observed that the other people in the room watched as the person moves around. It was not a direct staring watch, but rather one where the people looked up and watched for a second, then continued working, then looked up again and continued working. The second the door opened to leave the room, people will again look up and nod to acknowledge the environment has now changed. This acute awareness in the room shows the security is tightened. Even upon leaving the lab, the people left in the restricted lab want to know the state of the lab and who is in there. This is again an example of uncertainty avoidance. If the engineers that are in the lab are uncertain about the state of the lab, it is less secure. The more the state of the lab is known, the more control each engineer has in the lab over the information being used.

No Assigned Seating and Uncertainty Avoidance

With all the security and awareness in the lab, it's not very shocking to learn the engineers don't like change. Change brings out uncertainty and makes it harder to be certain about the environment. It is hard to change things like the placement of the desks or the systems in the rooms, but it is very easy for the individual engineers in the room to change seats.

In both labs, rarely did seat changing take place. When change did occur, the move was typically only one seat away. In the open lab, it happened more often because there are no PC's in there because the areas are designed for special purposes. If an engineer needs to solder, there are 4 soldering stations available. Each engineer seemed to have a preferred station to use for this. If there were 3 people working in the lab, each day they would be seated at the same place. But sometimes special tools were needed available at only one station. When this happens, the engineers seem to get confused.

One story to explain this occurred over a course of two weeks. Three engineers, Tim, Dave, and Bill were all in the open lab working on different projects. Bill is a young electrical engineer with about one year of experience. Dave is a tenured electrical

engineer with about 20 years of experience. Tim is a mechanical engineer with about five years of experience. The first week and a half they all stayed at the same station working. Then Bill switched stations one morning because he needed some special equipment available at only one station. The one station happened to be where Dave was working prior. When Dave came in the morning and saw Bill at his station, he asked him to move. He said "Hey! That's my soldering station man! Go back to yours!" Bill explained he could not because of the equipment. Instead of Dave moving to a new station, he decided to work at his desk on other things until that station was open again. Once Bill was done with the equipment, he went back to "his" station.

This example shows again uncertainty avoidance and power distance. Bill needed to change his station, a simple seat change, but Dave did not want this to happen. Instead of going to a new or different station, Dave chooses to avoid the situation and wait for it to pass. This also shows power distance. Dave is a veteran engineer and is in a higher rank than Bill. Even though Bill did not move and submit to Dave, Dave understood after Bill's explanation that Bill needed the station. On the other hand, if Bill did not need the station, Dave's confrontation would likely cause Bill to move back to his original station. This shows Dave is of higher rank than Bill.

In the restricted lab, the personal computers (PCs) are networked. This means that there is no reason the engineers need to switch computers. But when going in the lab, they always stay at the same PCs. However, this does not happen very often. Monitoring where people sit is a very easy job because they do not move! The five main computer systems were always utilized by the same people. Sometimes the chairs had to be moved in order for a group to look at data on the same PC. When this happened, more power distance appeared.

When people had to move together to review something on the same PC, the most tenured person was at the center of the group. The other engineers would gather around this person's PC. This gave the person in the center the most control since s/he could operate the PC and control it. The others could only simply watch. Even when critiques of programs were going on this is noticeable. Two software engineers, Sid who has about 40 years of experience and works as the manager, and Doug who has about 5 years of experience and is Sid's employee, were working together in the restricted lab on a PC. While they were looking at some stuff that Doug wrote, Doug moved to Sid's computer and sat next to him. Doug

watched as Sid critiqued his work and explained it. Doug never touched the keyboard or mouse, even when explaining something that could be taken care of much easier by doing so. This again shows power distance, but this time in the restricted lab between two employees.

Acute Awareness of Information Control Mechanisms

In everyday life, people always run into things that need to stay shut and possibly locked. When a person gets out of his/her car, s/he shuts the door and locks it presumably. When a person leaves his/her home, s/he shut the door and locks it. When a person gets food from a refrigerator, s/he shuts the door to make sure the cold stays in. All of these are examples of actions that really happen subconsciously to keep something safe.

At ARRC the same thing happens, but to a bit more of an extent. In the open labs, when an engineer leaves the room, he (he because there are no women at ARRC, to be discussed later) may shut the door, but never looks back. When he opens a cabinet and shuts it, he doesn't look back.

In the restricted lab, when an engineer leaves the room, he pulls the handle on the door to make sure it is shut and shut tight. When he opens a cabinet or safe in the room, he always gives it a tug to make sure it is shut. This again helps avoid uncertainty. When he realizes it is shut, he is more certain it is more secure. This small extra step speaks a lot to the extent to which the engineers go to make sure security is high. This is not a mandatory thing to do, but something every engineer picked up while working in the secure environment. The idea that it was picked up, shows it was likely picked up by a more tenured employee and followed by the rookies. This display also shows power distance.

This extra display also plays into Hofstede and Hofstede's [3] third dimension of culture, "individualism and collectivism". Individualism is defined by Hofstede and Hofstede [3] as pertaining "to societies in which the ties between individuals are loose: everyone is expected to look after himself or herself and his or her immediate family" (p. 76). They then move on to explain that collectivism "pertains to societies in which people from birth onward are integrated into strong, cohesive in-groups, which throughout the people's lifetimes continue to protect them in exchange for unquestioning loyalty" (p. 76).

The idea that the engineers learned this value from tenured employees and not from security training, gives way to the idea that individuals learn from their elders. Roger Schank [7] explains that "[n]onconscious learning is the most common form of learning" (p. 173). The engineers were not consciously trying to learn these values, it just happened. This can be true of either collectivism or individualism, but taken into account the idea that most of the time the engineers work together, it is more of collectivism than individualism. Hofstede and Hofstede [3] also identify three characteristics of companies that makes the company a more collectivism company type. One is training, which ARRC is not short of at all (even informal training). Another is applying skills. At ARRC, if you don't have the skills, you can train to obtain the skills and use them. The last one is good physical conditions, which ARRC is careful to make sure the safety of the employees comes first and the environment is conducive for engineers. Finally, as will be seen in the next few sections, ARRC engineers take the idea that "security is everybody's responsibility" to heart. They work together to ensure that only top notch, secure products leave with the ARRC name on it. By controlling the products that leave, the information is also controlled.

Safety, Security, and Friends

With safety and security being a top concern to engineers in the restricted lab, one has to ask what they are keeping secure. There is a very simple answer to that question, data, information, and knowledge. Each one of those is used interchangeably but is very different.

In a lecture given on August 22, 2007, to a DISC 8110 class, Dr. Anthony Debons of University of Pittsburgh defined data as a "representation of space, energy, matter, and/or time, in a symbolic form that is bound by certain rules (or algorithms)" (A. Debons, DISC 8110 lecture, November 22, 2007). This indicates that data has no real meaning and is simply a recording or representation of one of the mentioned such as a time stamp, amount, weight, or color. Debons then went to explain that data can be processed to form information. Debons defined information as "[a]n awareness representing a state of being that contains the essence of 'that' being represented by what-where-when-whom" (A. Debons, DISC 8110 lecture, November 22, 2007). From this information that is gathered, knowledge can then be formed. Debons defined knowledge as "the state of understanding, physically or cognitively,

and understands how and why” (A. Debons, DISC 8110 lecture, November 22, 2007).

Debons led into a conversation about his model EATPUTr, which is a model that shows how systems work and how information is transferred within them. The model explains how information, data, and knowledge are communicated within the system. The systems can be an environment, person to person, computer to computer, or any mix of each. Each letter in EATPUTr stands for something specific. Debons designed this model to address how an information system (or any real system) works and the major parts of the system.

E represents an event or situation that occurs. This event happens by energy in the environment that stimulates some action. The event could be something like a person talking. The words coming from the person’s mouth are the energy being generated.

From this event, A is the acquisition for data of the event. This is usually a sensor whether electronic, biological, or a mix. The acquisition records data from what happened. This could be a person’s ears picking up the sound. At this point in the model, the energy is still simple data.

After data is recorded, it is able to be transmitted as it is understood by the acquirer, this is the T. Transferring includes flow of the data. The transferring is moving the data from the recorded area to an area where it can be analyzed or processed. This is like the receiving person’s ears hearing the information, and then moving it from ears to the brain.

Once the data makes it from point A to point B in a system, it is able to be processed, the P in the model. Once processing occurs, whether by the human mind or an electronic system, it becomes information. Information is processed data, so it now has a context within it. This is like the person’s brain analyzing the data to understand it.

Next, utilization of the information occurs, the U in the model. Utilization is the point when the information becomes knowledge as it is used for decision making. This is the person using the information to form knowledge to make a decision or use the knowledge in some way.

This knowledge is transferred, the T in the model out to environment for the utilization, or knowledge

source. This is the person talking about what s/he heard and stating his/her understanding of it.

Finally, r is the response. The response is critical to the system to keep performing. Without response, feedback is not used, context is lost, and the communication can break down. The response is the person then asking a question or giving more information to the original person talking.

So the reason the engineers protect all three is because the data can lead to information, and information can lead to knowledge. The data is sensitive because it contains information that the Pentagon feels can be used against the nation’s defense and cause harm in great numbers.

Employees at ARRC are read statements by the facility security officer, from the Pentagon exactly how it appears on the sheet, about security and nondisclosure. This is very precise and exact. It outlines what the consequences are if information is released (either by accident or on purpose) and what the employee (and company) will face as a result.

For this reason the classified data, information, and knowledge that are on paper and held by the employees, are always in the employee’s hands or within arms reach. Upon entering the open lab, papers are hung up and spread out on the table. When other people enter, the papers could be in plain view. In the restricted lab, the papers are neatly laid out in front of an engineer and within arms reach. This is another action picked up by younger engineers from the more tenured engineers. This is not a requirement, but it is more secure and safe. This is true even for non-classified material. I asked one engineer why he did this; his response was “I don’t know. It’s safer. Even if it’s not classified, I don’t want people to see it and think it is classified. Plus, anything you use back here (referring to the restricted lab) is sensitive in one way or another”. Again, this shows his sense of security is heightened in the restricted lab. The heightened security in turn holds onto information control.

Information Hiding

Think about high school students in the United States of America at a party. A few of them are sitting in the basement and an adult, one of the kid’s parents, walks down. The kids hear this and hide beer bottles they are drinking because they are not allowed to be doing so. The kids were startled because the unexpected happened. In the restricted lab, one participant displayed similar behavior. Not because

he wasn't supposed to be doing something, but because he wanted to make sure people who weren't supposed to see what he was working on, didn't see it.

Sid, the tenured engineer, is very careful how he handles classified material, on paper and digitally on the screen. When people enter the restricted lab and he is there using a computer, he immediately moves towards the screen as to cover it up. Once he acknowledges the person, he waits for the door to be shut and backs away. This display shows he is very careful about what people see. This again isn't a security requirement, but one more display how the engineers go the extra step to safeguard the information through information control.

I asked Sid why he does this. His response was "I don't do that". This became part of his subconscious routine but for some reason was not picked up by any other engineers. This display leads into another one of Hofstede and Hofstede's [3] dimensions, "long-term orientation and short-term orientation". Hofstede and Hofstede [3] describe long-term orientation as "the fostering of virtues oriented toward future rewards – in particular, perseverance and thrift" (p. 210). They then move onto describe short-term orientation as "the fostering of virtues related to the past and present – in particular, respect for tradition, preservation of "face," and fulfilling social obligations" (p. 210).

Although not directly seen, Sid displayed ideas of short-term orientation. The idea that he needed to secure the information right away showed concern for his personal stability. His position also gave him social and status obligations. He is one of the senior engineers and needs to display the highest level of security. If information that is classified is ever divulged by him, he loses his reputation.

He does this whenever the door in the restricted lab is opened. This is when someone is leaving or entering. A story to test how often this occurs happened. One engineer left the restricted lab one time, and immediately opened the door back up, shut it, and opened it back up. Every time, Sid covered his screen. Comparing this to the open lab, when Sid is in there, he freely lays down papers and never covers the screen. One engineer walked by and looked right at his screen and he simply says "What are you doing?" Not having to highly secure information in one's possession lowers the sense of understanding of the environment around them. When it does need protected, the information is heavily controlled.

Dr. Robert Skovira [8] of Robert Morris University used the idea of "information landscapes or infoscapes" to help explain the corporate ecology of information use. One of the main ideas of an infoscape is the use of "frames". Skovira [8] describes a frame as "organizing structures of experience that define situations of information use" (p. 310). From this definition, Sid is shown to have two different frames that are used in each lab. In the restricted lab, he is highly secure, in the open lab, he is not. In the restricted lab, Sid is much more apt to control the information.

Observed Security

When an engineer enters the open lab, he can go to shelves and drawers pull things out, and nobody notices. The restricted lab is not the same. Upon entering the restricted lab, the engineer is watched until he sits down. If he gets up at any point, he is watched. There is a safe and a cabinet in the restricted lab that holds classified material. If anyone opens it and pulls things out, he is being watched.

There were several times when some engineers would take a bit longer searching the cabinet. If the engineer takes too long, someone in the room will ask "[w]hat are you looking for?" This indicates that uncertainty is coming back into play. As mentioned before, uncertainty means less security. The goal of the restricted lab is to be highly secure.

What makes it more interesting is to ask someone why he asked if help was needed help. When this was asked, one engineer responded "[y]ou are taking a long time. I just thought you didn't know what you are looking for." Then the other engineer taking his time said "I don't know what I'm looking for, but I'll know when I find it." Seeing that this answer made the first engineer more uncomfortable, he said "[w]ell explain what you want, and maybe I can help." From this point, the second engineer stopped there and told him he wanted to see how others would react. He didn't want to drag it out because again, security is serious in this lab, and he could have got in a lot of trouble.

Two things play into the trouble. First is power differential. The security officer has a lot of power over the engineer. He can easily get the engineer thrown in jail and investigated if he thinks the engineer may have compromised any classified material. Second are emotions. Dr. Rosalind Picard [6] of MIT explains in her book *Affective Computing* that "[o]ther results have emerged from neuroscience, cognitive science, and psychology, indicating a

pivotal role for emotion in attention, planning, reasoning, learning, memory, and decision making” (p. 1). Thagard [10] supports this claim by stating in his book *Mind* that “emotions play a role in human thought and action, explaining why people do what they do often requires us to refer to emotional states” (p. 163).

Cleared employees sign off on a document that is very serious and fuses emotions of respect and fear together. Respect for the information being obtained and used, fear in not letting it ever be released. Then when only certain people can access a room comes into play, the respect is enhanced. The room itself helps raise these emotions through the use of locks, boards on the walls to stop sound, gates over any ventilation, and locked safes in the room. When employees are in this room, these emotions come out to the forefront. This is another reason awareness is heightened. Fear is what drove the engineer to tell the other engineer why he was taking so long at the safe. He did not want the other engineer to think he was searching for information that he should not have access to. Benjamin Libet [4] explains in his book *Mind Time* that “[t]he popular notion that people have a continuous stream of consciousness is contradicted by the time-on requirement for conscious awareness” (p. 112). What Libet is saying, is that people don’t have a continuous stream of consciousness, and at some point, conscious awareness is removed and unconscious actions take over. Libet [4] also explains later that feelings can take over an unconscious state to make someone more aware by explaining a study where people were asked to record clock times when s/he was ready to act (p. 132). Applying this to the situation with fear, means fear drove unconscious lower, making conscious thought more prevalent, increasing awareness, thus increasing communication and security at the same time.

Organized Security

The emotions played a big role in how far the engineer in the previous story was willing to test the waters. Another experiment involved leaving the room while papers were still out on the desk. Although this isn’t against the policy, when it was tried, two engineers, Sid and Doug, stopped the engineer from leaving the room and said “you left these in here.” The engineer told them he would be right back, so Doug said he would hold them for the engineer until he returned.

Another time, the engineer left the door to a cabinet open after he took things out. Doug pointed it out as

the engineer walked back to his seat. This again indicates he was watching the engineer as he moved and went in the cabinet. The engineer went and closed the cabinet.

A third time when the engineer was leaving the lab with Doug, he closed the door and turned the combination lock on the door. When there is nobody in the lab, the lab has to be locked. The engineer started walking away and Sid went and pulled the handle to make sure it was closed for sure. The engineer usually does this, but he wanted to see if Sid would check it. When they left the restricted lab, they went to the open lab. When they left the open lab together, the engineer shut the door to see if Sid would check it. The engineer was careful to shut it so it could have easily been open again and was not fully shut. Sid didn’t go back to check it.

This indicates Sid doesn’t care about the door being shut. The door has to be shut in the restricted lab, but not checked for stability or how well it is shut. The engineers again, just picked up on double checking. Double checking increases the security, reduces uncertainty, and helps ensure information control is followed.

Information Control in an Unsecured Area

As indicated before, when engineers are in the lab they are very conscious of their surroundings. Part of this is emotion. The emotion that comes from handling classified material through respect and fear stays with engineers even when they take classified material out of the restricted lab.

Doug once took classified material out of the lab to staple it with a large stapler in the front of the building. When he took this, he held it close to his body; his arm was around an entire folder, holding it close to his chest. When he stopped to talk to people, the folder didn’t move and he kept moving, not stopping to talk. He is usually a guy who likes to talk, but on the occasion of having the material, he made his conversations short and quick.

This was also noticeable for others who carried material outside of the lab. Ted, an electrical engineer with over 15 years of experience and a strange sense of humor, took a folder of documents out that needed to be transferred to another building. Along the way, he had to stop and talk to some of his engineers who report to him. He kept the material on him at all times and never set it down.

This idea of the classified material carries the emotions with the engineers even after they leave the restricted lab. If they do not carry material out of the lab, they tend to be more relaxed. The second the material leaves with them, they are very serious and the sense of awareness and security is still heightened.

In terms of EATPUTr, this means that the last T or transfer is very secure. At this point, the information has become knowledge. When the engineers are walking around with the classified material, the knowledge they hold is very important and needs to be secure. The r is blocked until they return the material to a safe area. As the information leaves the lab, it can be considered an event, and the engineer is determined to ensure that the A or acquire does not happen. The reason the material is knowledge is because the information leaving the lab that is classified is leaving to be transferred. By controlling the transference of knowledge, the information is implicitly controlled since knowledge cannot exist without information (since information becomes knowledge).

Physical Protection of Data Hiding

As mentioned in the “Safety, Security, and Friends” section, all the engineers keep the classified material within an arms reach. When the door opens, Sid covers his screen to protect material, and that is within an arms reach. But the other engineers also cover their papers or turn out of view when the door opens also. This means if there is a paper in an engineer’s hand, when the door opens, he will put it straight up so it cannot be seen from the door. Once the person is acknowledged, the paper will return to a comfortable position.

This indicates again that the sense of security is heightened in the restricted lab. In the open lab, when an engineer is reading something, he continues to read as people walk through and make no attempt to cover anything up. This is the reason many things are hanging from the above shelves at eye level. It is more comfortable and easy to read from the seats at the soldering stations. The material does not need to be secure, so there is no reason to treat it as restricted material, no need to control the information.

Complex Security Devices

Another sign of security comes from the locks themselves. As mentioned in the “Entering the Labs” section, the locks are not normal locks. The locks give the environment a look and feel of security. But

having an engineer sit in front of a lock that takes a few minutes to open, gives it even more a look and feel of security. When an engineer goes to open a lock and is in conversation with another engineer, they both become quiet until the lock is open. The locks cannot simply be smacked and opened like a jukebox is smacked to work when it skips or won’t play.

There is a reason for the silence. As seen in Debon’s EATPUTr model, communication happens on several different levels. If at any of those levels there is a break or distortion, the communication can become unsuccessful. Entering a combination is like transferring information. A person talking while inputting a combination can be like an extra input because of lack of attention. The breakdown happens at the transfer level. This is where the person is processing the next number. If the previous number is not remembered, or the previous sequence, this will be off. This causes a processing error and thus makes the information wrong. Then the wrong information is transferred as knowledge to the combination lock. Since the pattern is not exactly what is expected, the combination will not open.

The quietness shows an increase in communication and awareness in the restricted lab. The open lab contains no combinations so it does not need this quiet time. The idea of being quiet is also translated into general conversation. As one person is talking, everyone else is quiet. When the restricted lab has people talking, it’s not like a conversation where interruptions are common. It is less likely to have interruptions so everyone is on the same page. After talking to a couple engineers, a conclusion of emotions comes back into play. The engineers all said they wanted to make sure everyone was on the same page. This hope of everyone being on the same page comes from the fear that there might be a breakdown in communication, thus a breakdown in security is more likely, leading back into uncertainty.

Chain of Custody

Since the information in the restricted lab is so important, the security people at ARRC want to know everyone who has combinations as mentioned above. The combinations indicate that the person is able to open the room or safe. In order to be able to identify on a daily basis who opens what, there is a sign in sheet. Whenever someone is the first person to open something, he must sign off on a sheet. Whenever someone is the last person of the day close something, he must sign off on the sheet. The signoff becomes very subconscious. Since someone is

putting his signature on the paper though, emotions come back into play.

When someone is taught how to shutdown the restricted lab, he is trained to lock things up, move the combination a bunch of times, and pull to make sure it is fully locked. In this sense, it is part of the process, but not the policy. The policy is simply to lock it up, not check it. But out of the emotional fear, engineers ensure it is definitely locked, by mitigating uncertainty.

Special People Constraints

The chain of custody gives rise to a unique concept at ARRC. Only certain employees know the combination to certain things. This is again determined on a need to know basis. If an engineer needs to know the combination, he will be given it. Otherwise, nobody is allowed to disclose it. But there are well over five different combinations for the restricted lab. There is one for the door, one for an alarm, one for a cabinet, one for a safe, and more. The funny thing is that someone can have the combination to the safe, but not the combination to get in the room where the safe is! According to the *Official (ISC)² Guide to the CISSP CBK (2007)* this is known as “[c]ontrol and separation of environments” (p. 576) or better as separation of duties in other common bodies of knowledge.

The same thing can be said about the combination lock to the door. Even though someone might have that combination, he might not have the combination to disarm the alarm once the door is open! The reason is simple. Only certain people are allowed to open the lab. Once it is opened and the alarm is disarmed, it stays that way until the end of the day. So if nobody is in the lab during the day, some people may want to enter. By not manning the alarm after every leave, it is easier and safer for people to enter. The alarm is silent, so it could easily trigger a false alarm if it’s on and the police would show up. This causes a fine to the company and some angry managers! The payoff is the information is controlled at different levels and different areas.

RESULTS

The results indicate that the restricted lab has stronger information control as suspected. The results also support the identified theories of emotional control, Hofstede and Hofstede’s [3] five dimensions of culture, and the heightened sense of communication that factored into information control.

CONCLUSIONS

Comparing the open lab to the restricted made the obvious come out, and the not so obvious. Of course the restricted lab is going to have more security in it. That is the point of the lab. But how it effects emotions, communications, unconscious actions, and the culture was not so obvious until patterns began to emerge.

Looking at Hofstede and Hofstede’s [3] five dimensions of culture, each one has fit in the ARRC culture. But only four were mentioned above. What is the last one? The last cultural dimension given by Hofstede and Hofstede [3] is “masculinity and femininity”. Hofstede and Hofstede [3] describe masculinity as “when emotional gender roles are clearly distinct: men are supposed to be assertive, tough, and focused on material success, whereas women are supposed to be more modest, tender, and concerned with the quality of life” (p.120). They then move on to describe femininity as “when emotional gender roles overlap: both men and women are supposed to be modest, tender, and concerned with the quality of life” (p.120).

It is hard to define this dimension at ARRC at first glance because there are no women that work as engineers here. But given that fact, one would then tend to lean towards a more masculine culture. Our society tends to push men in science and women in arts. This is changing, but it is prevalent at ARRC. There are no women engineers working here. There are women working here, but they are administrative positions and assist the engineers in the administrative arena. This by no means makes them less valuable, but the administrative area is geared more towards quality of life and peace, rather than the core work of the company. The core work is engineering, but it also couldn’t get by without administrative detail. What does this mean? One could say ARRC is more feminine for that reason, but emotional roles are still prevalent. The engineers are seen as tough and assertive, where the administrative people aren’t.

Given that information and that only the engineers are cleared for the lab, one can only assume then that the restricted lab is masculine. The open lab is also masculine because engineers are the only ones who use the lab. Masculinity involves assertiveness and success. This is probably why the power differential exists between tenured engineers and young engineers. The tenured engineers want to keep a good reputation, meaning no security breaches. This

is why the sense of security and awareness is heightened in the restricted lab, but not as much in the open lab since the open lab contains no secure information.

In order to maintain this security, the restricted lab needed to have better communication. As seen in the EATPUTr model, communication has several different stages where data is processed to information, and information is turned into knowledge. If data, information, or knowledge is tampered with or affected at any stage, each stage thereafter is affected. This causes a huge issue in communication and security. The first stage of EATPUTr, the Event stage, also brings the context in. Since the context is happening in a highly secure and aware environment, the end result should also be highly secure and aware. If it is broken down at any point, the security is compromised. This event context includes emotions of fear and respect that heighten the senses. This heightened sense is the reason for a more structured environment, because the structure weakens uncertainty, thus increasing security.

From the described above components of information control, one can easily get confused on the interactions between all of them. The interesting aspect is really that they all interact at all areas. Emotions cause an increase in communications, causing an increase in security, making power differences apparent, opening up a move to make uncertainty less available, making it start all over increasing emotions. Each aspect plays on the others and causes changes in them. Each aspect is different for each frame described by Skovira [8].

So with emotions running high, masculinity in the air, uncertainty low, a collective team feeling, short term goals, power distance separating each of these, and communication clear, security is high. With this

secure feeling comes a feeling of responsibility and personal satisfaction. So it's no wonder that when the engineer leaves the restricted lab to move to the open lab, the open lab seems less secure. The engineer probably lets his guard down to relax for a bit!

REFERENCES

1. Geertz, C. (1973). *The Interpretation Of Cultures*. New York: Basic Books.
2. Hall, E. T. (1989). *Beyond Culture*. New York: Anchor Books. (Original work published in 1976)
3. Hofstede, G., & Hofstede, G. J. (2005). *Cultures And Organizations – Software of the mind* (2nd, ed.). New York: McGraw Hill.
4. Libet, B. (2004). *Mind Time – The Temporal Factor In Consciousness*. Cambridge, MA: Harvard University Press.
5. Norman, D. (2002). *Emotional Design*. New York: Basic Books.
6. Picard, R. (1997). *Affective Computing*. Cambridge, MA: The MIT Press.
7. Schank, R.C. (1999). *Dynamic Memory Revisited* (2nd, ed.). Cambridge, MA: Cambridge University Press.
8. Skovira, R. J. (2004). Using informational Landscape as a Model to Understand Information Use and Design Within Organizations. *Issues In Information Systems*, 5(1), 308-314.
9. Spradley, J. P. (1980). *Participant Observation*. New York: Wadsworth.
10. Thagard, P. (2005). *Mind – Introduction to Cognitive Science* (2nd, ed.). Cambridge, MA: The MIT Press.
11. Tipton, H.F., & Henry, K. (Eds.). (2007). *Official ISC² Guide to the CISSP CBK*. Boca Raton, FL: Auerbach Publications.