Physical Security Audit
Findings and Recommendations

Prepared for: [redacted]

Prepared By: Full Scope Security, LLC.

Date: 10 December 2023

Table of Contents

1. Executive Summary

This report provides a detailed overview of the findings and recommendations from the physical security audit conducted by Full Scope Security, LLC (“Consultant”) on behalf of [redacted] (“Client”) conducted between 27 OCT 2023 and 10 DEC 2023. The objective of this assessment was to evaluate the Client’s physical security posture by simulating real-world attacks.

Key finding highlights include critically weak external-facing access controls, little to no access controls for internal areas once inside, weak employee awareness / training, and weak controls protecting cash and other valuable assets.

High-level recommendations include fortifying external-facing points of entry, securing and segmenting internal areas especially after hours, training employees on security best practices, and securing cash and other critical assets inside the building.

2. Introduction

As discussed in pre-operation planning and scoping meetings, Client’s main concern was to find and resolve the “low hanging fruit” security issues that rely on low-skill attacks and do not require heavily nuanced or specialized tools or skill sets. As such, the scope of testing was generally limited to those more simple types of attack vectors, with adjusted scope for some social engineering tests as outlined in the statement of work (SOW-1).

The assessment was conducted in accordance with industry best practices and followed a scope and methodology as defined in the statement of work (SOW-1) and operational plan (POD-2).

Client website ([redacted]) was tested for common vulnerabilities.

Objectives, more completely defined in the Mission Goals List (POD-4), are listed below, along with brief notes on the success of each goal:

- Gain unauthorized building access and take photos of vulnerable equipment to simulate a physical data breach.
    - **Success** - gained unauthorized physical access to the building

- Gain unauthorized physical access to management's offices and workstations.
    - **Success** - gained unauthorized physical access to the management offices

- Implant keylogger device on management device.

    - **Mixed success** - no management devices present to attack, but keylogger successfully implanted in employee workstation

- Obtain unauthorized access to management workstation.
    - **Miss** - no management workstations present to attack

- Obtain physical access to mech shop, stock room.
    - **Success** - gained unauthorized physical access to these areas

- Obtain physical access to key box and cash boxes.
    - **Success** - gained unauthorized physical access to building keys and cash box

A brief outline of the top 4 most easy or affordable immediate fixes is below (section 5.3 in this document includes a full Phased Implementation Plan):

1. Add Double Door lock (to only be locked at night after closing)
    a. If Consultant had not been able to get into the Double Door, other security flaws inside wouldn't have been *as* critical
2. Add shielding to cover Double Door gap
3. Adjust camera angles to provide more complete coverage
4. Train employees on security awareness and proper lockdown procedure at close

3. Findings

3.1 Physical Security Assessment

NOTE: The alarm system was considered out-of-scope during this engagement, and Client provided a keyfob to Consultant to disable the alarm system. While a fob was provided to Consultant prior to the engagement as indicated above, it should be noted that there was an easily-accessible fob to disable the security system in an unsecure area of the building. This fob could be used by an attacker to disable alarms without knowing the security code.

3.1.1 Initial Building Entry

Three entrances to the Client's site were identified. Figure 1 shows what the Consultant refers to as the "Front Door", Figure 2 shows what the Consultant refers to as the "Double Door", and Figure 3 shows what the Consultant refers to as the "Employee Door". While Figures 1-3 (below) were retrieved from Google Maps as part of initial reconnaissance and there have been alterations made to the building since the photos were taken, the Figures are similar enough to the Client's current building layout to be acceptable representations.

Figure 1: Front Door

Figure 2: Double Door

Figure 3: Employee Door

3.1.1.1 Front Door

The Front Door is in a well-lit area of the building's East perimeter, and directly faces a strip of well-populated stores across the street. There is a camera in the window above the Front Door. The lighting, camera, and positioning of this door are moderately to highly likely to deter an attacker from attempting entry through this door. However, it should be noted that despite the heavily-trafficked area, there was no undue attention made to Consultant, nor any authorities called, as Consultant was attempting entry through this door, despite the obvious efforts to forcibly enter the door without a properly authorized key. The Front Door's security is moderate, and the pins of the lock were noticeably sticky, likely due to lack of normal use (locking from inside instead of with key) and exposure to the elements. Consultant attempted single-pin picking, raking, and using a lockpick gun to gain access, all of which were unsuccessful. This does not indicate that entry via picking through the Front Door is impossible, but that the state of the lock core and pins simultaneously provide an extra layer of difficulty and add the possibility of breaking the lock or getting a tool stuck inside the lock. Due to these risks, Consultant ceased lockpicking attempts on the Front Door after approximately 20 minutes. Consultant also attempted the use of a "J-Tool" (a.k.a. "Thumb Turn Flipper") to reach through the gap of the door, but was thwarted by an overlapping piece of metal (Figure 4, below) that did not allow the tool to pass through the gap, even with air wedges deployed to widen the gap.

Consultant's efforts to enter through the Front Door were unsuccessful.

Figure 4: Metal overlapping strip on inside of Front Door

3.1.1.2 Double Door

The Double Door is in a moderately to poorly lit area of the building (some lights present, but relatively dim), with some additional concealment provided by the nearby dumpster and trees. The door is along the South perimeter of the building, several feet from the Eastern perimeter. The same populated stores to the East referenced above for the Front Door are also visible from the Double Door, but to a lesser extent. There is a camera above the Double Door on the Southeastern corner of the building, but its angle is not effectively watching the area in front of the Double Door (more detail later in section 3.1.2 Cameras). The lighting, positioning of this door, and the misaligned camera angle are unlikely to deter an attacker from attempting entry through this door. The Double Door does not have external handles or locking mechanisms, which increases difficulty of entry. However, Consultant was able to deduce that the door was likely operated by crash bars on the inside and was possibly left unlocked due to fire code rules. The gap between the doors was able to be widened by air wedges, which provided a clear sightline into a large area of the building, as shown in Figure 5.

Figure 5: View through the Double Door gap widened by air wedges

This opening and sightline can provide critical information for a potential attacker. With the gap widened, Consultant was also able to fit a “Double Door Tool” through the gap to reach around and manipulate the crash bars (Figures 6a and 6b).

Figure 6a: Consultant reaching through Double Door after widening gap with air wedges

Figure 6b: Inside angle of the Double Door Tool hitting the crash bar

After some manipulation, Consultant was able to successfully engage the crash bar and open the Double Door (Figures 7 and 8 below), gaining unauthorized access to the building. Another possible method of entry to the Double Door is via removing the exposed, insecure, external-facing hinges and walking the door off the frame entirely. Consultant did not attempt this method due to its general 'destructive' nature, but was able to determine that the hinges are vulnerable to this type of attack from an attacker less concerned about maintaining the integrity of the door during the attack. Overall, the Double Door is the most vulnerable external entry into the building. The lack of security on the door, a general lack of deterrents, and a misaligned nearby camera all work to make this door the *most likely point of attempted entry for an attacker*.

Consultant's efforts to enter through the Double Door were successful.

Figure 7: Double Door successfully bypassed with air wedges and Double Door Tool

Figure 8: Consultant with the Double Door Tool and air wedges after having successfully bypassed the Double Door

3.1.1.3 Employee Door

The Employee Door is in a well lit area of the Southern building perimeter, near the West edge of the building. This door is not easily visible from the surrounding areas due to a restaurant to the West, and trees to the South and East. Figure 9 shows the sightlines blocked by nearby restaurant and trees.

Figure 9: Employee Door visibility blocked by surrounding environment

The lighting is a potential deterrent for an attacker. The door is locked by an electronic access control panel to the right of the door (Figure 10). A nearby camera on the Southwestern corner of the building and a camera on the access control panel are also potential deterrents. Another camera not owned by Client on the restaurant building's corner also acts as a deterrent. Overall, despite the large amount of concealment, an attacker would be moderately likely to be deterred by the nearby cameras and strong lighting. One possible method of entry to the Employee Door is via removing the exposed, insecure, external-facing hinges (also visible in Figure 10) and walking the door off the frame entirely. Consultant did not attempt this method due to its general 'destructive' nature, but was able to determine that the hinges are vulnerable to this type of attack from an attacker less concerned about maintaining the integrity of the door during the attack. This type of attack may be mitigated by the door's magnetic lock, unless the attacker is also able to disable the magnet or slip a disruptive item between the magnetic poles to reduce its effectiveness.

Figure 10: Employee Door, showing access control panel and exposed insecure hinges

Another type of attack on the Employee Door would involve tampering with the electronic access control device, which initial reconnaissance identified as a Ubiquiti Networks UA-Pro-US UniFi Access Reader Pro (Figure 11).

Figure 11: Ubiquiti UA-Pro-US webpage from initial reconnaissance

Cloning of an employee's NFC fob is unlikely to be successful due to the MIFARE DESfire encryption used for authentication confidentiality. This electronic access tampering attack would likely only be attempted by a highly skilled, dedicated, and well-equipped attacker. As such, with the scope of this engagement predominantly focused on the low hanging fruit attacks, Consultant did not dedicate significant effort to bypassing this device. One way that the electronic access control could be easily surpassed, however, is in the circumstance that an attacker finds a lost or stolen employee fob and is able to easily enter the door under 'traditional' non-tampered use of the access control system. Additionally, even if an attacker is not skilled in access control bypass, they can still remove the UniFi Access Reader Pro from the wall with an easily-accessible T6 security screw on the bottom of the unit. Removing the unit from the wall would expose the unit's back panel where an attacker could remove the Ethernet cable which is providing power and data. The attacker could then try further access control attacks with access to the live wire, or could merely steal and sell the fob reader itself.

Consultant's efforts to enter through the Employee Door were unsuccessful.

NOTE: While attempting to bypass the security system was out-of-scope in this engagement, Consultant did test some of the system's controls. Critically, Consultant found that the entry sensor on the Employee Door and the motion sensor inside the hallway near the Employee Door were not triggering the alarm system. Consultant tested this via multiple methods, including quite simply putting the alarm on Away mode, waiting for the system to show as fully engaged, and then opening the door and walking / jumping in front of the motion sensor. None of these tests showed that these sensors were working. **Consultant recommends immediate review of all of the security system's functionality.**

3.1.2 Cameras

Generally, there were many cameras inside the building and on the exterior with what appeared to be moderately effective camera coverage. Several cameras were not at optimal angles to capture the most-likely exterior security vulnerabilities, as shown in Figures 11a, 11b, 12, and 13.

Figures 11a and 11b below show the camera pointing towards the employee parking lot, positioned on the Southeast corner of the building (the same camera referenced above the Double Door in 3.1.1.2). This camera is not able to see the area directly outside the Double Door, providing a blind spot for attackers to take advantage of. The angle of the camera is catching too much sky view, reducing the amount of relevant information in the picture.

Figure 11a: Exterior camera view on dumpster side (Southeast)

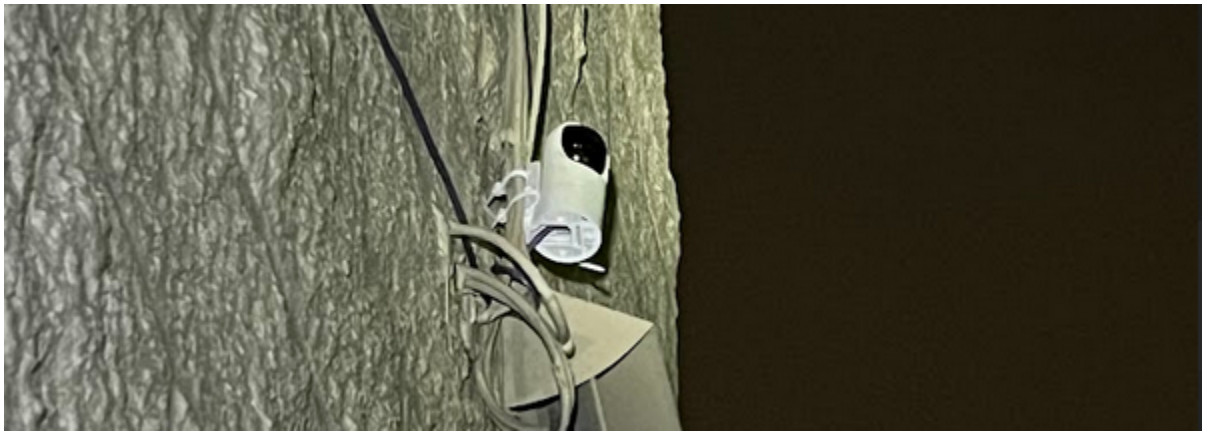

Figure 11b: Outside view of camera, visibly misaligned with bad viewing angle

Figure 12 below shows a camera pointing towards the employee parking lot, positioned on the Southwest corner of the building (the same camera referenced above the Employee Door in 3.1.1.3). While this camera is angled slightly better and more downwards compared to the camera in Figures 11a and 11b, this camera still does not provide a very clear view of the area

in front of the Employee Door with fob access. This camera would still likely be able to capture the presence of an attacker, albeit with little detail on the image.

Figure 12: Exterior camera on restaurant side (Southwest)

Figure 13 below shows a camera pointing towards the guest parking lot from the window above the Front Door (the same camera referenced above the Front Door in 3.1.1.1). This camera's view is obscured by the bright exterior lights and the general smudges and dust on the window. Additionally, the angle of the camera would not effectively capture a detailed view of an attacker attempting entry through the Front Door.

Figure 13: Camera in window above Front Door

The interior cameras have a fairly complete view of the building (Figure 14, below), which partially mitigates the possibility of someone entering the building out of sight from the cameras in Figures 11a, 11b, 12, and 13, but is not a perfect resolution to these misalignments.

Figure 14: Overall camera panel, showing all available camera views

3.1.3 Internal Security

In general, the physical security on the interior of the Client site was minimal, even completely lacking in some areas. Once entry was made into the building overall, there was very little to stop a potential attacker from accessing business-critical assets, documents, and areas.

3.1.3.1 [redacted] Office

The door into [redacted] office did not have a lock on it at all (Figure 15), so once entry was made into the building overall, there was free access to [redacted] office.

[redacted] office contained several assets that seemed important or business-critical including, but not limited to: financial and healthcare related documents (Figure 16), production servers for the business (Figure 17), the controller for the security access control system (Figure 18), the NVR for the camera system, a computer setup for [redacted], several sets of keys (Figures 19a and 19b), a Simplisafe fob for the building's alarm system, and other valuable equipment such as a 3D printer (Figure 20).

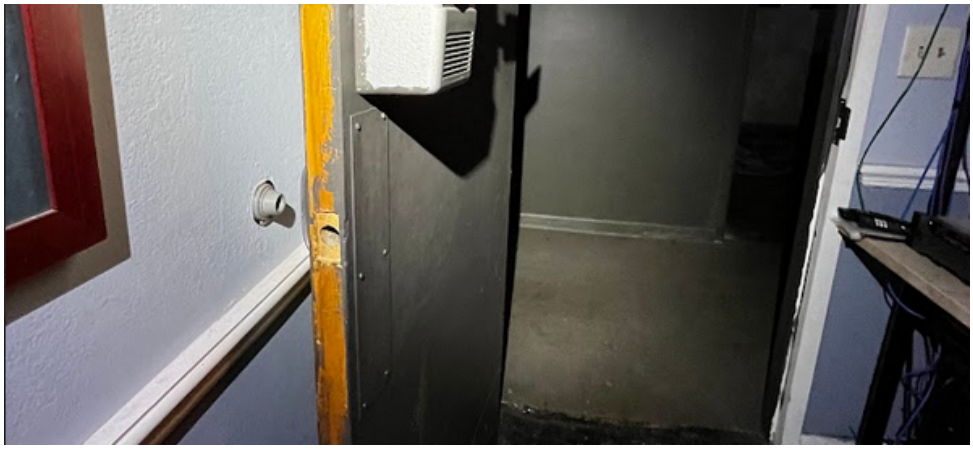

Figure 15: [redacted] door, left open and lacking a lock

Figure 16: Private documents in unlocked storage area of unlocked room

Figure 17: Production server

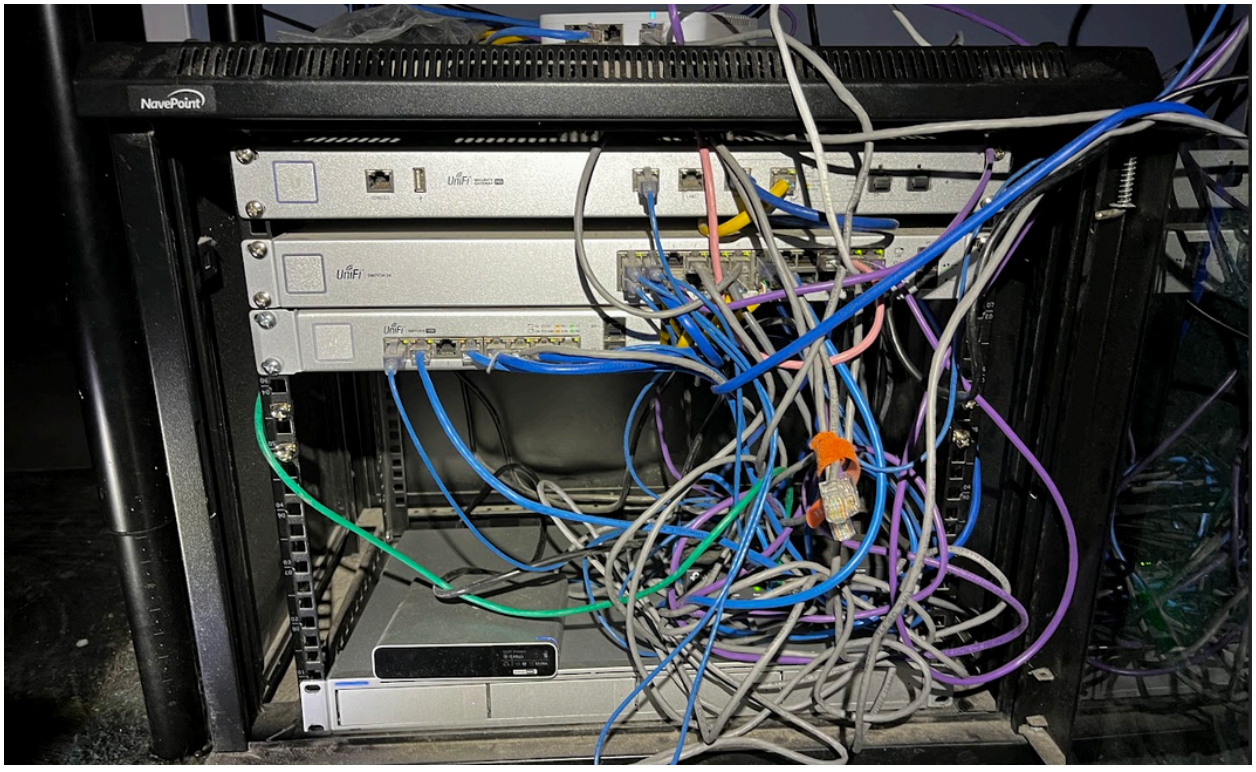

Figure 18: Security system and NVR for Cameras

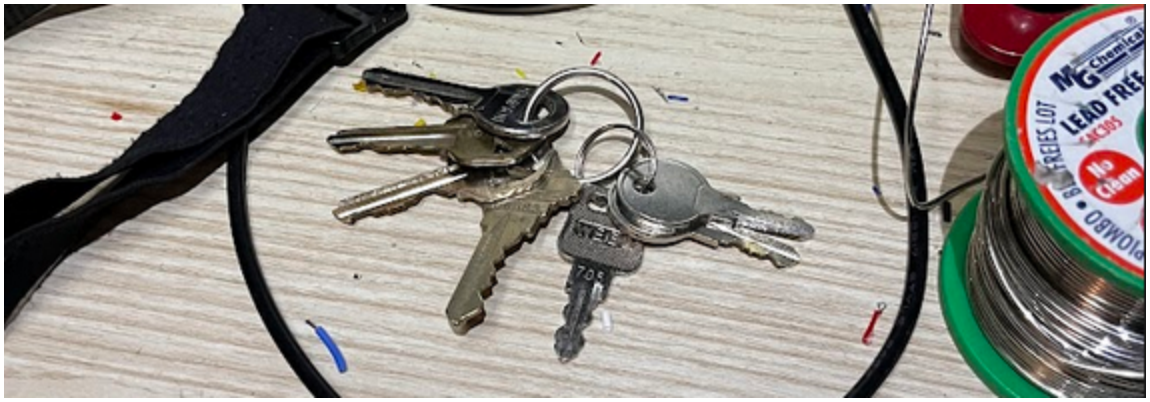

Figure 19a: Keys in [redacted] office

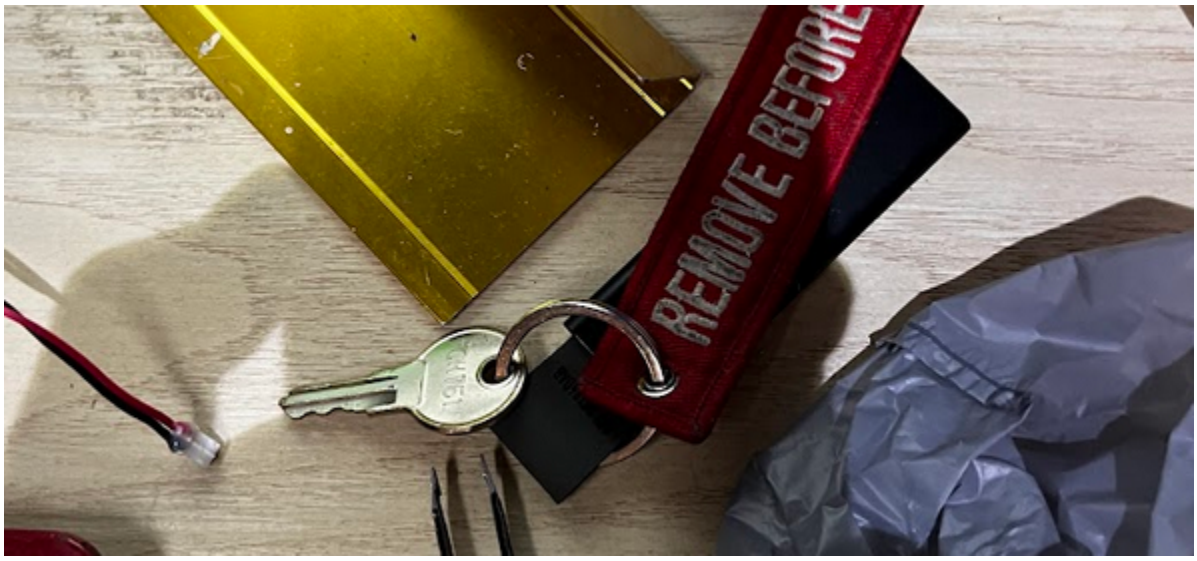

Figure 19b: Keys in [redacted] office

Figure 20: 3D printer in [redacted] office

3.1.3.2 Manager's Office

The door into the Manager's office appeared to be the most secured area of the interior of the building. The door is secured with a biometric lock (fingerprint scanner). However, to ensure that no one is locked out if a battery dies, there is a keyhole backup "hidden" behind the fingerprint scanner that can be easily accessed to be picked (Figure 21). In addition to revealing the keyhole, sliding the biometric scanner's front plate to the side also reveals some screws that may allow an attacker to access the internals of the lock and critically bypass the security. Consultant did not attempt this method, as it could be considered 'destructive'.

Consultant was able to use a plastic shim card to completely bypass the lock by reaching through the frame of the door and pushing the latch back to an unlocked position. Upon further examination, Consultant found that the locking mechanism does have a dead-latch, which should protect against such shimming attacks if installed correctly. The success of the shimming attack indicates improperly fitted doors/locks that do not engage the deadlatch at all, rendering it useless in this instance.

The Manager's office did not appear to contain any critical-level assets, as it appears that both managers bring their laptops/tablets home with them after work. However, several items of interest were found, including but not limited to: general business documents, client contract documents, and a safe (empty) that had the keys inside the lock.

Importantly, Consultant noticed that the Manager's Office contained a document shredder, which is a positive security feature that reduces the usefulness of dumpster-diving reconnaissance strategies by attackers trying to learn information about the company or its employees. Figures below.

Figure 21: Management Office door lock with front plate rotated away, showing key hole

3.1.3.3 Control Room

The door into the Control Room was already open when Consultant entered the building, providing free access to the area.

The Control Room contained several assets that seemed important or business-critical including, but not limited to: computers for controlling the [redacted], a set of keys that included a key to the Refreshment Area's cash register and a Simplisafe fob for the building's alarm system (Figure 22).

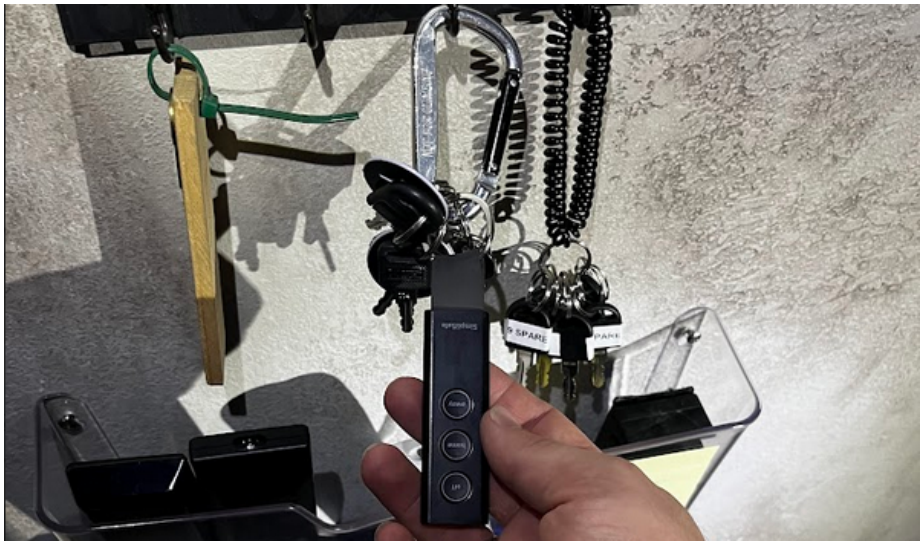

Figure 22: SimpliSafe fob and other keys left exposed in the unlocked Control Room

3.1.3.3.1 Control Room - Keylogger Implant

With easy access to the control room and the computers within, Consultant was able to implant a keylogger device on the center workstation (Figure 23). The device is a small, relatively innocuous looking piece that appears at a quick glance to be a keyboard adapter. Consultant took the added step of adding a strip of tape that said "DO NOT REMOVE" to both cover the arming button's hole and add a layer of deception to make it appear that this device was added by management and should not be tampered with.

Figure 23: Keylogger device

Upon retrieval of this device, Consultant was able to plug it into their attack machine and exfiltrate the data that the keylogger had gathered. This data included a multitude of business and personal email account logins, [redacted] logins, and [redacted] logins. One [redacted] login that was retrieved was for an admin level user with elevated privileges. There were also some items that appeared to be username/password combinations that Consultant could not determine the exact use of ([redacted]), but given more time may have been able to leverage for further access or information. Below are figures demonstrating access to [redacted] (Figure 24) and [redacted] (Figure 25).

Note: Consultant did not alter or modify any data or settings of these accounts. Consultant also did not attempt to access any of the several personal gmail or yahoo accounts whose logins were exposed in the keylogger data.

Figure 24: [redacted] access as admin

Figure 25: [redacted] access

3.1.3.4 Workshop / Mech Shop / Stock Room

There are 2 entrances to the Workshop, both of which were completely unlocked during Consultant's test.

The East entrance is a double door with a locking latch knob. Consultant found this door to be completely unlocked. However, even if the door had been locked, there is no deadlatch on that particular lock, providing an easy route to hook the latch open to access the area.

The West entrance is through the building's stock room. There is no door between the Stock Room and the Workshop. The door to enter the Stock Room did not have a lock on it at all, so once entry was made into the building overall, there was free access to the Stock Room and therefore the Workshop as well.

The Workshop contained several assets that seemed important or business-critical including, but not limited to: the Simplisafe base station (Figure 26), building materials, a 3D printer (Figure 27), and valuable equipment such as a mitre and table saw. Additionally, several pieces of equipment in the Workshop are dangerous and could cause harm to a wandering guest if they got their hands on them (Figure 28).

The Stock Room contained several assets including but not limited to: a cash box (Figures 29a-29c) with weak security, a wall-mounted cash drop box, and stocks of refreshments and souvenirs. Figures below.

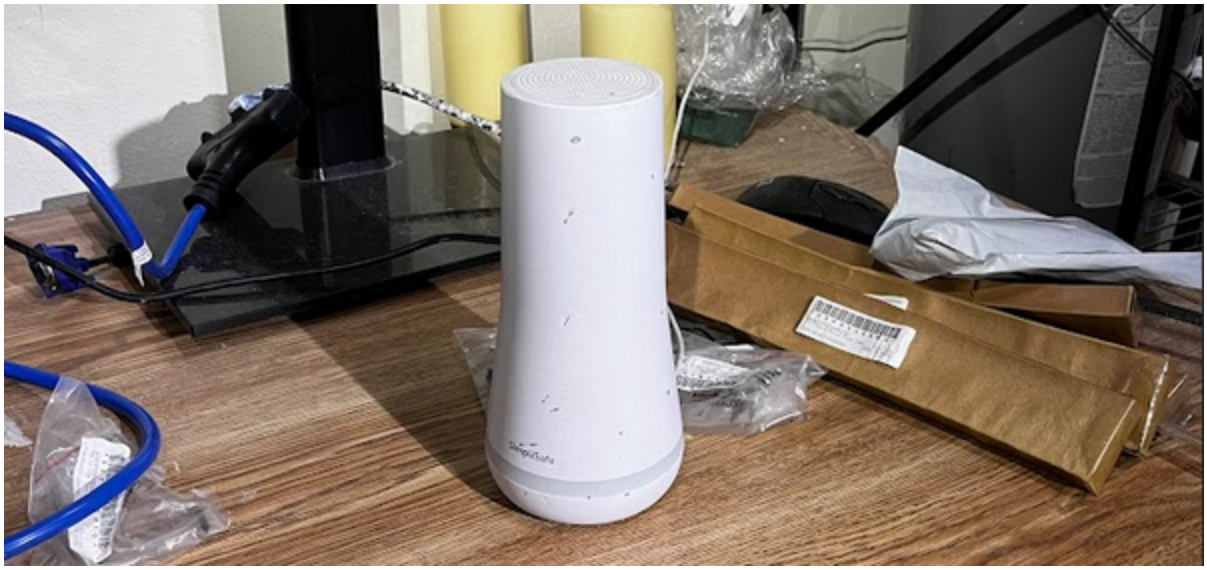

Figure 26: Exposed alarm base station

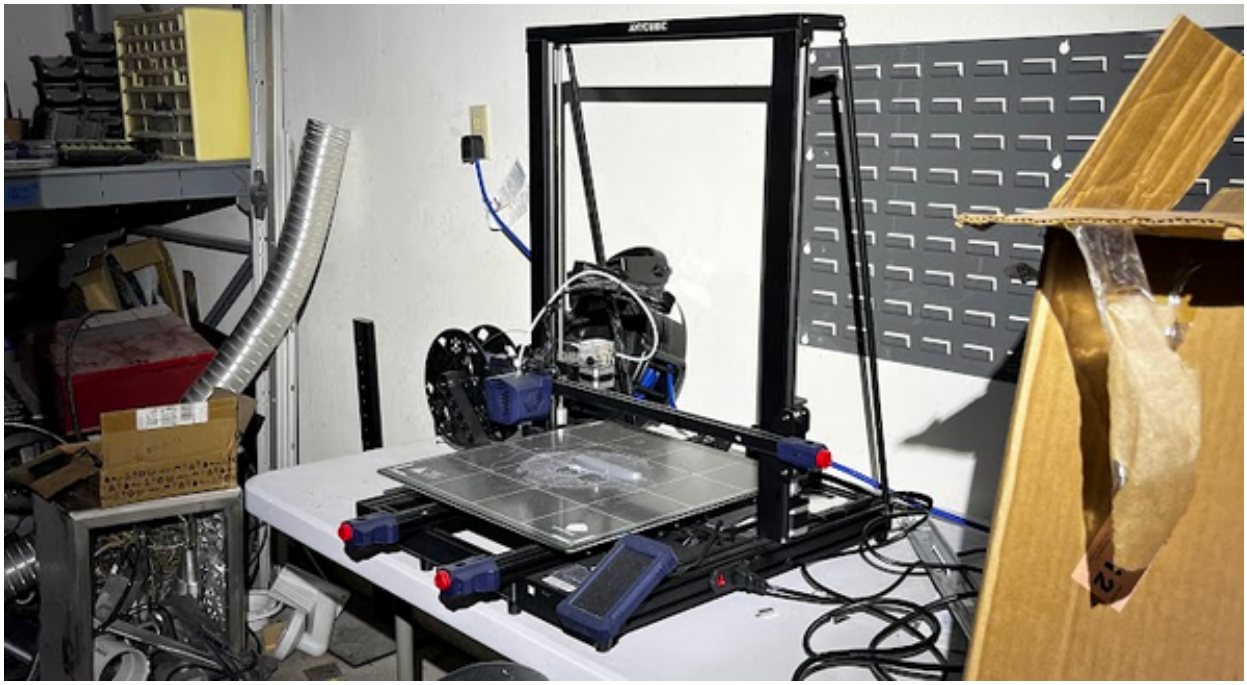

Figure 27: 3D printer in Workshop

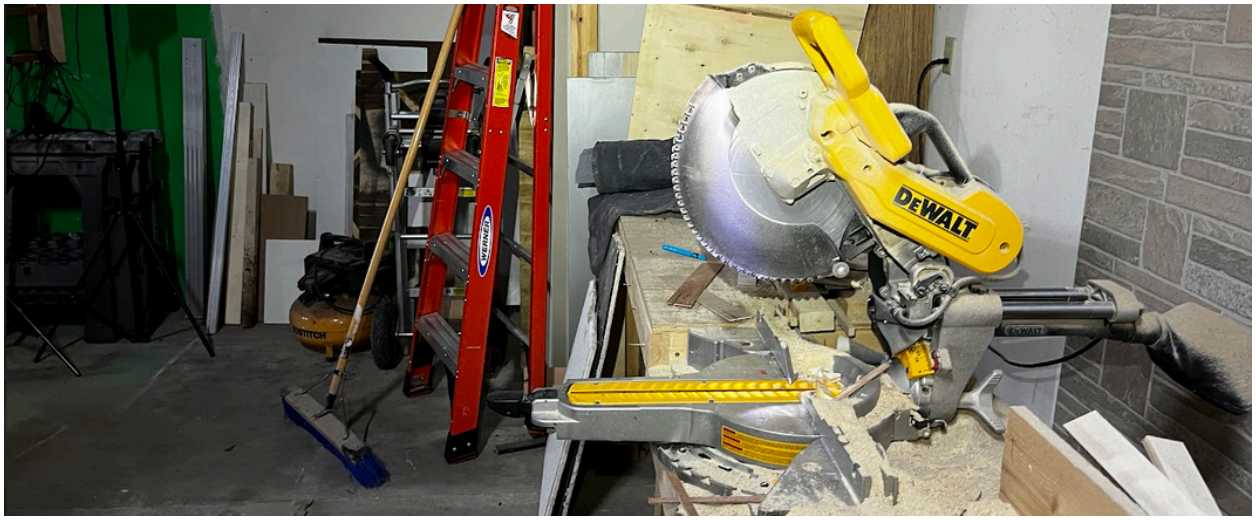

Figure 28: Easily accessible, dangerous equipment

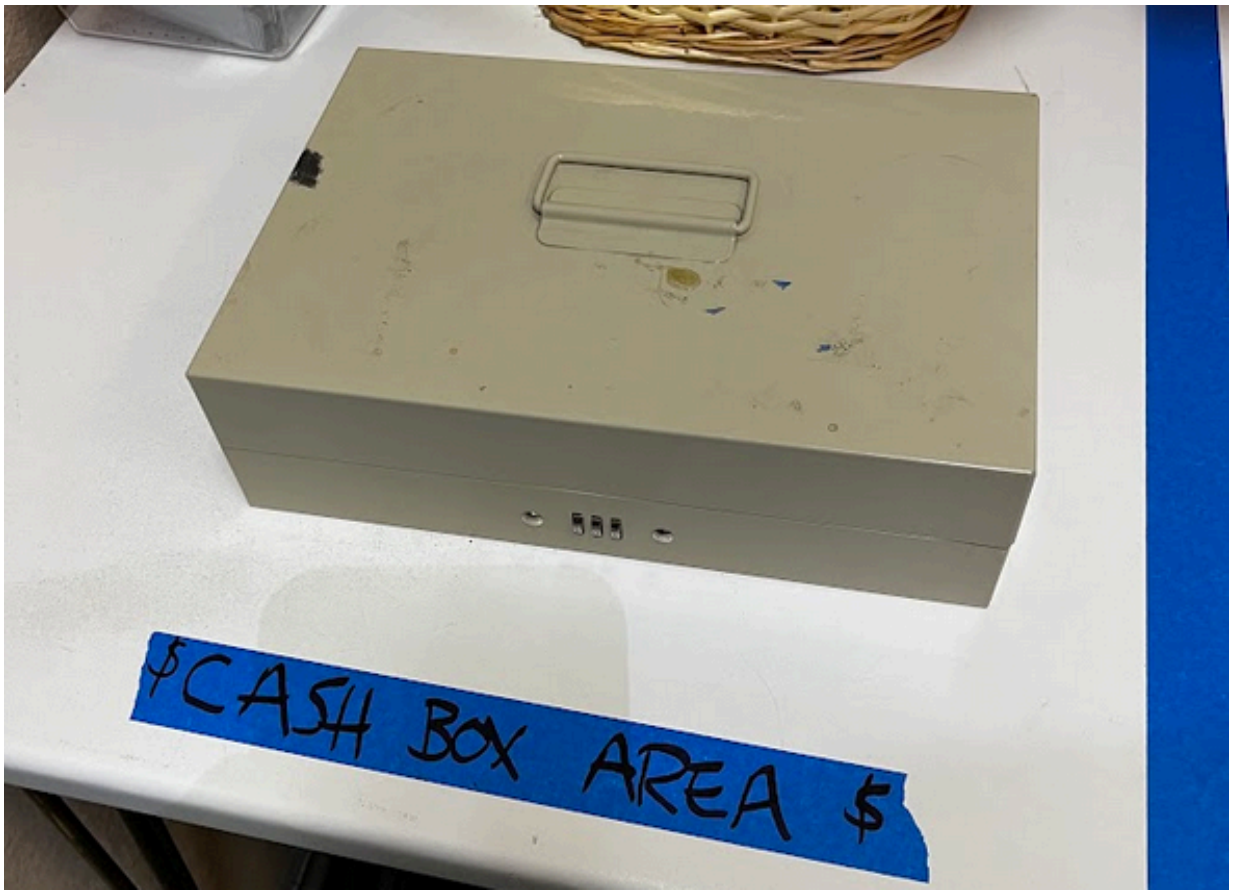

Figure 29a: Exposed, portable cash box (not secured to stable object)

Figure 29b: Weak security on cash box

Figure 29c: Cash box easily accessed

3.1.3.5 Front Vestibule

The Front Vestibule area would be the first area encountered by an attacker coming in through the Front Door. There are 2 doors from the Front Vestibule that lead into the rest of the building. One door is locked via an electronic lock and a magnet that is controlled by the employees on their computers. This door's security is effective. The other door to the left of the desk has no handle on the Vestibule-facing side, and is locked by a crash bar on the interior-facing side. The crash bar's locking latch sits over a bar on the inside (Figure 30). However, the latch sits only a couple millimeters onto the bar, and Consultant was able to grab the bottom of the door by hand and jiggle the door to free the latch and open the door.

Figure 30: Front Vestibule door's latch barely sitting on locking bar

3.1.3.6 Refreshments Area

The Refreshments area has an electronic lock with a keypad on the door. However, the ordering window of the area is not secured (and in fact is not able to be secured at all), and Consultant was able to access the area via climbing through the window.

The Refreshments area contained several tablets (Figures 31 and 31b) and a cash register that was stocked with $292 and change (Figure 32).

Figure 31a: Tablets in Refreshments Area

Figure 31b: Tablets in Refreshments Area

Figure 32: Cash register easily accessed

3.1.3.7 Electrical Room

The Electrical Room just inside the Double Door was completely unlocked when Consultant attempted entry. There is a knob with a locking latch that includes a deadlatch. Despite finding the room unlocked, Consultant tested the locking latch and found that the fitting was appropriately sized to engage the deadlatch. However, the gap in the door provides a space through which an attacker can reach with tools to widen the gap to disengage the deadlatch, and then hook the latch open.

The Electrical Room contained power infrastructure for what appeared to be the whole building, which could cause business-wide ramifications if tampered with.

3.1.3.8 [redacted] Rooms

All doors to [redacted] Rooms were fully unlocked. While this is likely a safety feature so that guests can leave whenever they want or need, this also exposes the assets and materials in the room to potential theft, which could have serious effects on the business.

3.1.3.9 Employee Break Room

The door into the Employee Break Room was already open when Consultant entered the building, providing free access to the area.

The break room contained various insignificant items, but importantly also contained a tall double-door electronic cabinet (Figure 33). This cabinet was identified through internet research as a ULINE electronic storage cabinet (Figure 34). Consultant was able to identify the model of the cabinet and find a manual that details how to use a hard key bypass in the event that the electronic element loses battery (Figure 35). Consultant used this information to pry off the override key cover plate, which exposed a keyhole with the identifier “99” written on the faceplate (Figure 36). Consultant was able to search through the keys found freely available in [redacted] Office to find a matching identifier on a key (Figure 37), which ultimately unlocked the storage cabinet. Inside the cabinet, Consultant found Credit cards, deposit slips for a bank with routing and account numbers, and valuable electronics such as DSLR cameras and other equipment (Figures 38-44).

Figure 33: Electronic storage cabinet in Employee Break Room

Figure 34: Recon identification of cabinet model

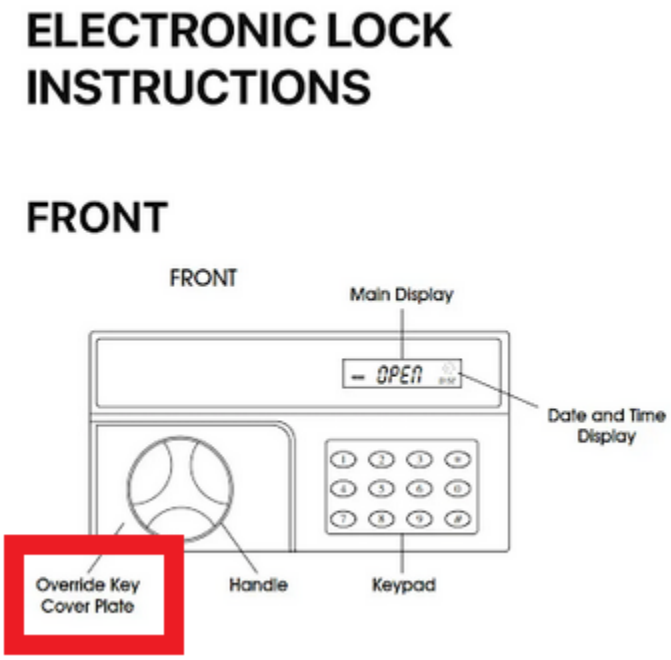

Figure 35: Recon identification of manual bypass to electronic access control

Figure 36: Consultant's removal of the override key cover plate

Figure 37: Matching key found in [redacted] Office

Figure 38: Opened electronic storage cabinet

Figure 39: Charge cards

Figure 40: Deposit slips with account information (Consultant redacted numbers)

Figure 41: DSLR camera

Figure 42: DSLR camera

Figure 43: Misc equipment

Figure 44: Misc equipment

3.2 Security Process and Employee Training/Awareness

Generally speaking, the overall security inside of the building was lackluster in all areas, and even completely absent in some areas. The most secure room that was locked upon Consultant's arrival was the management office which actually had very little in terms of valuable assets, cash, or business-critical items. There is an evident lack of security process at the end-of-day closing, in which no doors or rooms are locked securely.

During the reconnaissance phase of the engagement, Consultant engaged in social engineering and employee manipulation. Consultant called [redacted] and requested WiFi credentials "to be able to log into when I'm there". Employee was initially successful in stating that WiFi can be given while on-site, but Consultant spun a story to give an excuse for needing the WiFi login info ahead of time. Employee eventually provided the guest WiFi login info to Consultant. With this info successfully gathered ahead of time, Consultant was able to connect devices to the guest WiFi network without needing to try and break the WiFi password encryption for access.

Consultant also learned from [redacted] that the keylogger placed in the control room (ref section 3.1.3.3.1 above) was at some point removed by an employee and left on top of the desk. [redacted] stated that he saw the device on the desk, suspected it might be for the pentest engagement, and therefore left it in place on top of the desk. The reasoning for the initial removal of the device is uncertain, but it suggests that there was an employee that was skeptical of the device's nature and unplugged it, which is generally not a bad practice. However, when Consultant returned to the Client site to retrieve the keylogger, Consultant found that the device had been plugged back into the control room computer where it was initially planted. This allowed for Consultant to gather even more data from the keystrokes on the computer.

4. Risk Assessment

With the objective of this engagement being to find low hanging fruit attack methods, and given the levels of success that the Consultant achieved in the objectives, Consultant views Client site's risk of attack as moderate to high.

While there are some security features in place such as exterior lights, some electronic controls, and cameras that may deter or prevent an opportunistic attacker from gaining entry, there are still significant gaps in security that an attacker can easily take advantage of.

5. Recommendations

The recommendations in this section will cover mitigation strategies for each of the major findings listed above in section 3. Section 5.3 below will provide a phased implementation plan which will suggest a roadmap of security enhancements starting with most beneficial mitigations listed first, and the more niche, optional, or costly mitigations listed later.

5.1 Physical Security

Overall, physical security of the exterior was moderate, but still successfully breached by Consultant. Camera coverage was good on the interior cameras, but exterior cameras had angle and coverage issues. Internal security was almost entirely lacking, with just a few areas having a low- to moderate-level of security.

5.1.1 External

Consultant was unable to gain access via the Front Door or Employee Door using ethical methods that were non-destructive. This test indicates that an opportunistic attacker looking for low hanging fruit would be unlikely to gain entry through either of these doors easily as well.

Consultant's successful entry into the back Double Door indicates the weakest zone of external physical security.

The gap of the Double Door was a critical way for Consultant to both see inside for more information and gain initial entry into the building. Consultant recommends adding shielding to the door to remove the presence of a gap altogether. If the Double Door had shielding preventing Consultant from reaching through to activate the crash bar, and given the other doors' securities, Consultant may not have been able to enter at all, or would have at least needed to attempt more complex or destructive methods.

The Double Door was completely unlocked, though the lack of a handle on the outside might stump low-skilled attackers. This in addition to the gap referenced above allowed for the successful use of tools through the gap to activate the crash bars. Consultant recommends adding a lock to the Double Door which will only be engaged during the closing process (door likely must remain unlocked during business hours for fire safety code).

The hinges of the Double Door and Employee Door were exposed and insecure. Consultant also recommends using more secure hinges or jamb pins to prevent attackers from removing the hinges and walking the door off the frame.

5.1.2 Cameras

The presence of cameras was generally well implemented, with the only major gap being in the Workshop. The angles of the exterior cameras provided little to no sightlines of important areas of possible entry.

Consultant recommends adding at least one camera to the Workshop. Consultant also recommends adjusting exterior-facing camera angles to more completely view all of the exterior doors and their immediate surrounding areas.

5.1.3 Internal

Internal security on site was almost entirely lacking. Most doors were either left unlocked or did not even have a lock on them at all. Consultant recommends adding locks to all internal doors, but especially to those that lead to areas that have critical business assets or information (e.g., [redacted] Office, Control Room, Workshop).

Consultant also found several doors that had locks, but whose locks either completely lacked a dead latch, or the fitment of the lock in the door frame was improper which made shimming the doors open possible. Consultant recommends that the locks on internal doors be equipped with properly fitting dead latches at the very least level of security, or electronic access controls (such as the one on the external Employee Door) at a higher level of security.

Besides the almost completely open and available internal areas (closing and security process will be covered below in section 5.2), Consultant found several additional items of interest and concern that should be reassessed and addressed.

Primarily, Consultant found several sets of keys in the Control Room and [redacted] Office that allowed for even further access in the building. One of these sets of keys also included the fob for disabling the security system. Consultant recommends storing all keys and access control or security devices in a lockable key box that is securely affixed to the wall. With this implementation, even if an attacker makes their way into the building, they would have a harder time finding keys, and would then also have to know how to break into the key box to retrieve any keys. Accessing this key box could be managed by each employee having their own key to the key box. Each employee already has a key fob to get into the exterior Employee Door, so just attaching a key box key onto their keychain with their fob would be an accessible and easy solution for employees to retain access to the building keys while preventing access from attackers.

Consultant found many financial, benefits-oriented, and private documents in [redacted] Office that could be used in further social engineering attacks. Consultant recommends investing in a locking document box that will keep those letters more securely stored.

The cash box in the Stock Room was not affixed to a solid surface, and had low security. Consultant was able to visually decode the locking wheels and gain access to the box. Consultant recommends affixing the cash box to a stable surface and investing in a more secure box.

The door in the Front Vestibule to the left of the desk has no lock and is operated by a crash bar on the interior which has poorly overlapped fitment, allowing for a quick jiggle to open the door.

Consultant recommends adjusting fitment of the crash bar to prevent this attack, or adding a lock to the door to only be locked during the closing process for overnight security.

The cash register in the Refreshments Area was not affixed to a solid surface, and had low security. Consultant was able to jiggle the cash register open with a standard jiggler. Consultant also found the key for the cash register in the Control Room. Consultant recommends securing the cash register to a stable surface, and getting a more secure lock for the register. The key box recommendation above would be sufficient mitigation to cover the issue of the easily accessible key.

The door to the electrical room was completely unlocked, despite the door having a deadlatch lock installed. Consultant recommends locking the electrical room at all times, and providing key access via the key box mitigation listed above.

The electronic storage cabinet in the Employee Break Room is generally a good and secure option. However, Consultant was able to find a key in [redacted] Office to get into the cabinet without knowing the code. The key box recommendation above would be sufficient mitigation to cover the issue of the easily accessible key.

5.2 Security Process and Employee Training/Awareness

Consultant found several process and employee awareness items that are in need of remediation.

Primarily, upon the last employees leaving for the night during the closing process, all internal doors that can be locked should be locked. This recommendation, in tandem with the above sections' recommendations to increase the number of lockable doors inside the building and adding a lockable key box, will reduce the likelihood that an attacker that gains entry to the general building would then be able to enter interior areas that contain valuable or business critical assets.

Consultant was able to garner guest WiFi login information over the phone. While this is not necessarily a critical failure by itself, it's one step closer to easy WiFi access for an attacker that finds themselves successfully gaining physical access on-site. Consultant recommends that employees don't freely give such information over the phone; there is no reason that a guest would need the WiFi login info ahead of time while not inside the building.

Consultant's implanted keylogger device was initially unplugged, which is generally good practice to unplug unknown or suspicious items while trying to learn from higher-ups if they're legitimate or intended devices. However, an employee eventually plugged the keylogger back into the computer, allowing for Consultant to gain more information. Consultant recommends that Client employees do not plug in devices without knowing their purpose or legitimacy from higher-ups. When in doubt, employees should default to asking management about a device before plugging it in.

Via the keylogger referenced above, Consultant was able to gather credentials for not just business accounts, but personal accounts as well (Consultant found ten [10] personal login username/password combinations). Consultant recommends that Client employees do not log into personal accounts on business assets.

5.3 Phased Implementation Plan

This phased implementation plan is organized in a priority list style, which will provide the most beneficial and accessible fixes first while saving more niche, optional, or costly fixes closer to the end.

5. Add Double Door lock (to only be locked at night after closing)
    a. If Consultant had not been able to get into the Double Door, other security flaws inside wouldn't have been *as* critical
6. Add shielding to cover Double Door gap
7. Adjust camera angles to provide more complete coverage
8. Train employees on security awareness and proper lockdown procedure at close
9. Adjust Front Vestibule door's crash bar fitment
10. Add jamb pins to insecure-hinged doors
11. Add a key box and secure the key box to stable surface or wall
12. Adjust existing locks' fitments to properly engage deadlatches
13. Add locks with deadlatches to internal doors (preferably to all internal doors, but especially to those rooms containing valuable or critical business assets and cash)
14. Secure Refreshment Area's cash register in place
15. Secure Stock Room's cash box in place
16. Add camera to Workshop
17. Add a more secure Refreshment Area cash register to replace existing
18. Add a more secure Stock Room cash box to replace existing
19. Add a lockable document storage solution
20. Add secure hinges for all doors with exposed hinges.
21. Add more lighting on exterior to both improve camera picture and deter attackers
22. Add electronic access controls (fob-activated) to critical internal doors such as [redacted] Office, the Control Room, and the Workshop and Stock Rooms.

6. Conclusion

Client's security posture is currently assessed as moderately vulnerable to attack. Due to the scope and limitations of this engagement, the findings and recommendations included in this document are not all-encompassing, but rather are a foundation to build off of in the process of improving Client security to most quickly and effectively address many low hanging fruit vulnerabilities.

Once implemented, the recommendations in this document will drastically improve Client security.

We are committed to ensuring that you have the support and assistance that you need through your security mitigation process. Please feel free to reach out to the Cyber Operations Analysts assigned to your engagement with any questions.