SpenJace

Security Assessment Report

09-May-2019

Report Prepared by:

Paul Flanagan

paultflanagan@gmail.com

1+ (908) 872-7911

|  |  |
| --- | --- |
|  |  |
|  | |  | | --- | | The information contained within this report is considered proprietary and confidential to SpenJace. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss to SpenJace. This report should be distributed to individuals on a Need-to-Know basis only. Paper copies should be locked up when not in use. Electronic copies should be stored offline and protected appropriately. | |

Class ID: CMP-124

Semester: Spring 2019

Name: Paul Flanagan

Customer Description: Flichael: current Executive Director at a community genetic engineering lab in NYC.

Outline:

[**Executive Summary**](#_arzhnp5zc09r) **5**

[**The Customer in this project is Flichael, and I will be visiting SpenJace, the lab in New York City where he works.**](#_suaray4ye0xf) **5**

[**Top-Five List**](#_68n0z7czogq2) **5**

[1. Wi-fi Password Placement](#_ufqvj6vtg5ao) 5

[2. Network Equipment Placement](#_ky917jo6mppl) 5

[3. Weak Protection of Public Laptops](#_qcetyf9ddp2d) 5

[4. Wi-fi Enabled Lab Equipment](#_gdrycqxfj28r) 6

[5. Lack of User Education Protocol](#_i5yu58vz6w0f) 6

[**Introduction**](#_aq8iwcjnjlxp) **6**

[**Scope**](#_mjswflh35pcq) **6**

[**Project Scope**](#_kf2gq0vbm76j) **6**

[In Scope](#_bojw4ppdvzh6) 6

[Out of Scope](#_1opo291aedsc) 6

[Site Activities Schedule](#_epgqkw5nmdo4) 6

[Date – 05-Mar-2019](#_fdslwrzeq5f3) 7

[**Background Information**](#_fiqr9qsqx7z0) **7**

[**SpenJace**](#_34zt12pj25um) **7**

[**Network and Wireless Security**](#_slpg5q907ci) **7**

[Wi-fi password is on display in the middle of the main room.](#_dmtm454omgdk) 7

[Wi-fi network equipment is located in a corner behind some stacks of chairs](#_j9ztbqhd8dgp) 8

[How many users are typically connected to the network?](#_pmrhsypi7471) 10

[Does the network possess any hardware or software firewall?](#_uj1mvmd0yjt1) 11

[Are there protocols for planned network maintenance and downtime?](#_e215g69rwkd0) 11

[**System (PC/Server/Device) Security**](#_27prrhzgbvhb) **12**

[How is it decided whether a device can connect to the network?](#_xppivc8jmk7a) 12

[What software, e.g. firewalls, is used to protect individual devices?](#_asw0hogzbs39) 13

[How often to common devices undergo software updates?](#_o47i7jok0wdt) 13

[What lab equipment is connected to the network?](#_qdhlua11jasb) 14

[**AAA (Authorization/Authentication/Accounting)**](#_9fpfgsa8no94) **15**

[Is any AAA software being used for the network?](#_cfe17rw55mgb) 15

[Are any restrictions placed on how users can access the network?](#_l1bfmechf26u) 15

[How is access to shared resources (e.g. laptops) controlled?](#_auzv6ohon2f5) 16

[What sorts of privileges do different users have?](#_xogm9sfpksot) 16

[How is user activity tracked and monitored?](#_ji8wqbfcwvc6) 17

[**Backups/Disaster Recovery**](#_nmt9jvwsv6qo) **17**

[How is vital data stored on-site?](#_ohbpcoa6orc6) 18

[Is any backup software used?](#_6dvkmgyfkvog) 18

[How often is data backed up?](#_5eb28x7xrl91) 18

[Are there off-site backup locations?](#_uha98brmzxug) 19

How often are they backed up? 19

[**Physical Security**](#_p9633opsptvd) **19**

[Where is the router stored, and how is it protected?](#_85ah39cc3rho) 20

[Where are any permanently wi-fi connected devices stored, and how are they protected?](#_xb1obxabc2sd) 20

[Who has access to these locations?](#_fd2e2ginv8j) 21

[Are there any publicly accessible ethernet ports?](#_s72grd91dfa) 21

[What sort of locks are on the building?](#_8b4tzdz03k4i) 22

[**User Education**](#_akpyt5c8jvmy) **22**

[What features of the network are used the most by the users?](#_7mxlc96k3c8v) 22

[Is there a standard practice when transferring data between staff members?](#_4fgni01wi85e) 23

[What threats are users most vulnerable to?](#_cntxqqzad8an) 23

[Has there been any history of previous data leaks at this network?](#_vjp4ss97ph06) 24

[What is the contingency plan for handling a data leak?](#_5m4mtrnvvr0r) 24

[**Action Plan**](#_pbxzb3f92pat) **25**

# 

# **Executive Summary**

# The Customer in this project is Flichael, and I will be visiting SpenJace, the lab in New York City where he works.

From earlier questions, I know that at SpenJace the researchers primarily use a wi-fi network for internet and file access.

I plan to find out if he has any ethernet-connected devices, what sort of wi-fi security measures he employs, whether their network uses a firewall, how they typically handle file transferring, and which individuals have different access rights and privileges over their network.

# **Top-Five List**

The list below contains the “top five” 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. Additional information about each is provided elsewhere in the report.

It is recommended that these be evaluated and addressed as soon as possible.

### 1. Wi-fi Password Placement

The password for the Wi-fi network is displayed in the center of the office, on a piece of paper taped to the wall above a whiteboard. This is not a safe practice, and exposes the network, and the machines on it, to threat actors.

### 2. Network Equipment Placement

The network hardware is kept in a corner to the right of the doorway, behind two stacks of chairs. In addition to being a mild fire hazard, keeping the equipment relatively unrestricted and unsecured permits physical access to crucial network equipment.

### 3. Weak Protection of Public Laptops

The lab offers public laptops for use by either staff, members, or guests. These laptops are lent without any logging of usage, which can obfuscate any attempts to keep track of suspicious behaviour performed on these laptops.

### 4. Wi-fi Enabled Lab Equipment

One piece of equipment in the lab is Wi-fi accessible, and runs on the same public network available to guests. This increases the vulnerability of the equipment and allows for the possibility of a threat actor on the public Wi-fi gaining access to expensive equipment and lab samples.

### 5. Lack of User Education Protocol

The users (members and staff) at the client organization are not given any form of education in terms of general information and network security practices. While not necessarily imperative for a small company, certain steps can still be taken to help avoid scams and malware.

# **Introduction**

# **Scope**

# **Project Scope**

### **In Scope**

The following activities are within the scope of this project:

● Interaction and discussion with staff members at SpenJace to gather basic information regarding site and network setup.

● Examination of physical security and placement of various crucial network devices and locks.

● IP scans of the network and Port scans of several devices on the network conducted from within the SpenJace facility.

### **Out of Scope**

The following activities are NOT part of this security assessment:

● Inspecting or testing the security integrity of the surrounding Suite Complex.

● Attempting to simulate threats by engaging in White- or Grey-hat hacking.

● Testing Disaster Recovery Plans or Emergency Response Plans.

## **Site Activities Schedule**

## **Date – 05-Mar-2019**

First visit, conducted analysis of physical integrity, ran scans of network and port security, and discussed with several staff members. Due to the length of the visit (~5 hours), all required tests and data were able to be run and collected.

# **Background Information**

# **SpenJace**

SpenJace is a community-centered genetic engineering lab. As a smaller business, their security requirements are not as high as larger corporate locations, but they still make use of a private wi-fi network, use devices such as personal and shared laptops, a desktop, and one wi-fi enabled piece of equipment in the lab area, and use Google Drive to handle file transferring. Each user brings their own devices from home, for the most part, and is proficient in using these devices. The network is almost exclusively used for internet access.

The facility is located in Sunset Park of Brooklyn in New York City. It is a part of the Briq leasing complex in a building in a 2,500 sq. ft. suite, and has neighboring suites on both sides.

# **Network and Wireless Security**

# **Potential or Actual Vulnerabilities**

Listed below are the ***potential or actual*** network security vulnerabilities reviewed during the assessment.

### **Wi-fi password is on display in the middle of the main room.**

**Explanation**

Having a password protecting the wi-fi adds another layer of security to the network. While SpenJace does well to have one, displaying it on a wall certainly weakens the protection it provides. The network is not protected by a network firewall.

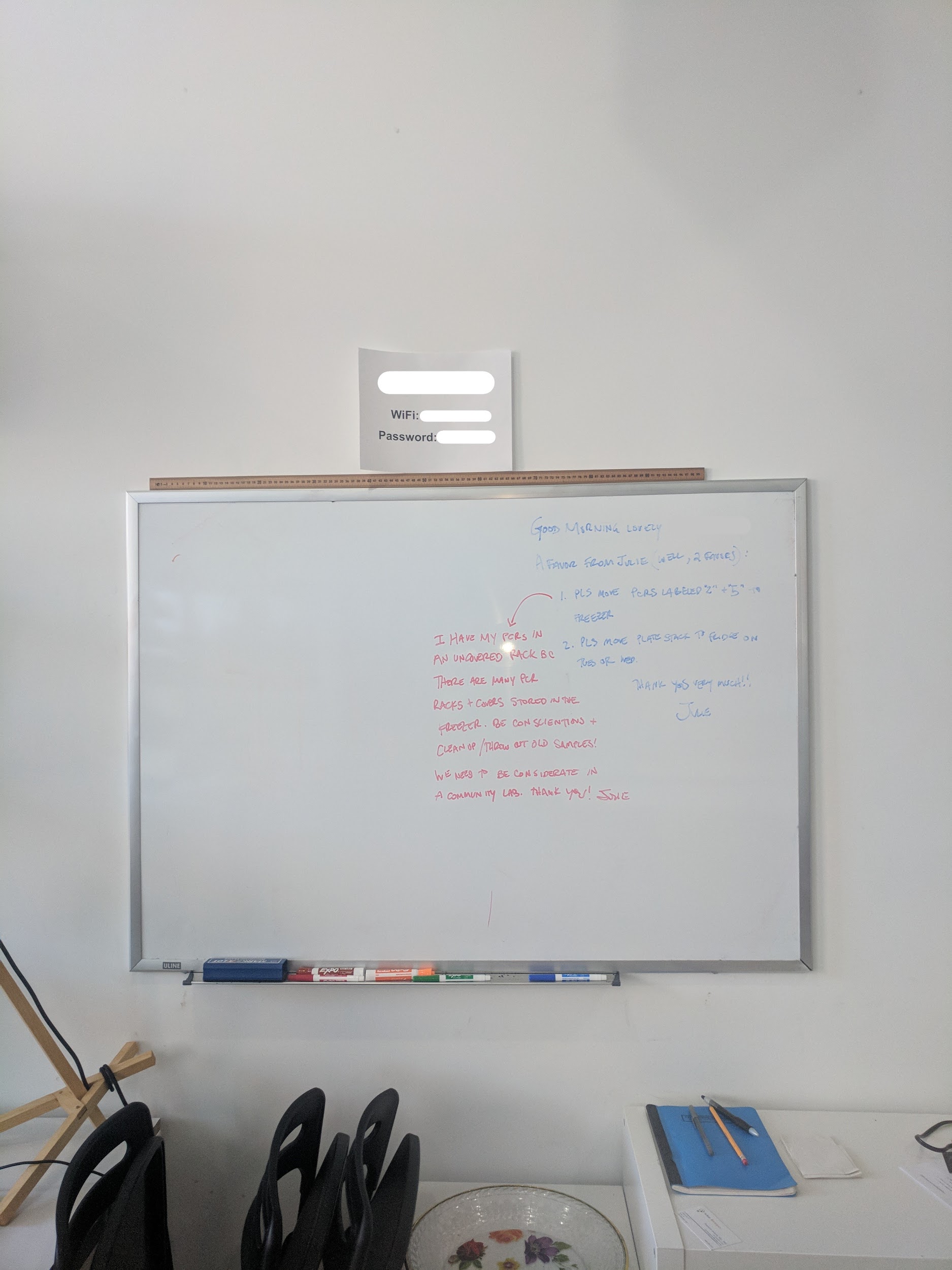
**Risk**

Having the password displayed in this way means that anyone who enters the location once has gained permanent access to the main wi-fi network.

**Observations/Examples Found**

One consideration is the fact that the lab offers classes on site, and the sign on the wall is the easiest way to quickly convey the information to the students if internet connectivity is required.

Additionally, while it is visible from anywhere within the facility, the sign is not visible from outside the electronically locked door. In this way, the wi-fi password is still protected in a sense, in that it is only available to those allowed entry onto the premises.

**Documentation**

**Recommendations**

* Remove sign from its prominent location
* Set up an additional network for use by visitors. The password for this more public network can still be displayed, but it should not be shared by the sensitive devices of the staff members.

### **Wi-fi network equipment is located in a corner behind some stacks of chairs**

**Explanation**

All of the network hardware (router, modems, etc.) is stored in a corner of the entry location by the door. There are two stacks of chairs in front of the equipment.

**Risk**

When vital network equipment are stored out in the open, it makes them easier for a threat actor to access and initiate a breach.

**Observations/Examples Found**

The stacks of chairs, however, provide an interesting type of security: combined with the smaller size of the facility, it would be very difficult to inconspicuously acquire physical access to the equipment without attracting the attention of staff members. In a way, it is under constant watch by anyone inside the room.

**Documentation**





**Recommendations**

Having a locked glass case to protect the equipment from tampering.

### 

### **How many users are typically connected to the network?**

**Explanation**

On a typical day, there are around 7-10 users connected to the network (2-4 non-staff plus ~5 staff members). On days with classes, there can be up to 30 users, but usually around 15.

**Risk**

Despite there being two distinct groups of network users, the private staff members and the public visiting users, they all have access to one network. A threat actor might be able to enter the building as a visitor and use the same network as the staff members, a potential flaw.

**Observations/Examples Found**

While at SpenJace I witnessed a class take place. As I suspected, the students all accessed the same wi-fi network used by the staff members.

**Documentation**

Discussed with staff member (05-Mar-2019).

**Recommendations**

Again, I would recommend implementing a parallel network to be used solely by staff members, with a more public network available to those visiting the building.

### 

### **Does the network possess any hardware or software firewall?**

**Explanation**

A firewall, hardware or software, serves as a protection against potentially harmful content that might attempt to infiltrate the local network.

**Risk**

Lack of a firewall means that the data taken off of the internet is not checked first for the safety of the users. While not as crucial for a small business, installation of a hardware or software firewall will ensure that users of the network are better protected against harm.

**Observations/Examples Found**

SpenJace does not have a network-level hardware or software firewall.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Again, installing a firewall is not imperative, but will certainly increase the safety of the network by a large margin.

### **Are there protocols for planned network maintenance and downtime?**

**Explanation**

Unexpected network downtime can be a flag for suspicious activity and potential network threats.

**Risk**

Not having a protocol for notifying users of planned downtime can cause these occurrences to be inconvenient for users and difficult to distinguish from threats.

**Observations/Examples Found**

There are no such protocols.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Either sending out an email to staff members or putting a notice on the whiteboard will help to reduce confusion and inconvenience should the network need to be temporarily disabled.

# **System (PC/Server/Device) Security**

# **Potential or Actual Vulnerabilities**

Listed below are the potential or actual system security vulnerabilities reviewed during the assessment. Significant problems are noted and recommendations to remediate them are described.

### **How is it decided whether a device can connect to the network?**

**Explanation**

Having a system through which devices are checked before granted access to the network provides another layer of defense against unauthorized activity.

**Risk**

Not checking devices before they are allowed onto the network means that a device with insufficient security or non updated software can be allowed to interact with sensitive devices.

**Observations/Examples Found**

When connecting to the wi-fi, all devices were granted access without a clearance granting process.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Implementing software which monitors the devices attempting to access the network will help to fix this issue.

### **What software, e.g. firewalls, is used to protect individual devices?**

**Explanation**

In addition to a network firewall, personal firewalls can be used to further protect users from threats.

**Risk**

Not having a unified standard for firewall security across the network-connected devices means that whatever is strong enough to penetrate the weakest link could gain access to the rest of the network as well.

**Observations/Examples Found**

No software firewalls are mandated for individual users.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Acquiring a subscription to a secure firewall for the staff users would help secure the network as a whole.

### **How often to common devices undergo software updates?**

**Explanation**

Developers publish updates to their software in order to improve functionality and to fix known bugs and exploits in their systems.

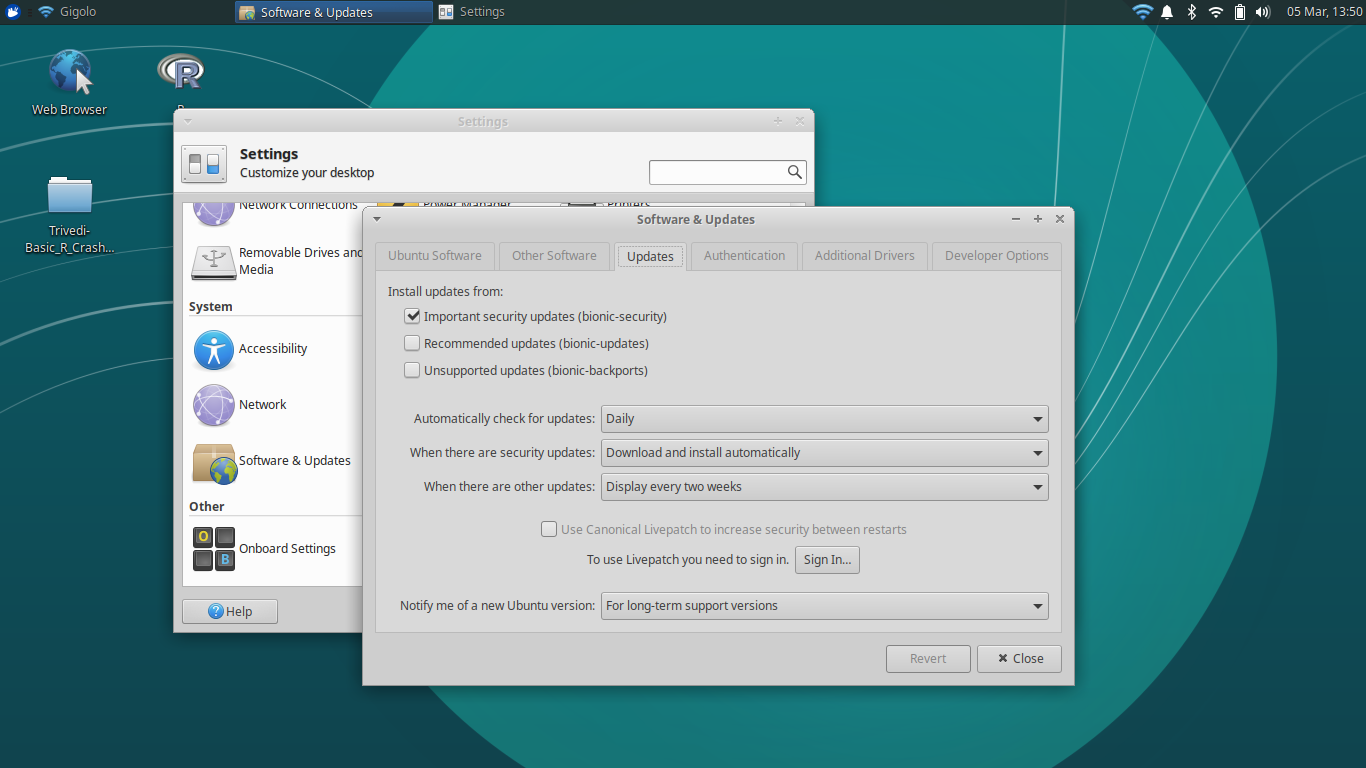
**Risk**

Regular software updates are crucial in order to help protect devices against weaknesses in their operating systems. Failure to keep up to date with these updates allows for threat actors to use these known exploits against your devices.

**Observations/Examples Found**

I checked the public laptops available to visitors and looked at the Settings and Software & Updates menu.

**Documentation**



**Recommendations**

None. Shared devices’ updates are well maintained.

### **What lab equipment is connected to the network?**

**Explanation**

Non-PC devices connected to the network offer a different set of possible vulnerabilities to the network, which need to be protected against threats the same as other devices.

**Risk**

If these other devices are not protected, threat actors might be able to cause costly damage to delicate equipment.

**Observations/Examples Found**

Lab has a robotic liquid transporter for handling pipetting of fluid samples. It is accessible over wi-fi network via a tailored driver/application available for installation online.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

The application provided by the manufacturer appears to be well-protected against invasive action.

# **AAA (Authorization/Authentication/Accounting)**

# **Potential or Actual Vulnerabilities**

Listed below are the AAA potential or actual vulnerabilities discovered during the assessment. These are considered significant and steps should be taken to address them.

### **Is any AAA software being used for the network?**

**Explanation**

AAA (Authorization/Authentication/Accounting) software allows network owners greater ability to monitor those attempting to access and manipulate their network.

**Risk**

Not having AAA software makes the tracking of threat actors much more difficult.

**Observations/Examples Found**

No AAA software is implemented.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Installation of an AAA software according to the needs of the company may be in order if such a need arises.

### **Are any restrictions placed on how users can access the network?**

**Explanation**

Businesses can choose to limit access to their network based on how secure they determine each device to be. This not only allows them to keep track of which devices are connected and when, but also prevents connection with devices deemed unsafe.

**Risk**

By allowing non-inspected devices of any kind to access the network, threat actors can introduce contaminated or otherwise harmful devices into the network and cause damage.

**Observations/Examples Found**

No restrictions are placed on how users can access the network or on what devices.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Can implement a system for checking new devices when they attempt to connect to the network. If a second network is installed for the business, then this system can be reserved for the designated private (more secure) one.

### **How is access to shared resources (e.g. laptops) controlled?**

**Explanation**

SpenJace owns a collection of laptops running a simple Linux distro which are permanently connected to the Wi-fi network and lends them to guests, members, or staff upon request.

**Risk**

Seeing as this is a freely shared resource which provides fairly unrestricted access to the network, it is possible for a threat actor to borrow one of these devices and be granted access to the network.

**Observations/Examples Found**

No control over access to this shared resource is exercised.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Introducing either a physical sign-out sheet for the laptops or opting for a more complex digital log-in system will help to secure this potential security weakness.

### **What sorts of privileges do different users have?**

**Explanation**

Organizing users into different privilege tiers based on their trustworthiness is one way to keep track of user activity and make sure that each individual connected to the network is only granted appropriate levels of network control

**Risk**

Failure to designate tiers of access privileges, or choosing to instead grant indiscriminate access to every user, allows for the possibility of threat actors walking on site and having the same rights as trusted staff members.

**Observations/Examples Found**

No privilege distinctions are made.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Even rudimentarily, separating network users based on trustworthiness (perhaps, for example, into tiers of Guest, Member, and Staff) will help sort users and prevent privilege abuse.

### **How is user activity tracked and monitored?**

**Explanation**

One way companies can get a better sense of user activity is to employ software which tracks the network usage of its users.

**Risk**

Failure to monitor user activity allows potential threat actors to act freely without worry of their actions being traced back to their session or identity.

**Observations/Examples Found**

User activity is not monitored.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

While it is likely that intense activity monitoring would not be necessary for this company, a network firewall which logs instances of users visiting suspicious websites or downloading suspicious files would certainly suffice.

# **Backups/Disaster Recovery**

# **Potential or Actual Vulnerabilities**

Listed below are the potential or actual vulnerabilities related to backups and disaster recovery discovered during the assessment. These are considered significant and steps should be taken to address them.

### **How is vital data stored on-site?**

**Explanation**

It is prudent to examine the ways in which the vital data of a company is stored on location in order to help keep it secure.

**Risk**

If data is insecurely stored, it becomes easier for threat actors to access it and ransom, sell, or abuse the information.

**Observations/Examples Found**

No crucial data is stored on-site.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

If this is the case, then I have no recommendations, besides the suggestion to keep vital data secure if any is stored on-site.

### **Is any backup software used?**

**Explanation**

Backup software is used to keep vital data safe from the dangers of destruction from uncontrollable sources.

**Risk**

If data is not backed up, then the threat of data destruction would mean the total loss of that data.

**Observations/Examples Found**

The company uses a third-party website to store sensitive data regarding employees.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

The company appears to be satisfied with its selection, so I have no recommendations.

### **How often is data backed up?**

**Explanation**

The frequency of data backups increases the security of a company’s data.

**Risk**

In the event of a catastrophe, all data will be reset to whenever the most recent backup was. Each company must make its own calculations to determine how often to back up its data based on this fact.

**Observations/Examples Found**

The third-party service backs up data about once a month.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

The impression is that this frequency is acceptable to the company, so I have no recommendations.

### **Are there off-site backup locations?**

**Explanation**

Off-site backup locations are another arm of the 3-2-1 Backup rule. In the event of an on-site disaster, e.g. fire, earthquake, flood, theft, data can still be recovered.

**Risk**

Failure to create an off-site backup exposes the company’s data to destruction from fire, earthquake, etc.

**Observations/Examples Found**

There are no off-site backup locations.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Something as simple as a lockbox in another location with a hard drive containing vital data or a separate secure cloud storage service would suffice.

### **How often are they backed up?**

(n/a)

# 

# **Physical Security**

# **Potential or Actual Vulnerabilities**

Listed below are the physical security vulnerabilities discovered during the assessment. These are considered significant and steps should be taken to address them. The list is divided into a list of vulnerabilities that relate to the building, the security perimeter, and the server rooms. The building group contains vulnerabilities within the SpenJace office. The security perimeter group includes the exterior office windows, doors, alarm system, and the surrounding area. The server room are specific to rooms containing server equipment.

### **Where is the router stored, and how is it protected?**

**Explanation**

It is important for the router of the network to be kept in a secure location which is simultaneously accessible to Staff and restricted from Guests.

**Risk**

Failure to secure the router means that threat actors can interact with it and potentially harm the integrity of the network as a whole.

**Observations/Examples Found**

The router is stored in a corner to the right of the door, behind two stacks of chairs.

**Documentation**

[See images above, under “Network and Wireless Security” section]

**Recommendations**

Again, investing in a locked glass case to protect the equipment from tampering will help secure this equipment.

### **Where are any permanently wi-fi connected devices stored, and how are they protected?**

**Explanation**

Wi-fi connected devices can include either desktops or pieces of equipment.

**Risk**

Devices which are left unattended and permanently connected to the Wi-fi are key targets for threat actors.

**Observations/Examples Found**

One piece of lab equipment, a remotely accessible test-tube manipulator, is connected to the Wi-fi network, and is kept in the lab area.The machine is only accessible with a specific software driver. The lab area is secured behind a locked glass partition.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Because the machine handles delicate materials which represent many hours of lab work, I would suggest that it be moved onto a more secure Wi-fi network, potentially one reserved for staff and members.

### 

### **Who has access to these locations?**

**Explanation**

Limiting physical access to locations containing important equipment is one way to help protect them from threats.

**Risk**

If anyone is allowed unsupervised access to this equipment, the risk of tampering or abuse is increased.

**Observations/Examples Found**

Only staff, members, and guests accompanied by staff are allowed to access the lab area.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

In the interest of both security and the lab’s status as a community resource, I would recommend maintaining the policy of Guest access given Staff accompaniment for this lab area.

### **Are there any publicly accessible ethernet ports?**

**Explanation**

Ethernet ports allow less restricted and more direct access into the network to which they are connected.

**Risk**

Through bypassing the wireless network and accessing the network directly, a threat actor can have an easier time attacking the network.

**Observations/Examples Found**

There are no public ethernet ports.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

I would recommend keeping ethernet ports protected and monitoring the private ones used by staff.

### **What sort of locks are on the building?**

**Explanation**

When discussing network security, an aspect which must not be ignored is physical security, like the locks on the building and on different rooms or containers.

**Risk**

If physical security is not kept strong, then the risk of equipment theft is increased.

**Observations/Examples Found**

The suite is secured by electronic locks which only open for specific key fobs.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

This system is both sufficient and not within the control of the client (short of changing location), so no recommendation is offered.

# **User Education**

# **Potential or Actual Vulnerabilities**

Listed below are some areas where the users should be instructed in the importance of different security issues.

### **What features of the network are used the most by the users?**

**Explanation**

The most common uses of a network include website browsing, email server access, and file transferring.

**Risk**

Not keeping a general understanding of user activity makes it difficult to know the specific sorts of risks users will face.

**Observations/Examples Found**

The network is mainly just used for internet and email access.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

This is the basic and expected usage, I would only recommend keeping an ear out for users considering any attempts of using it for other reasons.

### **Is there a standard practice when transferring data between staff members?**

**Explanation**

Companies can employ a template for official communications so that an additional layer of security can be evoked and understood by users when handling secure data.

**Risk**

Not having such a standard practice means it would be easier for threat actors to impersonate official individuals and have more success extracting information from users.

**Observations/Examples Found**

There is no standard practice in place.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

I would recommend drafting a standard practice outline for intra-company data transfer. Having users familiar with a standard procedure for transfer of sensitive data between staff will further help to avoid suspicious scams attempting to extract personal information from the staff.

### **What threats are users most vulnerable to?**

**Explanation**

Understanding user activity helps a company identify common threats faced by its users, and from there it can deploy its resources in a way that more appropriately addresses these threats.

**Risk**

Failure to analyze standard user activity and identify common threats can result in incorrect distribution of resources, leaving either more serious vulnerabilities exposed or less serious vulnerabilities over-protected.

**Observations/Examples Found**

Considering users mostly access the internet and email over the network, they would likely be most vulnerable to phishing scams or trojan horse attacks.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

Again, I would recommend drafting the template for secure data transfer to be used by Staff- or Member-level users.

### **Has there been any history of previous data leaks at this network?**

**Explanation**

Keeping a record of data breaches provides an important metric for determining the overall security of a company.

**Risk**

A significant history of data leaks at a company can suggest either a recurring vulnerability of the company or indicate that the company is a high priority target for threat actors and that a higher level of data security is required.

**Observations/Examples Found**

There has been no history of data leaks.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**~~Re~~commendations**

I commend SpenJace for avoiding data leaks.

### **What is the contingency plan for handling a data leak?**

**Explanation**

Companies are encouraged to plan for the possibility of data leaks, be they minor or catastrophic, so that have they have a plan to follow in the event of an emergency.

**Risk**

Failure to prepare a plan for the possibility of data leaks means that time has to be dedicated towards forming a plan when the leak occurs, when time could be dedicated towards taking action and resolving the issue.

**Observations/Examples Found**

The contingency plan is to be forthright and honest with all those affected as soon as information is available.

**Documentation**

Discussed with Flichael, Executive Director (05-Mar-2019).

**Recommendations**

I support SpenJace’s plan of honesty, and would only recommend a bit more specificity, like potentially drafting a template message for such an event.

# Action Plan

My primary recommendation is to install a second Wi-fi network. The first network can be kept public, with the password easily available to visitors, but a second network for staff, members, and Wi-fi enabled lab equipment would have the biggest impact on the general safety of the location.

I recommend either a sign in sheet or a network login system for the laptops so that usage can be kept track of and any attacks using the laptops will be discouraged.

Investing in a secure case for the network equipment as opposed to keeping it in a corner behind some chairs would increase its security and reduce fire hazards.

Taking steps towards building a tiered privilege framework based on user trustworthiness, e.g. into Guests, Members, and Staff, would help future efforts towards keeping user activity organized and legitimate.

Finally, I would suggest drafting a standard practice outline for intra-company data transfer to protect against phishing scams.