# Security Assessment Report

Version N.0

May 1, 2023

# 1. Summary:

This document is to help us increase the security of our image editing program.

## 1. Assessment Scope

We used tools like GitHub and PyCharm. Browsers used included Google Chrome and Microsoft Edge. Our operating system was Windows 11. There were no major limitations.

## 2. Summary of Findings

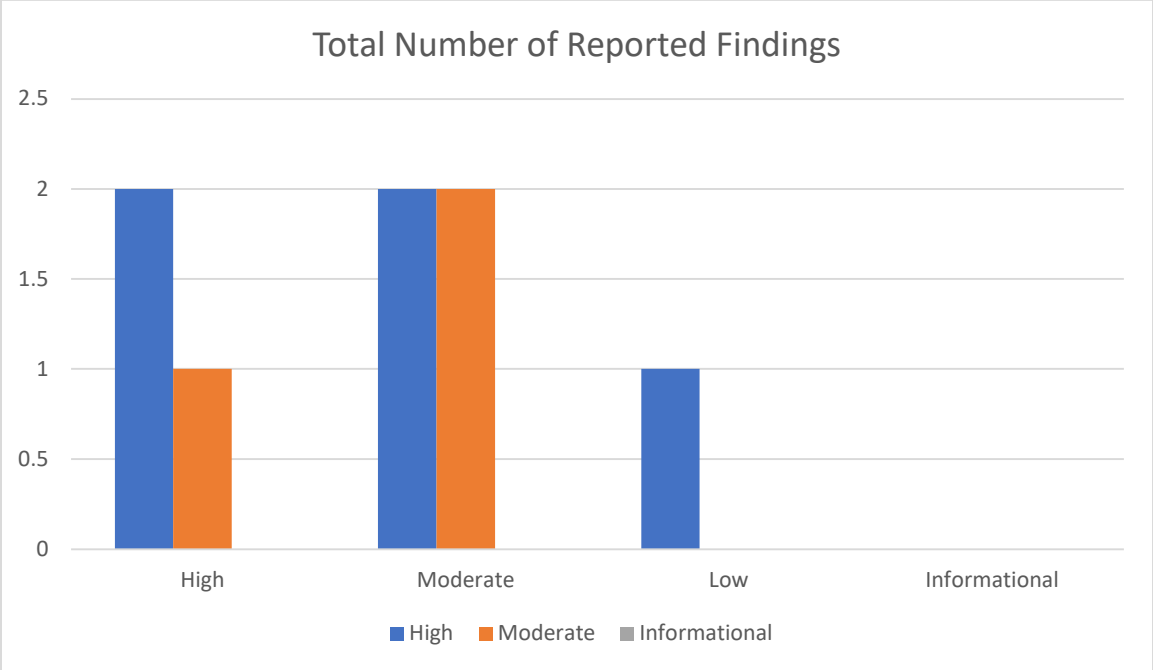


Fig 1. Findings by Risk Level

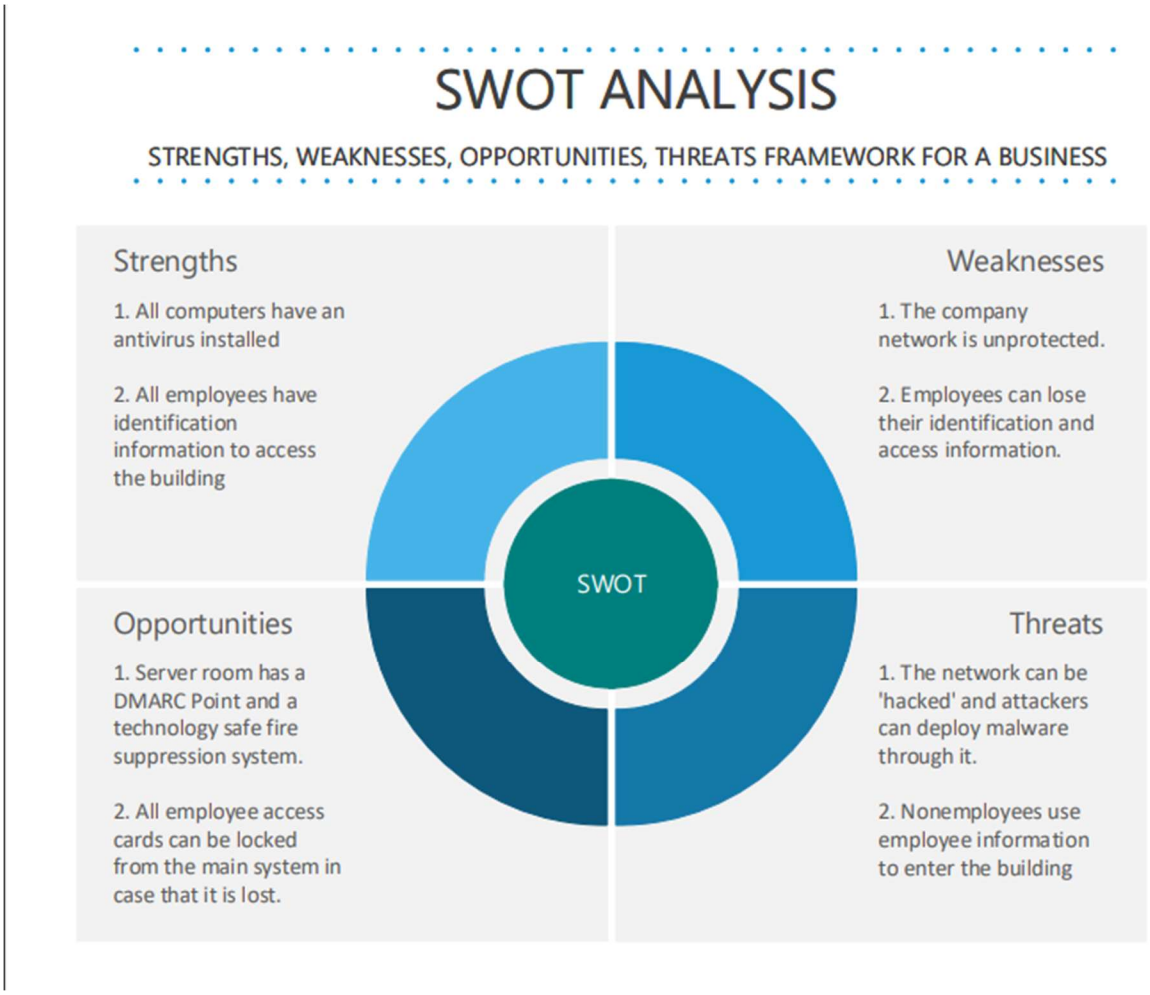


Fig 2. SWOT Analysis

The network for the Computational Vision lab is the university's public network. It has high levels of traffic and, since its public, has very little protection.

To enter our lab, the employees need to bring their identification cards and swipe them. There is a risk of them losing their cards and an unauthorized person gaining access through their identification.

### 3. Summary of Recommendations

While we cannot get a new network, or change the ID scanning process, we have decided to increase the security of our software in cases of a bad actor or error. Our data is encrypted, and new logging systems and tracking systems are being implemented.

## 2. Goals, Findings, and Recommendations:

### 1. Assessment Goals

The purpose of this assessment was to do the following:

- Ensure that the system was in compliance with university regulations and policies.
- Determine if the application was securely maintained.
- Etc.

### 2. Detailed Findings

(Reference Table 1)

- Data from software and machine learning models was unsecured and had no protection from other employees. Anyone could open a computer and either change or delete the data. (High Risk)
- The libraries used in code were not up to date. Code was eventually going to be broken down and become unusable. (Moderate)
- Doors were being left unlocked throughout the day. Even people without ID's would have been able to enter the lab and work on any of the computers/use the equipment.(Moderate)
- Unsecure network. The university network has high traffic and it's public. It becomes unstable often and can be susceptible to attacks. (High Risk)
- Employees were not following ITS Guidelines, which could leave a lot of vulnerabilities out to be exploited. (Low Risk)
- Infrastructure is unreliable and not up to date, which can cause it to disrupt normal operations. (Moderate Risk)
- Server room is unsecured, which makes it vulnerable to attacks from either unauthorized employees who do not know how to interact with it, or from malicious users. (High Risk)

3. Recommendations

(Reference Table 2)

- Encrypt all data – Easy
  It would make it harder for unauthorized users to have access to it.
- Update Libraries- Moderately Difficult (might need to relearn some material, use a new library)
  It would eliminate vulnerabilities.
- Reinforce ITS Guidelines – Easy
  Remind employees of the importance of staying safe, so they don't open up vulnerabilities.
- Use OS Access Control to allow only authorized users to change code – Moderately Difficult
  Separate employees into different groups to allow each access to different materials depending on their work.
- Platform user groups are used to only allow changes to be made to code by authorized individuals. – Moderately Difficult.
  Only programmers would be able to edit the code.
- Physical Security of computer is adequate – Easy
  Not easy to steal or break.
- Accounting Process includes logging (tracking of changes, user making changes, access attempts, etc) – Moderately Difficult
  Allowing employees to see who is working on the project and who makes each changes
- Use Security Testing - Moderately Difficult
  Use more testing to identify more vulnerabilities.

# 3. Methodology for the Security Control Assessment:

## 3.1.1 Risk Level Assessment

Each Business Risk has been assigned a Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in **Error! Reference source not found.** apply to risk level assessment values (based on probability and severity of risk). While Table 2 describes the estimation values used for a risk's "ease-of-fix".

Table 1 - Risk Values

| Rating | Definition of Risk Rating |
|---|---|
| High Risk | Exploitation of the technical or procedural vulnerability will cause substantial harm to the business processes. Significant political, financial, and legal damage is likely to result |
| Moderate Risk | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to organization. |
| Low Risk | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment |
| Informational | An "Informational" finding, is a risk that has been identified during this assessment which is reassigned to another Major Application (MA) or General Support System (GSS). As these already exist or are handled by a different department, the informational finding will simply be noted as it is not the responsibility of this group to create a Corrective Action Plan. |
| Observations | An observation risk will need to be "watched" as it may arise as a result of various changes raising it to a higher risk category. However, until and unless the change happens it remains a low risk. |

Table 2 - Ease of Fix Definitions

| Rating | Definition of Risk Rating |
|---|---|
| Easy | The corrective action(s) can be completed quickly with minimal resources, and without causing disruption to the system or data |
| Moderately Difficult | Remediation efforts will likely cause a noticeable service disruption<br>• A vendor patch or major configuration change may be required to close the vulnerability<br>• An upgrade to a different version of the software may be required to address the impact severity<br>• The system may require a reconfiguration to mitigate the threat exposure<br>• Corrective action may require construction or significant alterations to the manner in which business is undertaken |
| Very Difficult | The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling<br>• An obscure, hard-to-find vendor patch may be required to close the vulnerability<br>• Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity<br>• Corrective action requires major construction or redesign of an entire business process |
| No Known Fix | No known solution to the problem currently exists. The Risk may require the Business Owner to:<br>• Discontinue use of the software or protocol<br>• Isolate the information system within the enterprise, thereby eliminating reliance on the system<br>In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business |

| Rating | Definition of Risk Rating |
|---|---|
| | Owner, and reviewed by IS Management, to validate that security incidents have not occurred |

### 3.1.2 Tests and Analyses

This was completed using:

- Penetration Testing Process: easy to find information about the school/computational vision lab. Moderately Difficult to enter the lab (employees can recognize one another), easy to access code since there was no password/access control.
- White Box Testing: Code functions work well on their own, should hide path names.
- Grey Box Testing: Regression testing was used to ensure that functionality still worked after making some changes.
- Black Box testing: System does what it is required, added security performs as required.
- Tools used and purpose: Wireshark was used to analyze network traffic.
- Analysis of test results or Research into system vulnerabilities:
  While we did find many vulnerabilities, we are working hard to minimize them and make our systems stronger. It is vital that we analyze what attacks are more likely to happen to us based on our work. Since we use a lot of code and machine learning programming, finding what the biggest vulnerabilities are is important. Microsoft has been finding adversarial machine learning attacks, in which hackers try to either delete or alter the data that is being produced. They use common methods like phishing alongside other ML techniques. link to Microsoft blog

# 4. Figures and Code

## 1. Process Flow of System

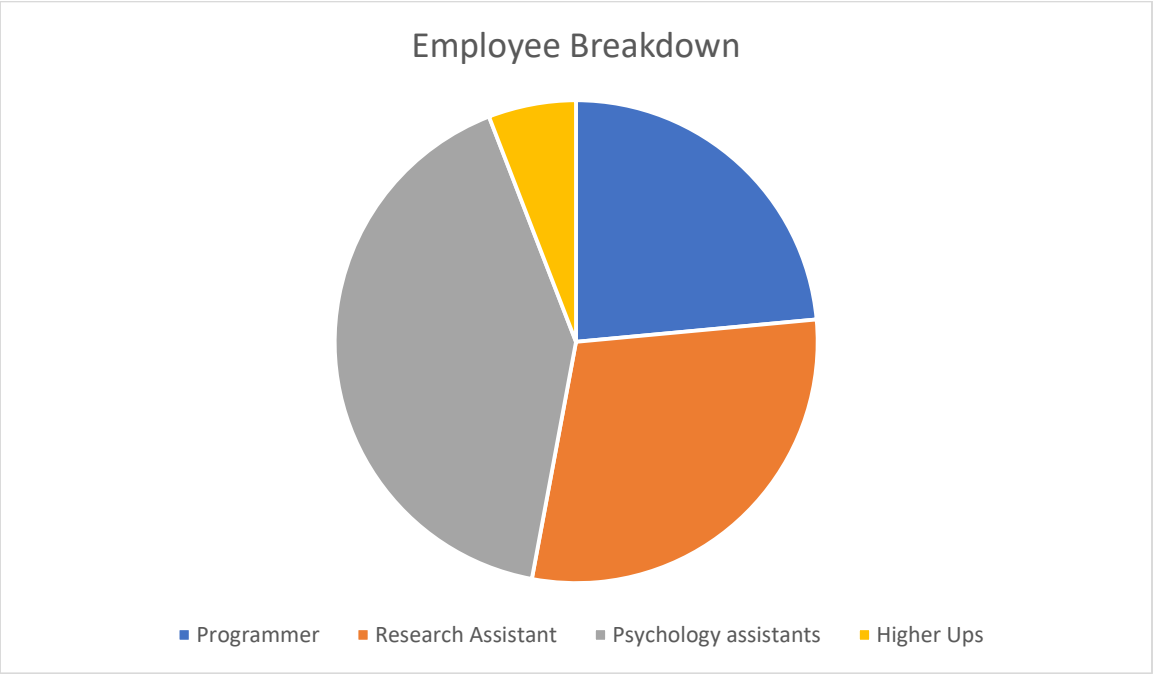


Fig 3. Employee Breakdown of Computational Vision Lab

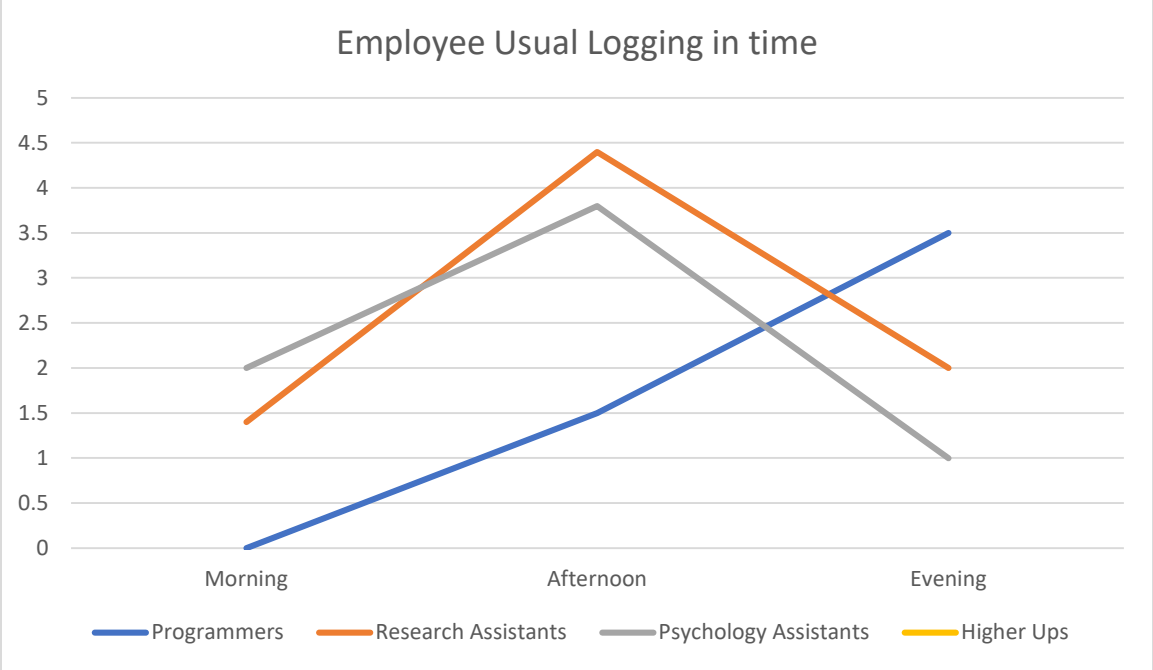

Fig 4. Employee Usual Logging in time

| | | Probability ----------> | Computational Vision Lab | | | |
|---|---|---|---|---|---|---|
| Severity | | Frequent | Probable | Likely | Possible | Rare |
| | Emergency | Network is unsecure and has no password or protection | Sensitive Data is unsecure and has no protection from outsiders or other employees | Overheating server room due to not good enough cooling and ventilation system/ doubling it as storage | Unsecure Server Room with no access control allowing anyone to go in | A sinkhole happens |
| | Major | | | Employees losing their employee information or credentials (keys, ID, etc...) | Tailgatting and piggybacking employees into secured areas | A new epidemy breaks out, causing more work from home and new security issues |
| | Moderate | Unstable network that increases vulnerability | Leaving doors unlocked/opened during the work day or night | Using unreliable infrastructure and not updating can be unreliable | Having no alarms systems in place in case of fires, theft, etc... | Category 4 or 5 hurricane |
| | Minor | Employees not following ITS Guidelines | Not updating the systems that are used can cause problems | Rooms packed with furniture and equipment, making it harder to evacuate in case of emergency | Unclear ITS Guidelines | Power Outage in building, stopping operations |
| | Negatable | Employee coming in late, causing some bottleneck effects in the process of the work day | | | Unorganized area, making it harder to find necessary things, or notice if something is missing | |

Fig 5. Risk Assessment Matrix

## 2. Process Flow of System

```
# Authentication... # from https://www.youtube.com/watch?v=Axi
username = "programmer"
password = "comp_vis"
uname = input("Enter a username: ")
uname = uname.strip() # removes spaces from before and after s
if uname != username:
    print("Incorrect username. Please try again.")
else:
    pwd = getpass.getpass()  # hides the password
    if pwd == password:
        print("Username and Password verified. Welcome.\n")
        print("Image Processing Program" + "\n")
        # Menu Options
        print("Choose one of the following options:\n")
        print("1. Resize images \n"
              "2. Crop images \n"
              "3. Extract image patches\n")
        choice = int(input("Enter choice here: "))
```

Fig 6. Authentication

```
# Libraries
import os
import cv2
from patchify import patchify
import tifffile as tiff
from PIL import Image
import getpass # module for authentication
```

Fig 7. Libraries

## 5. Works Cited


Samia Zaigham. “Python: Using Getpass to Enter Password.” *YouTube*, 21 Apr. 2020, www.youtube.com/watch?v=AxicSoTyMho.

Kumar, Ram Shankar Siva, and Ann Johnson. “Cyberattacks Against Machine Learning Systems Are More Common Than You Think.” *Microsoft Security Blog*, Mar. 2021, www.microsoft.com/en-us/security/blog/2020/10/22/cyberattacks-against-machine-learning-systems-are-more-common-than-you-think.

“Resizing Multiple Images in a Folder With Different Format.” *Stack Overflow*, stackoverflow.com/a/65585025.

DigitalSreeni. “Python Tips and Tricks - 5: Extracting Patches From Large Images and Masks for Semantic Segmentation.” YouTube, 23 Mar. 2021, www.youtube.com/watch?v=7IL7LKSLb9I.

“How to Crop All Pictures in a Folder and Save It to Another Folder by Python.” *Stack Overflow*, stackoverflow.com/a/68775392.

TryHackMe. “TryHackMe | Cyber Security Training.” *TryHackMe*, tryhackme.com/dashboard.

“---.” *Stack Overflow*, stackoverflow.com/a/65585025.