[redacted]

Security Assessment Report

March 26, 2019

Report Prepared by:

Robert Rivera, MPR (abd)

(AS/Criminal Justice, BS/National Security, CAS/Security Studies)

robrivera01@gmail.com

908-420-3421

THIS PAGE LEFT BLANK INTENTIONALLY

Executive Summary 5

Top-Ten List 5
1. Information Security Policy 5
2. Video Surveillance System 6
3. Alarm System 6
4. Electrical Continuity 6
5. Physical Barriers 6
6. IT Security Protocols & Plan of Action 6
7. Education 7
8. Visual Deterrence 7
9. Occupancy Accountability 7
10. Neighborhood 7

Introduction 8

Scope 8
Project Scope 8
In Scope 8
Out of Scope 8

Asset Identification 9

Assets of [redacted] 9

Threat Assessment 10

Threats to [redacted] 10

Laws, Regulations and Policy 11

Federal Law and Regulation 12

Summary 12

Executive Summary

On January 25, 2019, a general site survey of [redacted] located at [redacted], was conducted. During this assessment, a review of the exterior perimeter, interior premises, an evaluation of any existing security efforts, and limited interviewing was conducted. This evaluation was compared against statistical data from [redacted] Police Department[1] and other sources to determine the greatest threat potentials.

Organizations must ensure security management is collaborative, coordinated and monitored, and also establish a framework that brings together the various functions responsible for elements of security, and ensure all of the membership, at every level of the organization, are aware of and understand their responsibilities. The overall success of an organization's security management program is contingent on effective planning, communication, organization-wide collaboration and oversight.[2]

Previous to this evaluation, two security measures were implemented. First, a remote monitoring system was installed, including several door sensors and one motion detecting device. These were routed to a communications port[3] and integrated touch-key panel near the front door. The monitoring company responsible for the installation, monitoring, and upkeep of this system is ADT Security Systems of Boca Raton, Florida[4]. This system issued a faulty trigger on January 26, 2019, with a protracted response time by law enforcement of over an hour. Second, a video surveillance system involving numerous cameras[5] stationed throughout the interior and exterior of the building were installed. This system is inoperative, with inherently vulnerable wiring, poor placement of optics, video cameras that were deliberately disabled[6] in several locations, and no central device to monitor or record any activities whatsoever[7].

The three most pertinent security risks include (1) an inadequate audible alarm system, viable video security monitoring, or capturing device, (2) Attempts to breach physical security devices and barriers[8], and (3) a lack of awareness by the membership of the security systems or their importance, including the indications of internal circumvention of security measures.

Top-Ten List

The list below contains the "top ten" findings, weaknesses, or vulnerabilities discovered during the site security assessment. Some of the issues listed here are coalesced from more than one section of the assessment report findings. It is recommended that these be evaluated and addressed as soon as possible. These should be considered significant and may impact the operations of [redacted]

1. Information Security Policy, Protocols, and Plan of Action

An information security policy is the primary guide for the implementation of all electronic data security measures. It is recommended that [redacted] ensure the Trustee(s) coordinate(s) with the [redacted] principle officer and the various functional areas responsible for security; and, formalize the plan of action and security

[1] Appendix A

[2] http://www.nserc-crsng.gc.ca/_doc/Reports-Rapports/Audits-Verifications/PhysicalSecurity_e.pdf

[3] Appendix F

[4] https://www.adt.com/security-benefits

[5] Appendix B

[6] Appendix E

[7] Appendix G

[8] Appendix C

protocols to provide oversight of the security program. There is no formal security policy specific to [redacted].

Recommendation: Develop a security policy that specifically addresses the needs of [redacted] and its mission. Execute that policy as a basis for an effective security program. Penalizing individuals for the deliberate disabling or disarming of any aspect of the security system should be paramount to mitigate such behavior and ensure the most effective results for a properly functioning security strategy.

2. Video surveillance system

The introduction of a functioning video surveillance system with remote-monitoring would act as the primary means of deterring and/or capturing illicit activity in or around [redacted]. While a wireless camera system would be generally effective, a hard-wired system utilizing concealed Bayonet Neill Concelman (BNC) cable would ensure continuity and stability. This camera system should be routed to a central DVR/NVR for reference, as well as be transmitted via IP for monitoring to authorized users.

Recommendation: Install video surveillance system with remote monitoring and motion-sensing capabilities covering all points of entry, areas of highest potential for asset loss, and primary control areas (alarm panel, NVR, IP router, exterior power cutoff).

3. Alarm system

The introduction of a functioning traditional alarm system to supplement a remote-monitored video surveillance system is an essential element in deterring nefarious conduct, including forced or unauthorized entry. A system consisting of interior and exterior strobe lights and at least two interior audio devices would act as redundancy in the event that an individual deactivates one by force. In addition, in the event of forced or unauthorized entry, this system would act to deter an individual from trespassing into the building beyond the point of entry. It would also draw attention to the property by neighbors, passersby, and law enforcement.

Recommendation: Install audible/visible unmonitored traditional alarm system for all points of entry and attic door, as well as motion sensors in both stairways, bar area, downstairs rental space, and two in main [redacted] room, as well as strobes and audio devices.

4. Electrical continuity

The audio and video security systems rely on electricity. This electricity may be disrupted by natural, intentional, or unintentional threats rendering the systems inoperative. There is a main cutoff switch located outside of the building[9] that, if switched, would allow an individual to bypass the current system.

Recommendation: Secure area around outside power breaker with fencing or other physical barrier, padlock the breaker, and install power backups at the audible alarm panel, NVR/DVR device, and IP router to offer the best means of protecting the integrity of the systems.

5. Physical barriers

There is visible evidence of attempts to enter the building by means of prying at the door latches, deadbolts, and forcing open points of entry. This was observed at all points of entry. The locks have been partially compromised and the main entry at the front of the

[9] Appendix D

building is framed by thin, weak wood. The steel doors at secondary entry points, along with the main entry's deadbolts are intact and operational, though inadequate.

Recommendation: Replace the damaged locks, install steel front door or a minimum of a new steel frame, plant deterrent thorny foliage around perimeter of building, particularly near windows or areas of easier roof access. Additionally, lockable racks to protect the router, audio system, and NVR/DVR should be implemented. Finally, a perimeter fence is recommended.

6. IT Security Protocols & Plan of Action

Currently, there is no network or technology in place other than a single PC in the main [redacted] room. Files are stored in boxes and are susceptible to water, fire, and/or intruder.

Recommendation:

Digitize files on a non-networked, password-protected computer in the main [redacted] room under video surveillance. The files should be backed up to a digital cloud for remote redundancy.

7. Education

The membership has no working knowledge of the security system in place, hours the building is unlocked/accessible, or what to do in the event of an emergency of any kind, including a security alarm.

Recommendation: Create authorization process for those in senior positions, inform membership of security processes, and integrate emergency plans into the documents outlined in section 1 of this list.

8. Visual deterrence

While surveying the exterior, it was noted that there were footprints in the snow along the East side of the building, leading to a location where an individual urinated. This indicates that not only was this area easily accessible, but it was unilluminated and unmonitored.

Recommendation: Photosensitive lighting, motion-activated lighting on rear and both sides of the exterior of the building, and warning signs indicating video/alarm presence are recommended.

9. Occupancy Accountability

No schedule exists relating to the times the building is in use, therefore, it would be difficult to ascertain if use is authorized. There is no security officer, either on foot or motorized on this property at any time.

Recommendation: Schedule of events & routine daily walk-throughs with sign-in log verifying walk-throughs.

10. Neighborhood

The neighborhood is documented as HIGH in criminal activity by the [redacted] Police Department, including assaults, burglaries, and robberies. There is no video monitoring by [redacted]PD, nor is there known to be any form of community policing or neighborhood watch. The relationship between the membership and the adjacent properties is unknown. Housing located in an empty lot across the street[10] provided a limited degree of monitoring, however, it has been razed and no longer provides such over watch.

[10] Appendix H

Recommendation: Establish positive relations with neighbors, create neighborhood crime watch, work with local law enforcement both informally and formally to increase patrols, host community and/or police events, and petition the city for the addition of a video feed to their network.

Introduction

The objective of the audit was to provide assurance that governance, internal controls and risk management practices related to physical security management are adequate and effective. The audit assessed the effectiveness and adequacy of the security measures and management controls. The audit included an assessment of:

- Governance, roles and responsibilities of all parties involved;
- Physical security risk management processes and practices;
- Physical access to facilities, information, and assets; and,
- Membership awareness and compliance with policies and directives regarding physical security.

Scope

The scope of the audit included [redacted]. The scope included information and assets contained in this area. Compliance to the Occupational Health and Safety Regulation was not included in the audit, nor were the rules or regulations pertinent to security systems regulations [redacted], County [redacted], or State [redacted]. This security assessment report is not all encompassing and was submitted prematurely due to the extreme and immediate need for risk mitigation.

Project Scope

In Scope

The following activities are within the scope of this project:

- Interviews with key staff members in charge of policy, administration, day-to-day operations, system administration, network management, and facilities management.
- A visual walk-through of the facility to assess physical security.
- A test of the security system and procedures in its current configuration.

Out of Scope

The following activities are NOT part of this security assessment:

- Penetration testing of systems, networks, buildings, or facilities.
- Social engineering to acquire sensitive information from staff members including qualitative or quantitative data collection from individuals.
- Testing disaster recovery plans, business continuity plans, financial reports or allocations, or emergency response plans.

Asset Identification

Assets of [redacted]

The following lists document some of [redacted] tangible and intangible assets. It should not be considered a complete and detailed list but should be used as a basis for further thought and discussion to identify assets.

Tangible Assets

- Structure
- Furnishing
- Computer (Main [redacted] Room)
- Audio System (Main [redacted] Room)
- Audio System (Basement level)
- Televisions (Basement level & Main [redacted] Room)
- Kitchen Appliances
- Liquor (Bar area)
- [redacted] paraphernalia
- Historical records, images, and other memorabilia items including [redacted].

Intangible Assets

- Electronic data stored on computer, drives, or discs.
- Databases
- Trade or [redacted] secrets
- Video or audio recordings of all kinds
- [redacted] rosters, records, and contact information
- Proprietary information
- Financial records

Each item on these lists also has value associated with it. Each item's relative value changes over time. In order to determine the current value, it is often best to think in terms of recovery costs. What would it cost to restore or replace this asset in terms of time, effort, and monetary investment?

Threat Assessment

Threat assessment is a structured group process used to evaluate the risk posed by a student or another person, typically as a response to an actual or perceived threat or concerning behavior. Threat assessment as a process was developed by the Secret Service as a response to incidents of school violence. The primary purpose of a threat assessment is to prevent targeted violence. The threat assessment process is centered upon on analysis of the facts and evidence of behavior in a given situation. The appraisal of risk in a threat assessment focuses on actions, communications, and specific circumstances that might suggest that an individual intends to mount an attack and is engaged in planning or preparing for that event.[11]

Threats to [redacted]

The following lists document some of the known threats to [redacted]. It should not be considered a complete and detailed list but should be used to as a basis for further thought and discussion to identify threats.

Natural Threats

- Hurricanes
- Severe rain or snow
- Wind damage
- Earthquake
- Tornado
- Extreme temperature
- Wildfire
- Lightning

Intentional Threats

- Physical theft

[11] http://www.k12.wa.us/safetycenter/Threat/default.aspx

- Espionage (theft of information) both domestic or foreign
- Cybercrimes including hacking, theft of information, viruses, identity theft, etc.
- Terrorism
- Vandalism
- Robbery, assault, or battery crimes
- Arson
- Trespassing

Unintentional Threats

- Injury from hazard
- Accidental file deletion or modification
- Fire
- Falls resulting in injury
- Structural failure
- Malfunction of machinery
- Negligence
- Litigation relating to alcohol consumption

Laws, Regulations and Policy

[redacted]

Federal Law and Regulation

[redacted] is legally considered an “entity” and thus is subject to litigation.[13] "It is undisputed that [redacted] raise and spend millions of dollars each year to operate their [redacted] organizations. Each [redacted] is used for the periodic meetings of the individual organization that owns it. One important purpose of these meetings is to [redacted]. The first and last parts of these meetings are [redacted]. The meetings are often used to [redacted] are often tested to determine whether they have [redacted] The most important business of each [redacted], discussed at each meeting, is [redacted] activities. [redacted] not only support their own established [redacted] but also respond to one-time requests for [redacted] from other local, State, or national organizations." [14]

[redacted] Policy

[redacted] in regards to its internal structure is ultimately self-governed [redacted] who abides by its Constitution and By-Laws, supplemented by Robert’s Rules of Order. It is a subsidiary and ultimately accountable to [redacted]. Hierarchy beyond this framework is irrelevant for the purposes of this document.

Summary

In summary, the findings of this evaluation indicate significant threats to the [redacted] While it is clear some efforts have been made to mitigate these threats, they have all been either disabled, partially compromised, or simply inadequate. Remote monitoring by a third-party [redacted] has proven to [redacted] that does not fulfill its promise of a reliable system with an expedient response. A complete overhaul of the security is strongly recommended. This begins with the formulation of an action plan, allocation of funds to support this initiative, stripping the existing security efforts, and replacing with a comprehensive updated system.

---

[12] Ancient Accepted Scottish Rite vs. Board of County Commissioners, 122 *Neb.* 586, 241 *N.W.* 93 (1932)

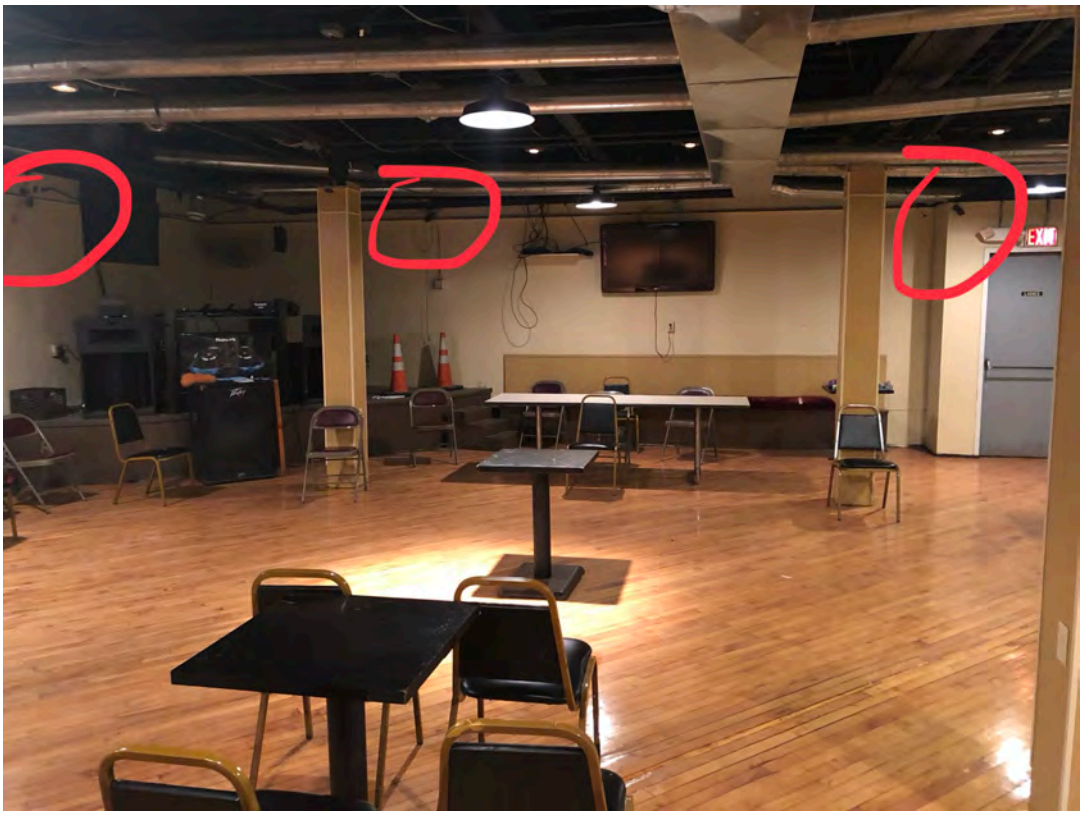
[13] [redacted]

[14] [redacted]

APPENDIX

Appendix A

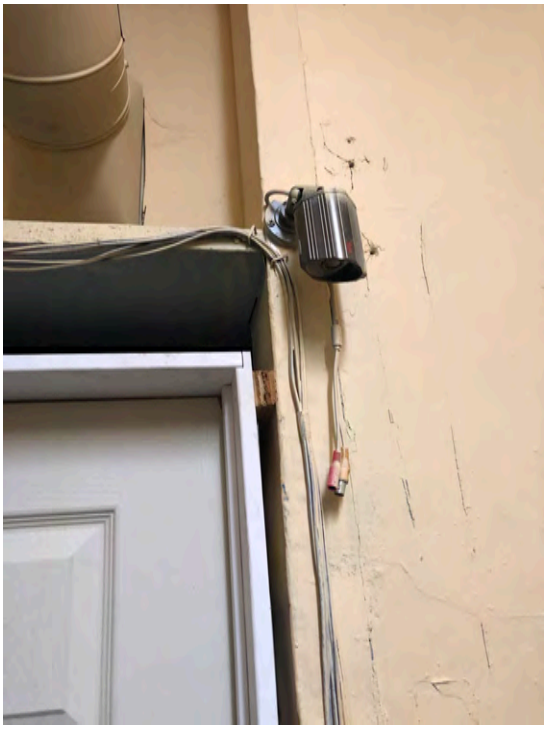
Appendix B



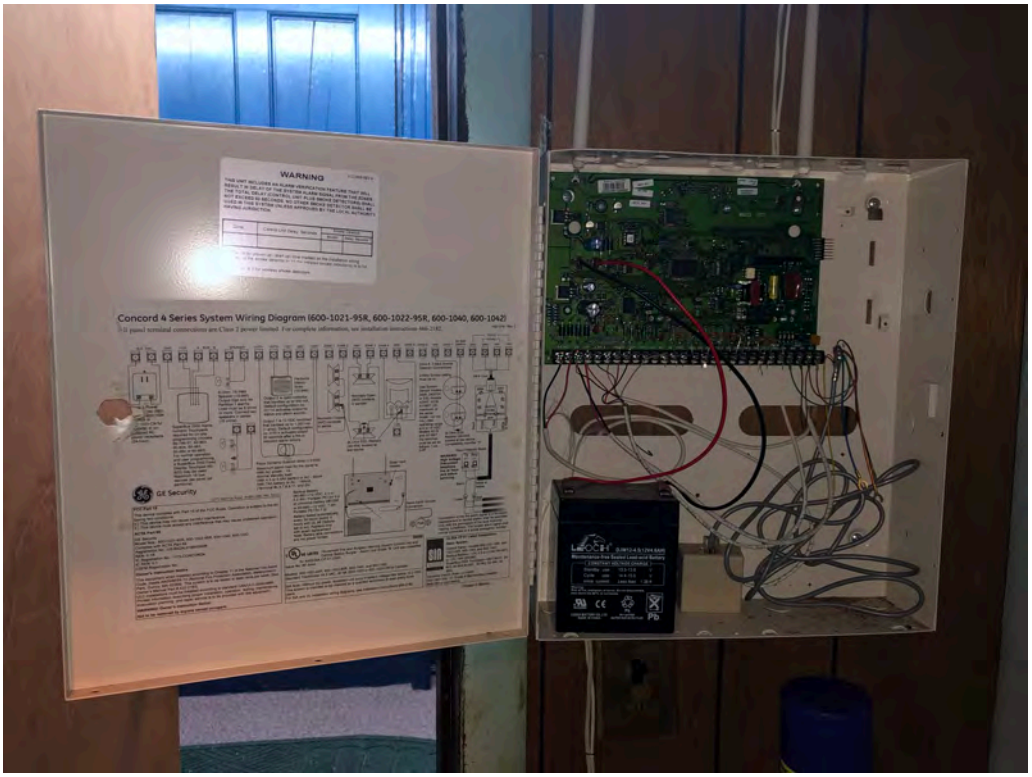
Appendix C

Appendix D

Appendix E



Appendix F



Appendix G

Appendix H

THIS PAGE LEFT BLANK INTENTIONALLY

[redacted] Security Review

02

what happens when *WE* respond?

False Alarm

- Waste of time for our members
- Fee by [redacted]
- Fee by alarm company
- Tying up law enforcement
- Cost to tax-paying residents

True Alarm

- Most burglaries complete in 8 mins
- Member may be mistaken for intruder
- Significant Danger to members, putting their lives at risk

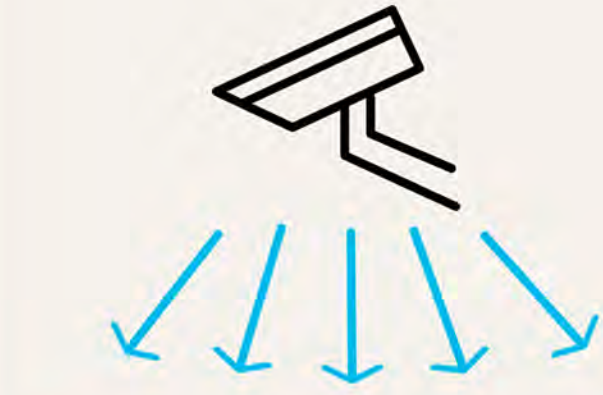
Bottom Line

[redacted] does not work to catch burglars as they advertise

Encountering an intruder is a danger to our members

Highly cost inefficient, and amount only increases over time

How do we solve this?



[redacted]

Security Review

01

Alarm Company Response

5-45 seconds

5-120 seconds

2-8 mins

1-3 mins

Minimum 7 mins

Minimum of 10 mins in surburban, low-crime area with no pending police calls

Police Dept Response

Priorities

1. officer needs assistance
2. violent crimes in progress
3. incidents involving personal injury
4. in-progress incidents to property
5. property loss (after)
6. field activity (i.e.traffic)
7. nuisance calls (i.e. noise)

Priority 2 Response Times

Bank Robbery 5-10 mins

School Shooting 18 mins

Response to the false alarm at our lodge in January was approximately 2 hours