

# DRT FRAMEWORK

Version 1.0

December 02, 2022

## **Table of Contents**

|  |    |
|--|----|
| <b>Table of Contents</b>                         | 2  |
| <b>About the Framework</b>                       | 3  |
| Dimensions                                       | 3  |
| Security   | 3  |
| Infrastructure                                   | 4  |
| Risk and Infrastructure Scores                   | 4  |
| Algorithms                                       | 5  |
| Budgetary considerations                         | 5  |
| Considerations for budgets and score-generations | 6  |
| Reporting  | 6  |
| Appendices                                       | 6  |
| <b>How to use this framework</b>                 | 7  |
| Overview   | 7  |
| Using the Visualizer                             | 7  |
| <b>Liability</b>                                 | 9  |
| <b>Case Studies</b>                              | 10 |
| Low-budget case study                            | 10 |
| Overview   | 10 |
| Information-gathering phase                      | 10 |
| Using the Framework (visualizer)                 | 12 |
| Next steps                                       | 13 |

## About the Framework

This section explains what the framework is and how to use it. It also provides recommendations on how to extend or modify the core principles outlined in this playbook.

### Dimensions

The framework discusses two major dimensions that a consultant would need to consider throughout the lifecycle of the contract. These dimensions are “security” and “infrastructure.” By defining a clear and manageable scope for both of these areas, the consultant can begin to provide value to the organization while avoiding common pitfalls.

Interestingly, the research shows that, if a consulting party can enumerate the inventory for both dimensions, then pitfalls in one will often lead to a corresponding issue or weakness in the other. For example, suppose a network

#### Security

Although this dimension encapsulates everything related to security (including physical or perimeter security), this framework places an emphasis on I.T. Security specifically. For small and mid-sized businesses, the emphasis is on Network Security in particular. The research suggests that many of these organizations are more likely to use effective physical security (perimeter and internal cameras), third-party applications or services to build web applications (such as Wix), and so forth.

In general, NetSec is still a “blind spot” for many organizations; the consultant will find it manageable to focus on this dimension first, then branch out to others on a needs basis. For example, if the organization uses a legacy point-of-sale system written in C++, the consultant should identify this as an area of risk. On the other hand, if they host their web applications in something like GoDaddy, and use the platform’s site-builder, this is out-of-scope; otherwise, the consultant would need to write a contract to test the third-party platform, and among other concerns, this alone would imply liability.

This should provide a narrow-enough scope for the consultant to bring value to the organization, while at the same time avoiding “scope creep.” This scope also helps the consultant avoid liability by preventing them from speaking to a security field with which they may have little or no experience.

## Infrastructure

In this framework, “Infrastructure” refers to the components of the on-premise worksite that facilitate the business needs through the I.T. structures. The framework emphasizes the “Network” portion of this because networking is a common blind-spot with small and mid-sized businesses.

The infrastructure is considered with respect to its ability to add performance; for example, if Wi-Fi is used, can everyone in the building connect with usable speeds? In some cases, the placement of the organization’s hotspots are the root cause; in other cases, ideal performance and wireless-network ranges will never fully become realized because of the physical properties of the building (for example, because the walls are made of materials that naturally block radio frequencies). For many organizations, a cable-management inventory is essential to identifying the root causes of performance issues.

## Risk and Infrastructure Scores

One major goal of this framework is to generate a score for risk and infrastructure. Each metric is valuable; however, the meaning will differ with respect to the organization. A healthy organization will yield a low risk score and a high infrastructure (performance) score. Conversely, a high risk or low infrastructure score will provide a consultant with the opportunity to discuss the weaknesses in the organization. Although this second case is unfavorable for the client, it does effectively become the opportunity for the consultant to provide tangible recommendations, set a clear scope-of-work, and ultimately provide value to the customer.

It should be noted that each score is more like a “starting point” for the process of providing recommendations. Each is based on the results of security and I.T. experts, along with well-established security and networking research. With that in mind, a consultant should be careful to explain the meaning of each result, and not to rely on it as a means unto itself. In other words, if a client brings in *another*, well-informed party to audit either score, it is the consultant’s responsibility to speak to the context and concrete meanings behind each score. Failure to do so will ultimately undermine the consultant’s reputation and, likely, their business.

Each score is built on several questions for each dimension. These questions are driven by algorithms (even very simple ones) as well as budgetary considerations (for the client). Each of these have their own rationales and caveats.

Finally, these “total” scores should have some kind of clear, simple meaning. The framework’s creators encourage the use of simple states like “ACCEPTABLE” and “NEEDS IMPROVEMENT.” This provides the client with a simple meaning to digest each individual metric as well as the aggregate metrics. Ultimately, the client is encouraged to use nomenclature

and terms that resonate with their audience, while still holding true to the meaning of each dimension's scores. Failure to interpret the numbers in a way that is meaningful for client could cause the client to lose faith in the consultant's ability to faithfully perform their work.

## Algorithms

For each dimension, there is a set of questions, each of which has a corresponding algorithm. The goal of each algorithm is to determine the score for that question alone. A collection of question scores becomes the overall "risk" or "infrastructure" score for that dimension. The framework's creators provide their recommendations for how to rate the risk or infrastructure of each question given a low-budget organization.

For example, a small business with a single router implies far less risk than an enterprise that uses the same kind of network. Conversely, a small business with ten routers may find itself using stale technology that someone set up and no one maintains anymore. This second case implies a lot more risk for a small business because unmaintained devices can be tampered without anyone knowing.

With that in mind, the framework is intentionally flexible. It avoids any concrete implementation of any algorithm because of the nature of business and the ever-changing nature of I.T. Security and Infrastructure. In general, the consultant is encouraged to tweak the algorithms that generate scores if it is appropriate or necessary for conveying a meaningful snapshot of the organization. The goal is not to rely on fixed numbers, but to leverage meaning through the numbers that are generated.

## Budgetary considerations

Budget is considered in this framework insofar as financial means can drive a client's ability to actually implement change in the organization. The framework's creators promote three "generic" categories of budget: low, medium, and high. The low and high budget ranges should be fairly easy to identify; we can infer that a local coffee shop will almost certainly have a low budget, whereas an enterprise software company might have a high budget. Defining the "medium" budget ranges is not fixed; however, there is still a need to identify these organizations, as they are often just large enough to find themselves the target of a security incident, but just small enough not to be taken seriously when trying to proactively implement security controls or infrastructure improvements.

The consultant is encouraged to use the budget as a means to tune their recommendations and implementation plan. This is normal in most software I.T. business models, regardless of the specialization or specifics of the implementation. The framework's creators recognize the

importance of “putting the client first” as the means to maintaining a healthy professional relationship.

### Considerations for budgets and score-generations

In general, the consultant is encouraged to prioritize the organization’s budget over any algorithm. Failure to do so could result in an inability for the consultant’s vision to be realized. The creators of the framework promote the idea that “perfection should never be the enemy of greatness.” In other words, if the client cannot afford to implement a consultant’s vision and plan, the contract will almost certainly find itself at risk, because no one can afford to implement it. In such a case, it makes sense to scale back the price of the changes in order to find a compromise.

### Reporting

The goal of the reporting section is to present aggregate metrics and the results of each dimension’s score. All data should be presented in a way that is digestible at a high level; information here is conveyed at a high level.

The framework’s creators provide the following recommendations for starting points based on the two key dimensions:

- **Risk score:** Lower scores are better
- **Infrastructure score:** Higher scores are better
- For each score, the top  $N$  weaknesses
- Graphs showing the total scores after the implementation plan is completed
- Total budgetary needs to implement changes

The top weaknesses should map to a question from the dimension’s set of questions.

### Appendices

The appendices will be any list or collection of information that is necessary for the implementation plan, but is not necessary to generate metrics. The consultant can and should track arbitrary information about the client. This could include a list of routers, compatible and up-to-date wiring, and so forth. While these are useful, they are not essential to the framework per se. These can change depending on the client and budget. In addition, the consultant is encouraged to make appendices that are specialized to the client. (Beef this section up.)

# How to use this framework

## Overview

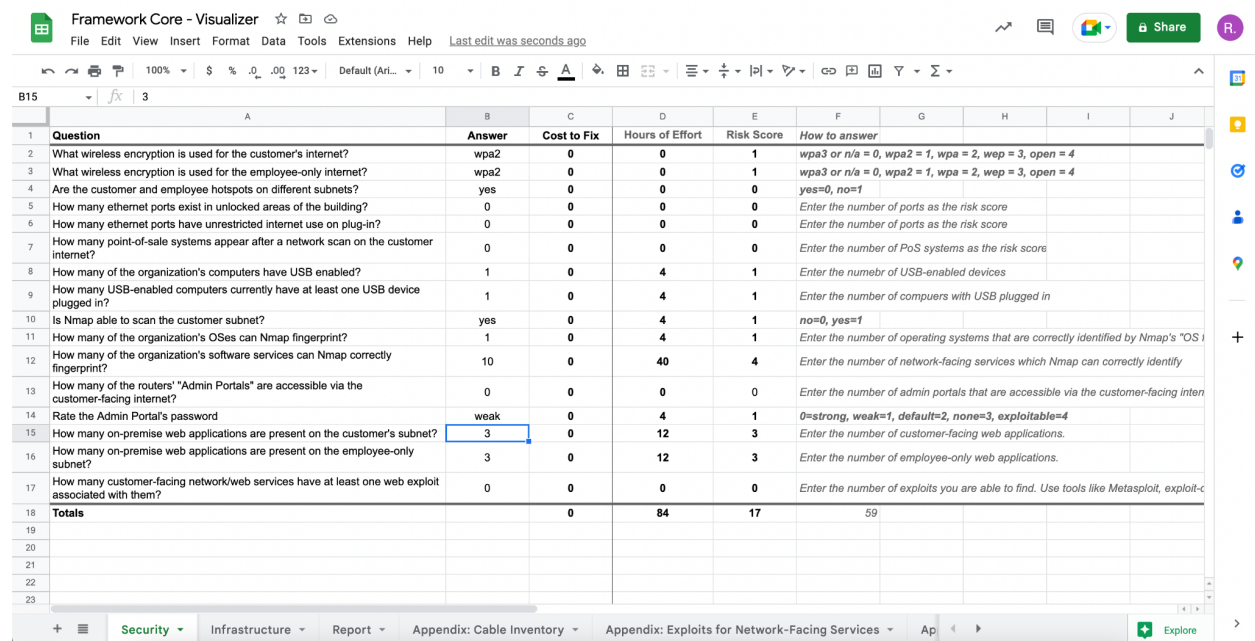
This framework will provide a budget outline for any given organizations IT and Cybersecurity company needs based on three budget tiers: high, medium, and low. This framework will outline some of the mitigation tactics within existing frameworks and provide solutions through a framework and the mentioned budget tiers.

This framework is not meant to take the place of any existing frameworks or guidelines an organization has in place; instead, it is meant to provide insight into possible Cybersecurity/IT necessities and how to include them within day-to-day operations or to use with an already established framework within an organization.

The budgets provided within this framework are for the reader to gain insight on how much it will cost to mitigate the outlined Cybersecurity/IT case study/problem. These budgets are for knowledge purposes and are not to be taken as mandatory assignments per each case study.

## Using the Visualizer

The creators of this framework offer an Excel spreadsheet to help all stakeholders understand the reporting process. The following figure shows the “Security” dimension with pre-populated data.



The screenshot displays the 'Framework Core - Visualizer' Excel spreadsheet. The 'Security' tab is selected, showing a table with columns: Question, Answer, Cost to Fix, Hours of Effort, Risk Score, and How to answer. The table contains 17 rows of security-related questions and their corresponding metrics. The 'Totals' row shows a total cost of 0, 84 hours of effort, and a risk score of 17. The 'How to answer' column provides instructions for each question.

| Question  | Answer | Cost to Fix | Hours of Effort | Risk Score | How to answer   |
|---|--------|-------------|-----------------|------------|---|
| What wireless encryption is used for the customer's internet?                                     | wpa2   | 0           | 0               | 1          | wpa3 or n/a = 0, wpa2 = 1, wpa = 2, wpa = 3, open = 4                                   |
| What wireless encryption is used for the employee-only internet?                                  | wpa2   | 0           | 0               | 1          | wpa3 or n/a = 0, wpa2 = 1, wpa = 2, wpa = 3, open = 4                                   |
| Are the customer and employee hotspots on different subnets?                                      | yes    | 0           | 0               | 0          | yes=0, no=1   |
| How many ethernet ports exist in unlocked areas of the building?                                  | 0      | 0           | 0               | 0          | Enter the number of ports as the risk score   |
| How many ethernet ports have unrestricted internet use on plug-in?                                | 0      | 0           | 0               | 0          | Enter the number of ports as the risk score   |
| How many point-of-sale systems appear after a network scan on the customer internet?              | 0      | 0           | 0               | 0          | Enter the number of PoS systems as the risk score                                       |
| How many of the organization's computers have USB enabled?  | 1      | 0           | 4               | 1          | Enter the number of USB-enabled devices   |
| How many USB-enabled computers currently have at least one USB device plugged in?                 | 1      | 0           | 4               | 1          | Enter the number of computers with USB plugged in                                       |
| Is Nmap able to scan the customer subnet?   | yes    | 0           | 4               | 1          | no=0, yes=1   |
| How many of the organization's OSes can Nmap fingerprint?   | 1      | 0           | 4               | 1          | Enter the number of operating systems that are correctly identified by Nmap's "OS I     |
| How many of the organization's software services can Nmap correctly fingerprint?                  | 10     | 0           | 40              | 4          | Enter the number of network-facing services which Nmap can correctly identify           |
| How many of the routers' "Admin Portals" are accessible via the customer-facing internet?         | 0      | 0           | 0               | 0          | Enter the number of admin portals that are accessible via the customer-facing inter     |
| Rate the Admin Portal's password  | weak   | 0           | 4               | 1          | 0=strong, weak=1, default=2, none=3, exploitable=4                                      |
| How many on-premise web applications are present on the customer's subnet?                        | 3      | 0           | 12              | 3          | Enter the number of customer-facing web applications.                                   |
| How many on-premise web applications are present on the employee-only subnet?                     | 3      | 0           | 12              | 3          | Enter the number of employee-only web applications.                                     |
| How many customer-facing network/web services have at least one web exploit associated with them? | 0      | 0           | 0               | 0          | Enter the number of exploits you are able to find. Use tools like Metasploit, exploit-c |
| Totals  |        | 0           | 84              | 17         | 59  |

## *DRT Framework: User Guide*

Please note that the visualizer is just a tool. It is the consulting party's responsibility to use this tool correctly.



## **Liability**

This framework is voluntary not mandatory. All of the outlined information is meant to be taken as suggestions and used as a means to gain knowledge.

A consultant or owner who utilizes this framework shall do so with the understanding that the framework cannot cover every single security or infrastructure need. Security incidents, network outages, and “acts of God” will happen even in the most robust networks. Liability is waived for the creators of this framework. If this framework is used by a consultant, it is assumed that the consulting party should have their client sign a waiver for their own liabilities.

Finally, it is the responsibility of the party who uses this framework to ensure responsible usage of the principles described here. Failure to implement this faithfully or responsibly is the sole responsibility of said party, not the creators.

Further, said party is responsible for creating any liability waivers for any processes that they are performing which exist outside the scope of this document; such procedures include specific survey questions, recommendations, or implementation. The authors recommend that the party who uses this framework create a liability waiver, with the help of legal consultation, prior to the engagement. This includes any preliminary work, such as network scans or employee questionnaire.

## Case Studies

### Low-budget case study

#### Overview

This case study was performed on a real organization, a restaurant, whose name will remain redacted. For this case study, we use our Excel-based organizer. The primary goal is to prove that we can generate metrics for each category regardless of the organizer. The benefit of using the organizer is that it automates the aggregate data.

The secondary goal is to prove that, if the implementation of each section ever changes (for example, the business logic that drives the Risk Score), the framework as an abstraction will still have merit. This second goal is crucial for the framework overall; it ensures that a consultant has the flexibility they need to modify the framework in whatever way best fits their clients.

#### Information-gathering phase

With the help of the organization, the authors of this document were able to gather necessary metrics. For example:

- On average, the organization receives about 5 - 30 patrons. This implies that, on busier nights, the potential for a threat actor to “blend in with the crowd” may prove easier.
- On average, between 3 and 5 customers are on the “guest” network at any given time. This implies that it may be easier to balance the load of any group on the network at a given time. It also implies that it may prove easier to identify a threat actor using nothing but “triangulation,” using the actual wireless signal strength from all routers in order to identify a person in the physical building.
- Orders are mostly managed through a Toast application. This allows customers to place their own order at any time. The service staff will see new orders and bring them to the bar or tables. The organization does have one point-of-sale system, an electronic Square interface, which has no lockout policy.
- No ethernet or hardwire ports are available for the general public. This is a good thing because, as a “game oriented” establishment, sometimes ethernet is provided for LAN parties or for optimized network speeds. By not offering this as an option, the organization prevents that attack vector from being abused by a malicious actor.

- The organization uses three routers. Two of them are reserved for use by the customers. One is tied to a private subnet which is restricted to employee-only use. Although they did not yield what the pre-shared key (password) is, they did agree that it was “guessable if someone really, really tried.”
- Port 22 (FTP) appears on Nmap scans as **Filtered**. This is a red flag as FTP is an insecure protocol. An attacker who can intercept this traffic will be able to see the plaintext contents of any messages or files. However, a filtered port is typically infeasible to attack via common methodologies; this may slow down an attacker who is trying unconventional methodologies of attacking the port or the underlying FTP service (the application or service itself), but the contents are nonetheless visible.

Although these points are not comprehensive, they should provide the reader with a clear idea of the size and scope of the organization.

To build on these findings, we performed a network scan, which yielded the following results:

```
~ % nmap 10.0.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-01 17:24 EST
Nmap scan report for 10.0.0.1
Host is up (0.0026s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
548/tcp   open      afp
631/tcp   open      ipp
8080/tcp  open      http-proxy
20005/tcp open      btx
49152/tcp open      unknown
49153/tcp open      unknown

Nmap scan report for 10.0.0.4
Host is up (0.000044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
5000/tcp  open      upnp
7000/tcp  open      afs3-fileserver
```

## DRT Framework: User Guide

```
Nmap scan report for 10.0.0.25
Host is up (0.0050s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE
5000/tcp  open  upnp
7000/tcp  open  afs3-fileserver
7100/tcp  open  font-service
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
62078/tcp open  iphone-sync

Nmap done: 256 IP addresses (3 hosts up) scanned in 29.40 seconds
```

The organization wished that we limit our activity on their network. So, this case study will stop short here. The reader is encouraged to consider a true “threat modeling” any time they assess the network.

### Using the Framework (visualizer)

In the first test case, a real organization’s security posture is assessed. The consultant is able to take inventory and perform security reconnaissance to gather the relevant information. Their findings are entered into the organizer as shown in the following figure.

| Question  | Answer | Cost to Fix | Hours of Effort | Risk Score | How to answer   |
|---|--------|-------------|-----------------|------------|---|
| What wireless encryption is used for the customer's internet?                                     | wpa2   | 0           | 0               | 1          | wpa3 or n/a = 0, wpa2 = 1, wpa = 2, wep = 3, open = 4   |
| What wireless encryption is used for the employee-only internet?                                  | wpa2   | 0           | 0               | 1          | wpa3 or n/a = 0, wpa2 = 1, wpa = 2, wep = 3, open = 4   |
| Are the customer and employee hotspots on different subnets?                                      | yes    | 0           | 0               | 0          | yes=0, no=1   |
| How many ethernet ports exist in unlocked areas of the building?                                  | 0      | 0           | 0               | 0          | Enter the number of ports as the risk score   |
| How many ethernet ports have unrestricted internet use on plug-in?                                | 0      | 0           | 0               | 0          | Enter the number of ports as the risk score   |
| How many point-of-sale systems appear after a network scan on the customer internet?              | 0      | 0           | 0               | 0          | Enter the number of PoS systems as the risk score   |
| How many of the organization's computers have USB enabled?  | 1      | 0           | 4               | 1          | Enter the number of USB-enabled devices   |
| How many USB-enabled computers currently have at least one USB device plugged in?                 | 1      | 0           | 4               | 1          | Enter the number of computers with USB plugged in   |
| Is Nmap able to scan the customer subnet?   | yes    | 0           | 4               | 1          | no=0, yes=1   |
| How many of the organization's OSes can Nmap fingerprint?   | 1      | 0           | 4               | 1          | Enter the number of operating systems that are correctly identified by Nmap's "OS fingerprinting" |
| How many of the organization's software services can Nmap correctly fingerprint?                  | 10     | 0           | 40              | 4          | Enter the number of network-facing services which Nmap can correctly identify                     |
| How many of the routers' "Admin Portals" are accessible via the customer-facing internet?         | 0      | 0           | 0               | 0          | Enter the number of admin portals that are accessible via the customer-facing internet            |
| Rate the Admin Portal's password  | weak   | 0           | 4               | 1          | 0=strong, weak=1, default=2, none=3, exploitable=4  |
| How many on-premise web applications are present on the customer's subnet?                        | 3      | 0           | 12              | 3          | Enter the number of customer-facing web applications.   |
| How many on-premise web applications are present on the employee-only subnet?                     | 3      | 0           | 12              | 3          | Enter the number of employee-only web applications.   |
| How many customer-facing network/web services have at least one web exploit associated with them? | 0      | 0           | 0               | 0          | Enter the number of exploits you are able to find. Use tools like Metasploit, exploit-db, etc.    |
| Totals  |        | 0           | 84              | 17         | 59  |

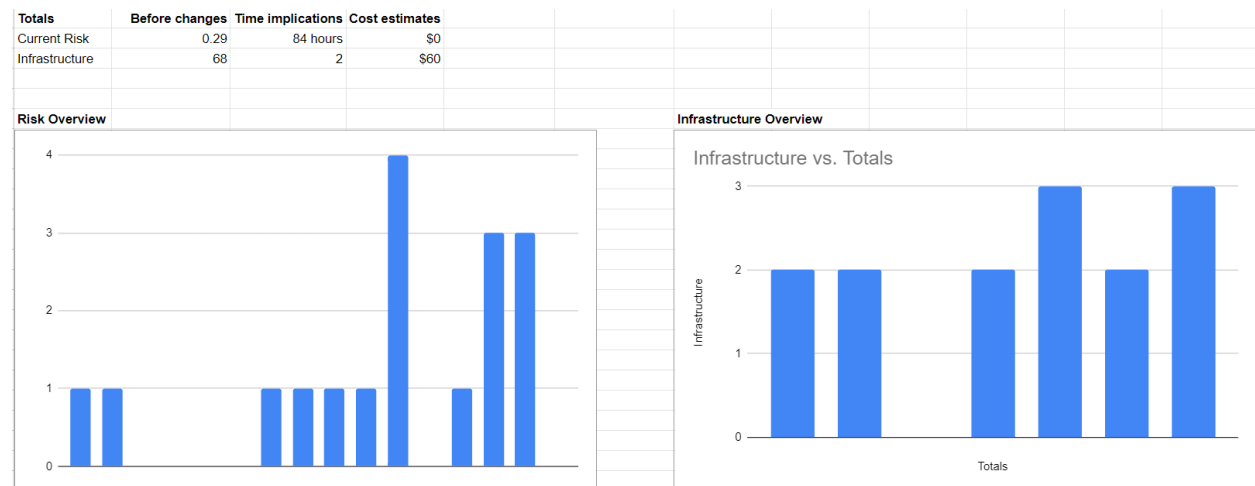
In this case, the correct **Totals** were generated: cost to fix, hours of effort (estimated), and the risk score (out of 59 possible points).

Next, the organization's network is assessed and documented in the following figure.

| Question  | Answer   | Cost to Fix | Hours to Fix | Infra. Score | How to answer  |
|---|----------|-------------|--------------|--------------|--|
| What is the network speed in MBPS while on the cusomter network?  | <100MBPS | \$30        | 1            | 2            | <25MBPS = 0, <50MBPS = 1, <100MBPS = 2, <150MBPS = 3, 150MBPS+ = 4             |
| What is the network speed in MBPS while on the internal network?  | <100MBPS | \$30        | 1            | 2            | <25MBPS = 0, <50MBPS = 1, <100MBPS = 2, <150MBPS = 3, 150MBPS+ = 4             |
| How many customer devices are using hardwired ethernet?   | 0        | 0           | 0            | 0            | Enter the number of devies using hardwired internet. Lower is better           |
| How many of the organization's devices (ex. point of sale systems or company PCs) are using hardwired ethernet? | 2        | \$0         | 0            | 2            | Enter the number of employee-only devices using ethernet. Higher is better     |
| What is the average Wi-Fi signal for all hotspots (in -dBm)?  | -34      | 0           | 0            | 3            | Enter the average hotspot connection across the building. Lower is better      |
| Which wireless protocol is used for the customer hotspots?  | n        | 0           | 0            | 2            | <g=0, g=1, n=2, ac=3, ax=4   |
| How many yards of CAT5 cable (estimate) are used on premise?  | 100      | 0           | 0            | 3            | Enter an estimate of the number of yards of CAT5 cable needed. Lower is better |
| Totals  |          | \$60        | 2            | 14           |  |

The data shows that this network is fairly well put together. The biggest blind spot is the download speeds. The consultant will encourage the organization to upgrade their internet speeds. Doing so will allow the organization's Wi-Fi network to remain stable during peak hours with many customers. This holds true to the framework's goal with respect to infrastructure improvements.

The report should present an aggregate of all data, along with a high-level visual of the different questions from each dimension. This is shown in the following figure.



## Next steps

In this case study, the organization was willing to sit down and consider their security posture. The organization stakeholders were appreciative for the opportunity to consider these weak points more in depth and to look ahead at possible changes to the worksite. Although a true implementation plan was not covered in this case study, we recommended the following next steps:

Website: <https://fangs-five.github.io>

- Move the service on port 22 to a non-standard port (above port 1023). The idea of a potential FTP server is seductive to a novice attacker. As this organization is close to a university, the potential for “script kiddies” and other amateur attackers is very high. Likewise, a conversation was held about the use of FTP, although this will not be repeated here.
- Update the password. If the employees found the password weak, the administrator should update it to a hardened, unguessable value. This could be stored in a password wallet, which is shared among owners or managers, and distributed or used on a needs basis. A 24-character pre-shared key, generated by a tool like Bitwarden or 1Password, is preferred to a simple, guessable one. To complement this, a password policy was recommended, which the stakeholders have taken into consideration.
- Update the ethernet cables. Many of the cables had been in use for about a decade. By replacing them with modern cables, the organization can be prepared for any future workloads which may stress the network.
- Set a lock-timeout for the digital point-of-sale system. Doing so will prevent unauthorized access to the system over a short period of time. Since the PoS system is not really used (compared to the Toast application), there is no great business reason to keep this unlocked for a generous amount of time.