Site Assessment:
Cummings Library

Name: Brendan Ancheta
Date: August 8, 2025
Course: CYBR10003 - Asset Security

Name of site:

Cummings Library and Collaboratory, Building C, Mohawk College

Location:

135 Fennell Ave W, Hamilton, ON L9C 0E5, Building C

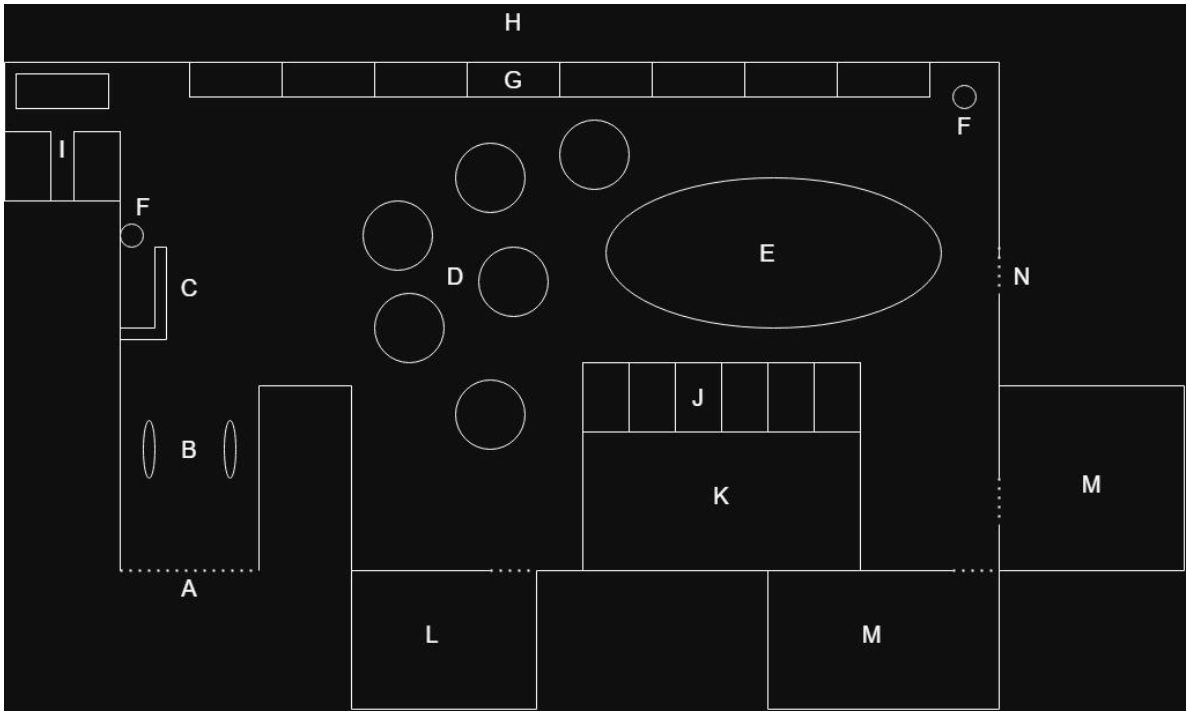
Introduction:

This is the primary library for students at Mohawk's Fennell Campus. On the first floor lies the library proper, which is kept as a quiet area for students and is where they hold their physical books and computers for use, as well as have various side rooms and private spaces available to students. On the second floor is the collaboratory, which is a more public space with computers and desks, as well as some big screens you can plug personal laptops into to display to a group of people. I focused my site assessment exclusively on the first floor however, as there seemed to be more than enough points of interest within to cover a report. Even only being one room there were several assets to consider, such as all of the machines, more than one point of entry, and of course all the books being openly available once inside.

Procedure:

Overall there was not much ground to cover, though there were several points of interest. After an initial walk around the floor, noting the layout and what was there, I went back through and took photos of important assets. I didn't get a chance to go into the side rooms, but otherwise I was able to photograph most of the premises. I asked the one staff member present at the time after photographing to confirm the number of cameras present being 2, which from their knowledge they affirmed as correct.

Site Sketch:



A) Entrance to the Library - Near the front entrance of building C at Mohawk
B) RFID Scanners - presumably RFID are on books
C) Front desk - Was occupied during open hours
D) Computers - Around 3-4 computers on circular desk; wiring was exposed though computers themselves seemed to have basic wire locks on them
E) Bookshelves - Only went up to waist level
F) Cameras - Confirmed with staff there were only the 2 shown in the diagram
G) Desks - Along the side of the library facing the front of the building; walled with windows on the whole side
H) Front of Mohawk Fennell Campus - Clear view of Fennel Avenue
I) Private Cubicles - Available via booking
J) Desks - Separated with dividers
K) Cubicle(?) - Was unclear on what this section was for; walled off but walls didn't reach the ceiling, could be storage
L) Room with unknown purpose - Would need to go back and investigate further; was left open but with what was inside it did not look like it was necessarily for the public
M) Silent Study Rooms
N) Emergency Exit - Fire alarm located beside the door; unsure where it led but looked like a staircase

Points of Interest

1. Entrance

The library is still just a room within a building, so there are 2 primary points of entry to consider. The main one of course being the actual library entrance, as we see has electric sliding doors, activated via motion scanner. Most sliding doors are not inherently the most secure, and I could not notice any obvious locking mechanism on it. Granted, it most likely has at least some form of lock on it, however how secure it is I can not say. The worst case would be that they simply deactivate the door during closed hours. This is still a public space, with staff at hand being able to watch over, so I could imagine the security of this specific door may be less of a concern. While not properly a part of the site assessment, it is also worth considering the entryways to the building as a whole, with the above photograph showing the closest exterior public entrance, having two sets of double doors with crash bars and mullions. While I did not document it officially, there are shifts of security guards roaming the campus, and cameras throughout the building. So, while I can't directly speak on the security of all of building C, it stands to reason there are standard physical security measures in place at least throughout Fennel Campus, which would add to protection against unauthorized entry to the library, regardless of the actual library entryway security. On top of this, outside of closed hours this is not a location that would want to constantly bar entry, given its purpose is for people to have free access to it

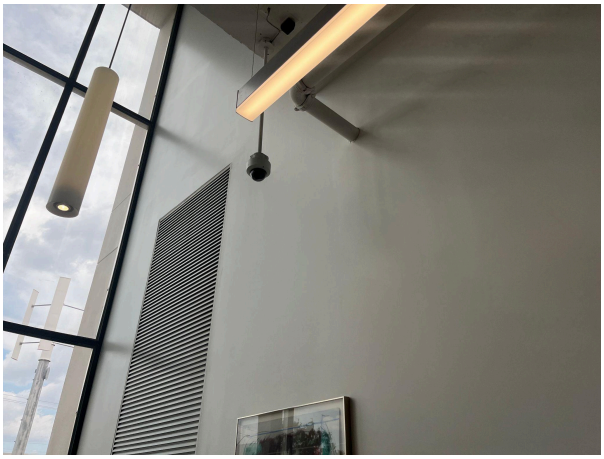
Risk: Low

2. RFID Scanners

As seen in both the above photograph and the last section, these are positioned right by the entrance beside the front desk. Granted, RFID scanners like this often do very little in actually preventing theft, due to their unreliability and many methods of attack against them. At the very least, since it is positioned right by a staff member it will be easy for them to notice if it were to go off. It does still provide general determent from theft with its presence, and the only real detriment it could pose is causing a sense of complacency in staff who rely on it to detect when a theft occurs, rather than keep an eye themselves. Overall though it most likely provides little harm to keep in place, even if it does not provide much benefit either.

Risk: Low

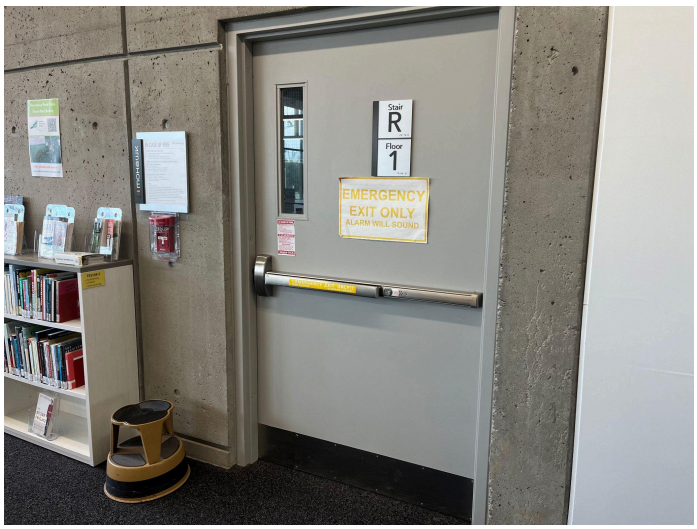
3. Cameras



There were only two cameras throughout the library. However, they were positioned in opposite corners of the room, so they most likely cover the entirety of the site, just based on their locations. While I did not properly confirm this, it is likely these cameras provide their feed to campus security rather than the front desk computer, as it would there would be little reason for that, as well as the fact it would provide a vulnerability in unauthorized access should someone without proper clearance have access to the footage of these cameras. Both cameras remain quite high up, making them hard to physically obstruct, though the one by the front desk is closer to the ground than the other one.

Risk: Low

4. Emergency Exit



This is the only other “point of entry” outside the main entrance. Granted, there should never be a reason someone would enter the premises from here. Most emergency exits often have alarms tied to them when opened, so of course I was not about to open it and see what lay behind it. What I did notice through the door window was a flight of stairs, and most likely there would be an entrypoint leading outside nearby, but that was not in view. The fire alarm was also beside, also having a case on it that when opened would also set off an alarm. If someone were to try to break in through this door, I would fail to see how it would be any easier, if not be more difficult, than the main entryway, as directly across the room lies one of the security cameras with a direct view of it.

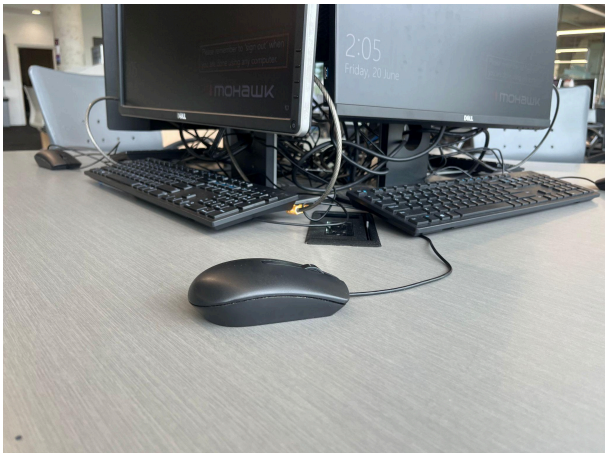
Risk: Low

5. Front Building Window

A large portion of the library walls are made of glass, of course adding to the aesthetic of the location, but more importantly it provides a lot of points of view from both inside and outside the building. Now glass is generally less durable than dry/brickwalling to brute force breakage attacks, but that doesn't make it necessarily easy in general to do so. This wall is positioned in a public area across from a road with regular traffic going through, so any attempt to do so would be easy to spot, on top of the cameras inside easily being able to catch any attempt. That said, the easy visibility from the outside does make this prone to those attempting to scout out the location from a distance to lower chances of suspicion around them. Of course this is a public location that pretty much anyone can freely access, but this still adds to the susceptibility of one being able to unknowingly gather information on the location for malicious purposes.

Risk: Medium

6. Computers and Open Wiring



Being a library, there are of course various computers available for use to those coming in. These are mohawk college machines, so to login to them you do require mohawk credentials to access them. After logging out of these machines, they will wipe any local downloads and changes made during use, resetting back to its default environment settings. Now these machines do have locks in place to help prevent theft. However, as seen in the second photo the wires are very much exposed. While there isn't much value to simply stealing some computer wiring, this does leave them exposed to attacks to damage/destroy them. While it was unclear to appropriately tell, if any wiring plugs/outlets are exposed, this could lead to certain vulnerabilities such as keyboard/mouse jacking. Compared to many other computer setups on campus, this is one that has the most open exposure.

Risk: Medium

7. Wifi/Router

There is of course campus wifi available within the library, and as shown on the picture the router for it lies on the ceiling, which is standard across campus. This makes it very difficult for access, which helps in preventing a threat actor from performing a form of physical attack against it. As for the publicably available networks, there is the main wifi, 'Mohawk Wifi', for Mohawk personnel, requiring login credentials, and then there is the Mohawk Guest, being available to the public without requiring credentials. While it may not present a direct threat to the library, any public wifi can always be a vulnerability to those using it, so there is still some potential hazard in its general existence.

Risk: Medium

8. Silent Study Rooms and Other Connected Rooms

I did not get the chance to take a direct photo of them, these rooms lie across from the front window as shown in the sketch. While I am unsure what exactly lies within them, considering there is probably some expectation of privacy to a degree within them, I would believe there to not be any cameras within them. The cameras within the main library have view points of them, but given their angle in relation to these rooms it would most likely be only enough to view who is coming through said rooms. Assuming these rooms indeed don't have cameras within, they would prove to be a blind spot within overall surveillance. I was able to observe a window within at least one of these study rooms. So potentially, were there someone who would want to gain unauthorized access without detection, this may be the best location to do so from.

Risk: Medium

Recommendations/Weaknesses:

1. RFID Scanners by Entrance

RFID scanners are often an unreliable form of theft detection, and as mentioned before there are various possible attacks on them. One common knowledge attack is wrapping whatever has the RFID tag in tinfoil to avoid setting it off, which could easily done in this case by a student, by lining their backpack with tinfoil prior to coming. Now it is not a direct detriment to have RFID scanners, as they can potentially deter attackers with their presence, even if it may be minimal. However, these scanners should not be used as a reason for library staff to be complacent in monitoring for theft, nor should they ignore situations where it does go off and they treat it as a false positive. At the very least, the cameras within the location help to cover detection requirements for security, and rather it should be noted if there are any blind spots within these cameras and the proper adjustments should be made to rectify that, should the library desire greater detection capabilities. Should someone be able to bypass the scanners while also not alarming staff, the amount of assets they could steal would most likely be minimal in value, as they would have to be small enough to hide in a bag and avoid detection. Though certain books kept at the library could potentially cost hundreds of dollars each, such as an encyclopedia, and if theft is repeatedly occurring the costs could add up.

Risk: Low to Medium
Cost: Low to Medium

2. Staff Members on Premise

Majority of the time there seems to be only one staff member on premise at a time who is heading the front desk, and therefore monitoring the library. There could of course be other Mohawk staff using library facilities there as well, but in terms of actual managing staff for the library there seem to be few at a given time. However, the location is not necessarily large, and primarily the staff at the front desk's primary duty is to allow people to rent out library assets and answer questions, so whether more staff would really be needed is up for debate. However, as mentioned in my procedure, when I approached staff to ask about the camera quantity, while I did explain the reasoning for my question, there was no pushback or further authentication asked to be given. Granted, they were familiar with students doing this project at the time, but it still could have been very possible for me to continue investigating further as I experienced very little pushback. Should I have been lying it would have been quite easy to confirm more details about the basic library security. In comparison to another site I had also considered, when I had asked this other business I wanted to take pictures of their building for a school

project, they at the very least told me to contact the owner before doing so. Meanwhile I was able to walk in the library uninterrupted, openly taking various photos across the location. While this is not necessarily a site that would require staff to thoroughly confront and authenticate an individual's intentions, an improvement to this potential weakness could be made by some basic training being provided on properly monitoring and inquiring into any form of potentially suspicious activity happening within this location. This could even be as simple as an announcement company-wide to bring attention to it, should they not want to invest too many resources into this.

Risk: Medium
Cost: Low

3. Open Wiring

As mentioned with the library computers, my photo showed a significant amount of wiring exposed, with potential access even to the outlets they were plugged into. In regards to the outlets however, this was not fully confirmed, however at the very least the wiring was very much out in the open. Now, the computers along with their hardware were secured with standard cable locks commonly used for securing physical assets in place. The keyhole for the locks was not easily visible, so while I can't confirm the pick-resistance or type of lock just with the factor if it being not noticeably accessible is a benefit, nor is the lock itself going to be easily destroyed with proper tools. However, since the wiring itself, while not exactly prone to being stolen, is open for easy access, anyone could easily go around cutting/damaging all of the wiring if they wanted to commit harm to the property directly. While most computer wiring is not individually expensive, should multiple wires, or wiring directly attached to other more expensive hardware be damaged, the costs of this risk could rise. Now the likelihood of this is probably not that high, especially since it would be very easy to catch. But the ease of access still makes this a risk of occurring should someone decide to do so. This could be resolved by using tables that instead have a closed off hollow section that can be secured, in which the wires can be housed more safely. Realistically the costs of table may not be that high, but it was also most likely require a redesign to some extent of the library floor plan

Risk: Medium
Cost: Medium

4. Mohawk Guest Wifi

This risk is more of an obligatory one, as there is always some form of threat in regards to a public wifi network. Being available to access to anyone on location of the library, should proper networking safeguards be in place, this could pose a significant vulnerability to Mohawk systems. This is not something I am capable of discerning properly of course, due to not having access to in-depth knowledge of Mohawk's IT infrastructure. However, there are other forms of threats, such as malicious actors creating their own public wifi with similar looking credentials as Mohawk Guest, with the intent of tricking people into using it without realizing it is the wrong network, and most likely exposing their information to the attacker. This is, however, more of a concern with the greater whole of the entirety of Mohawk to consider, rather than a problem of the library in particular, and IT functionality is not something that would be within direct control of library personnel. A potential way to help mitigate risk of users of the library attempting to gain access to wifi, is instead have staff be informed to recommend to people coming into the library to instead make use of the machines there, and especially if they are student or staff of Mohawk to recommend they use the proper wifi network that requires credentials to login. The total risk and cost of this potential issue are fundamentally hard to gauge, as they more so lie go beyond the scope of the library and exact details on the guest wifi's security is not necessarily publicly available knowledge, so the values of both could be skewed in either direction based on several publicly unknown factors.

Risk: Medium to High*
Cost: Low to Medium*

Conclusion

Overall, many of the points I deemed as potential risks are not huge concerns, and as a whole the location has sufficient security for the purposes it holds. While it houses various potentially valuable assets within, and is easily accessible by almost anyone, due to being a public space with many points of detection it would most likely be difficult to perform malicious activity without potentially being discovered. Even if there is little barring entry and exit to help defend directly against unauthorized access, the library itself lies within the Fennel Campus building, with even further methods of detection to avoid, as well as regular security patrols across campus, as I often walk past at least one security guard making rounds whenever I am on campus. In the end, this is a public space that intends for it to be easily accessible to both enter and use its facilities, while there are potential items worthy of theft within, the total value of assets would most likely pale in comparison to many other private businesses, even other libraries. For the purposes of this location, while the points I outlined for improvement could help in augmenting this location's security further, rather than being necessary to achieving acceptable security level, it would simply aiding in refining the current systems in place.