# Risk Assessment

**Learner Name: Chris Misch**

## Risk 1: Phishing Attack

### Describe risk or vulnerability:

Phishing is a social engineering attack where it looks for the weakest link in your network. Typically, it is your employees. The attacker will send out a phishing or whaling email getting the recipient to click on a link or download an attachment (trojan horse) that contains malware. If the recipient clicks on the link, it could open a malicious website that could track the user to gain information on what sites and applications they are using. By clicking on the link, it could also cause malicious script to run.

### Assess degree of risk and impact:

#### Degree of risk

Rate the degree of risk on a 5-point scale, with 1 being “very unlikely to occur” and 5 being “very likely to occur” and justify your assessment:

**1 2 3 4 5**

Justification:

This is very likely to occur because of inadequate security training for the current and new employees. It is getting harder to tell what a legitimate email is. Attackers have become very crafted in creating official looking emails. The only way to tell is to look for misspelled words or if the email address is not an official email address.

#### Impact

Rate the degree of impact on a 5-point scale, with 1 being “low impact” and 5 being “very high impact” and justify your assessment:

**1 2 3 4 5**

Justification:

The impact would be loss of integrity and confidentiality due to data leakage and network application penetration. This could be due to stolen credentials or holes within the internal Anchor Hospital network.

### Proposed controls for Risk 1 (Risk 1 only):

* **Mitigation:** Add spam filters to the email server and educate employees about knowing how to tell the difference between a legitimate email and nonlegitimate email. Implement controls that prevent direct download of files from the email server and prevent HTTP links without certificates from being accessed.
* **Procedure:** Configure the antivirus software to scan all documents before they are downloaded from a user’s email account. Set up IDS to block non-HTTPS connections via Anchor email accounts.
* **Policy:** Each year employees will be retrained on a best practice review on how to identify phishing and whaling attacks and who to notify if you suspect an email is illegitimate.

## Risk 2: DDOS Attack

### Describe risk or vulnerability:

A DOS (Denial of Service) or DDOS (Distributed Denial of Service) attack is where Anchor Hospital’s network is halted due to an abnormally large amount of TCP, UDP, or ICMP packets being sent to the network. A malicious attack could use a simple program to attack the network from outside or inside the Anchor Hospital’s network.

### Assess degree of risk and impact:

#### Degree of risk

Rate the degree of risk on a 5-point scale, with 1 being “very unlikely to occur” and 5 being “very likely to occur” and justify your assessment:

**1 2 3 4 5**

Justification:

This a high level of risk because it can cause the loss of availability to Anchor Hospital’s systems and network. Without proper load balancing and extra bandwidth, Anchor Hospital will not be able to take proper steps to mitigate this kind of attack.

#### Impact

Rate the degree of impact on a 5-point scale, with 1 being “low impact” and 5 being “very high impact” and justify your assessment:

**1 2 3 4 5**

Justification:

This has a high impact rating due to the scale of which it can stop Anchor Hospitals ability to perform day-to-day operations.

## Risk 3: SQL Injections

### Describe risk or vulnerability:

SQL Injection attacks try to inject SQL code into a webserver to access sensitive data. A malicious user can input SQL code into a comment field to extract information for SQL tables. This happens because user data is not validated, filtered, or sanitized properly by the web application.

### Assess degree of risk and impact:

#### Degree of risk

Rate the degree of risk on a 5-point scale, with 1 being “very unlikely to occur” and 5 being “very likely to occur” and justify your assessment:

**1 2 3 4 5**

Justification:

Injection attack is the third most severe category in 2022 according to OWASP Top 10. It is down from last year, but it is still high on the list.

#### Impact

Rate the degree of impact on a 5-point scale, with 1 being “low impact” and 5 being “very high impact” and justify your assessment:

**1 2 3 4 5**

Justification:

The impact of an injection attack will cause loss of confidentiality of Anchor Hospital’s data servers. The information obtained could be used against the hospital or individuals that have been compromised.

## Risk 4: Vulnerable and Outdated Components

### Describe risk or vulnerability:

Outdated or unused components in the network can allow someone to move vertically or horizontally without being noticed. This also included outdated software patches and unused applications. If a component is attached to the network but is no longer managed or updated a malicious hacker could use it as a stepping post to other components or even add backdoors to it.

### Assess degree of risk and impact:

#### Degree of risk

Rate the degree of risk on a 5-point scale, with 1 being “very unlikely to occur” and 5 being “very likely to occur” and justify your assessment:

**1 2 3 4 5**

Justification:

The risk of this has been coming down according to OWASP Top 10. With only 3 CVEs mapped to it the average weighted impact is at 5. However, Anchor Hospital uses many different IoT medical devices that could be affected.

#### Impact

Rate the degree of impact on a 5-point scale, with 1 being “low impact” and 5 being “very high impact” and justify your assessment:

**1 2 3 4 5**

Justification:

The impact of this risk could impact the confidentiality, integrity, and availability of Anchor Hospital by allowing someone into the system with easy access to the internal network. This could also impact IoT devices in the hospital. These devices are not always updated by the vendor.