Security Report DePaul

Robert Fretwell 2023

1. Executive summary

1.1 Overview Of Exercise Objectives

The purpose of this exercise is to show that there are some weaknesses in DePaul's physical security. The test is to show that if there were someone from within the company who wanted to do nefarious deeds that they would have a relatively easy time moving and gaining access to many different machines around the school. Also, the test can show that a even if there person was not a worker that the data below would show that they to would have a easy time getting access to DePaul computers.

1.2 Methodology Brief

Few ways the exercise was conducted via working and non-working hours. Snice I work in IT I get sent on many different tickets during the day to help fixes staff machines during this time I would do a couple of things.

1 I would keep on eye on how I am able to get to the machine of question (if a user was leaving a machine for me to pick up was there someone there to make sure I was the right person picking up or was the machine just left for anyone to grab)

2 If I was going to an office how easy was it to get into the office was like was there a front desk that I had to speak to and I would write down if the front desk would just let me walk back or if they would call the person and make sure they were expecting me.

Also, during the work hours after I would get the job, I was on done I might would go to another department of another floor of that building and see if I could get to sit down on a random machine.

During work hours I would go around campus and do the same as above just in different areas

My go to was just telling the person that I was talking to a couple of line.

“Hello, I’m with IT to look at the computer for X reason in X location.”

“Hey, we are doing a routine check up and update on a couple of computers do you think I could gain access to those areas.”

Those are just a couple of examples of the social engineering that I would do to gain access to the areas that I wanted to get to.

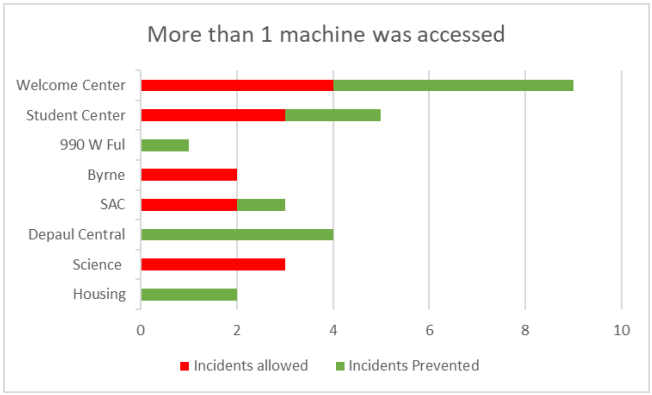
IF I WAS ABLE TO GET IN FRONT OF A MACHINE, I WOULD JUST DO WINDOWS UPDATES AND THEN TURN THEM OFF AND LEAVE NO DATA OR ANYTHING WAS MISSED WITH (The reason is I am not here to do anything bad this is all just to show because if someone really did want to do harm than getting in front of one machine that the school owns could be enough to do a lot of damage)

1.3 Key Findings and Implications

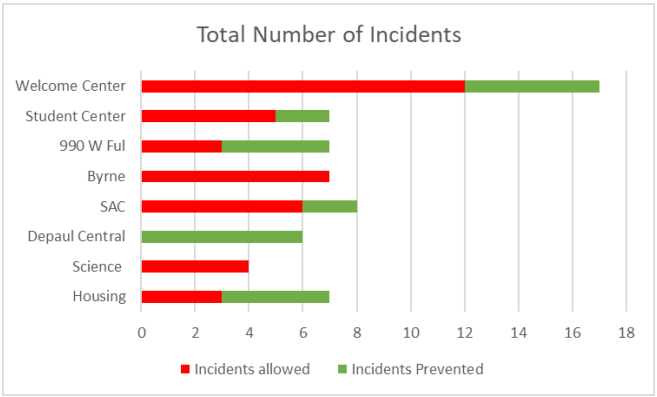
So after doing a couple weeks' worth of going around to different departments and locations around the school I am very confident in saying that there is 1 to much trust in who we are letting in based on them just saying they are with "IT" and 2 that there needs to be more checks in our physical security around the school and even though numbers are based on the Lincoln park campus I would imagine that the same is going on in the loop. The numbers below are just a week and a half of data collection these are events that I feel were the best for testing and really showing as there are many more events that were stopped or allowed below will be a chart showing different locations that I went to during work and while off to see if I was able to touch a machine.

The chart to the right show's incidents in which I was able to get access to 1 machine during the time that I was in the building. It shows that some departments like that of DePaul central being better at stopping people from just gain access to their machines which is a good thing snice they do deal with personal data and finances of students. However other departments like that of the welcome center did not stop to check once to see if I was with the school's, IT

department nor did they really check to see if the person I would claim to be seeing was aware of seeing me and thus they were never crossed check before sending me on my way.



The next chart *(Right)* shows all the times that I was able to get access to more than one machine during my visit and like the first chart shows the times that I was stopped and would leave as they were not letting be get to a machine. Here we still see that DePaul Central was 100% of the time checking and not letting me get to any machines that they along with housing. During the time of making this chart I would let the people know that I planned on messing with more than one machine so I would tell them that I was doing a massive update list and needed to get access to a wide range of their machines and this chart does show where the more problem areas are. Last chart is just a total number of attempts in each area and the allowed and stopped numbers of each just to give a summary of the data.



So what I will imply from this is that some departments are weaker and more ripe targets for someone who was going to do some bad things and the first target would be the welcome center as they were the one who happened to let me in the most but along with them Byrne

was not able to prevent me once and they happen to let me get into many different labs and other offices.

2. Importance

2.1 Overview Of Exercise Objectives

The reason that I wanted to do this was to show that physical security is just as important as digital security. More times than not it seems that many people and companies put a lot of time into making sure they are not able to be attacked from the outside world by making sure that their network is secure and that they heavily control who can connect to the networks but in many cases a lot of companies forget about the attacks that can come from inside the company themselves. There was a study done that shows there was a 47% increase in insider attacks from 2021-2023 many of these attacks are from personal gain for the employee either it be stealing sensitive data or sabotage and fraud. Making sure the proper routines and checks are set in place is the key to keeping attacks to a minimum. Just because DePaul is a university does not give it shield that stops it from being attacked. There are many reasons one might want to go after the school, there could be a disgruntled employee who wants to get back at the school or even student working trying to gain access to the grade database or even an attack on student and employee personal data there are many reasons that a university should be digitally and physically secure.

3. Methodology

3.1 Scope and Boundaries

There were limits to the testing done as I wanted to make sure to not be disruptive or destructive. One of the biggest rules I had set was that if I was able to sit down at a machine than I would not actually do anything to it at I would simply log in and log off or if there was a windows update that needed to be done, I would do that has this is just something people need to do more is update their computer. The main reason I wanted to set this goal was just in ensure that there was nothing that would happen to the typical machine and thus the school if I were caught big time than I would not actually get in trouble from breaking into computers. So, I also set rules for how I would go about doing the testing and that was there were just some places that I would not go to and that would be places like the President's office or anything dealing student activities like I did not see a use in trying to get into club areas. The main way that I chose the areas that I was going to "attack" was I was looking at where we get the most tickets from and from there I would just test those departments as there are many more areas of the DePaul that should and need to be tested however doing so for the entire campus would take months and months so had to narrow the scope to a couple of places that hold important and strategic importance to the school.

3.2 Execution Strategy

3.2.1 Social Engineering Techniques

(These attacks would be done off work hours) As states before in the first chapter I am a student worker for DePaul I work in the IT department, and I work mainly on staff and other administrative computers around the school, so I was not really impersonating anyone during the exercise. But I would determine my targets for the day, And I would show up at the building that I wanted to get on their machines I would look for any

offices that I could find. That I had not really be to before. After doing so I would simply walk in with my phone in hand, and I would open my works IT software (ServiceNow) which is how we get our tickets and talk to users. The main reason I would open the software was for both trying to get to a machine and it was a good excuse to leave if I had been caught. Most of the time there is a front desk in which I would say that I work with IT and ask if they could help me gain access to machines around the area or would they be able to get me in contact with someone who could, or I would even try to get on their front desk machine. While talking to people I would just tell them that I work for the schools IT and that I am there to do updates on computers or that I need to check out a printer in the back that went offline, After that it would go 1 of 2 ways they would either just accept the fact that I was with the IT department or they might ask who I was there to see or they might get suspicious because no one had told them there was going to be someone coming by and from there I would use the ServiceNow software on my phone and try to convince them that I was who I said I was and a good chuck of the time I would be let in to where I wanted and there was a number of times that people would stop me however, when I would sort of get found out there was no one to call security or to get someone to talk with me or to even figure out who I really was most of the time when I was turned down they would just saw they were not sure about it and that they would have to contact their boss first and then I would give some excuse about coming back later and then I would just leave and mark that data down for the day.

3.2.1 Other

(During work hours) I would not really go after computers but mainly just take notes and keep tracking of what could change during these interactions and if the interactions were secure and not just lazy and rushed. So for example I was talking to a user in the

housing department that need their laptop reimaged and they said that they would leave it with the front desk at Centennial Hall and that I could pick it up whenever. So I go to pick up that person's laptop and when I do I make note of the face that I was able to walk up to the front desk and talk the to student worker and all I said was "I am with IT and I am here to pick up a laptop for SOMEONE" I did not give the work my name or the user's name yet they simply handed me the laptop. Mind you I was not asked for an ID showing I am with IT, nor was I asked my name or who's computer that I was picking up. So, when something like this would happen, I would mark it as "Incident allowed" for the charts that appear in chapter 1.

4. Analysis & Recommendations

4.1 Vulnerability Assessment

4.1.1 Impact of no Identification

As a student work I have my student Id that is it I have no badge or anything showing that I work for the school thus when going around to work there is nothing, I can show off that lets others know that I am a worker. Thus, the school has gotten used to this, and it appears many other departments also do not have ID's which means the staff has gotten complacent to the fact that when another departments employee shows up to do work there is no thought of asking for their ID as many know this is not even a thing. Not having ID's is something that allows for me to easily get into to a place that I am not supposed to be as in many ways I am a ghost to many if the school had a ID system then it would be a oddity to see someone without one and thus it would lead to more people asking questions.

4.1.2 Impact of no Uniform

During work I am allowed to wear anything that I really want if it is not shorts and that it fits reasonable means (no obscene words, nudity, gore) therefore I and many other IT workers blend in with everyday students and guest. This is nice for those who are working as we are comfortable in what we wear but it sets bad standards around the campus as now those who are our lines of defense against people getting into restricted areas fall behind as now they are accustomed to every coming and going to be in “plan clothes” and thus it makes it harder to tell who is working and who is meant and not meant to be in the locations that they are in. We are given DePaul IT departments collared shirts however it is not required that we wear them and the other IT departments are not required to wear their DePaul Shirts either so that Is at least 20 workers who go around the school to areas that are off limit to students and these workers look like any other student and this needs to be fixed.

4.2 Risk Evaluation

4.2.1 Potential For Data Breaches

Allowing anyone access to a machine around campus might not seem all that bad at first however, Someone who is skilled and knows what they are doing and looking for can turn a machine in a random office or conference room into a staging point for a massive attack if they are worker than all they would have to do is log in and then they would be able to run software or to give themselves access to that machine as an admin if they do not already have it and from there they could install things like a worm on the network that slowly starts locking the school out of data or they could start digging around for data on the network and doing many other “man in the middle” attacks which allows

them to see data being sent without the sender or receiver knowing they could also if the machine of someone with sensitive documents this attack could install a simple keylogger which would allow them to see all keys the victim is typing giving them passwords to things like Bluesky and other websites/services used at DePaul.

4.2.2 Potential Damage from Malicious Insider

Damage that could be down by an insider ranges but the avg insider attack typically causes around $756,000 and which that is the avg for a private company that is with someone stealing company information with a university the number would be much higher as dealing with student private enough the school could be held liable for not doing enough to protect their students info and thus not only would they have to pay for the workers that would need to fix the issue but they would be up for lawsuits which depending on how many students were affected and what damage was done to the student the school could easily be looking millions of dollars in damages due to just 1 attack

4.3 Security Protocol Changes

4.3.1 Identifications for Staff

This solution would make a big difference within security measures in the school. All workers be it full time and student works would receive a badge that shows which department they work for or snice everyone who works for the school there could be a system in which when workers need to go places there would be a scan system that would then cross check our Microsoft Azure database and make sure the person has a staff tag and then this would make sure that there is a way to determine that people are

who they say they are and that someone who works in ID services is not going around pretending to be in ClassLabs. Neither of this would be costly to the school the second chose would most likely be the cheaper option but either or would be much better than the system that we have now which is no ID checks period.

4.3.2 Regular Security Training

This might seem like common snice that employees should receive training and that is true we do get training via little modules in which you watch videos and then take test however the training that we normally get are on sexual assault and things like mandated reporter we do get some training on that of security in the school but the main focus of these tend to be on that of phishing emails and other similar things I would say there should be a focus on training for front desk works and other staff to spot suspicious activity not only from students and guest but from other workers people should be more aware of what is going on around them and front desk workers should be better trained and equipped to deduce who they are talking with actually being allowed to go in the areas they are requesting to go.

4.3.3 Front Desk Expanded

There should be more areas in which workers cannot just scan into a get access to machines that are not supervised or there should be at least one stop made before getting to vulnerable machines. This would require more front desk and works that would be the first line of defense and mixed with the above training these front desk would act as in stop gap in which the person wanting access to said area then speaks to someone at the front desk and would show ID and then the person would be supervised

by someone or would need to show other proof of what they are doing is something was actually requested.

4.3.4 Supervision

In my time working here going to tickets it is not required that a user be there when I am working on their machine and I understand that this allows for better time management all around and many more tickets are able to be done at once as long as there is someone to allow access to the machine in question the worker can log in on their own and get to work. I think there should be policies that change this and if you need your machine worked on than it should be required that you are in the room with the worker and this just cuts down on many things it is hard to do malicious things when there is someone watching you and thus it adds more defense to the school however this might cause schedule issue and would be impactful on ticket completion and time. There could also be polices that there be more than one worker that has to responded to a ticket as to have someone else there and thus the attacker is being watched.

4.4 Follow-Up Actions

4.4.1 Regular Audits

Either using a existing security department or create a new one that their job is to look into actions of workers to double check people are going where they are supposed to be and checking ID swipe logs checking network usage and over all these audits should cover the entire cybersecurity spectrum from digital to physical and also they should be on a rotating/random schedule to make it harder for attackers to plan around this

checks. The more eyes there are looking at what is going on the better as there is someone who might catch something off and stop a major attack for going off.

4.4.2 System To Report Suspicious Activity

Allow for an anonymous or non-anonymous reports in which workers can file reports in which they thing someone might be up to something malicious with the training and all this system would allow for workers to go online and file reports about what happened at what time and at what location and then the security department would do an audit of that day to see what all was going down snice this department cannot be watching everything at every moment nor can they be everywhere at one time this system would allow for everyone around the school to become the eyes and ears for this department allowing for more protection all around and thus all it takes is one report and investigation to stop an attacker from getting what they want.