***Part A***

We are currently in living in times where the demand for cybersecurity skills has rapidly increased however the supply of the skills for the role have remained relatively unresponsive. We are currently living in times where almost every application in our lives is being digitalized and computers and connected devices are reaching further than ever before, and this trend will continue without a doubt. This makes for a difficult situation as we are becoming more and more vulnerable to the threat that cybersecurity presents. Every one would like to be able to be in an environment where they can fully trust their mobile phones, personal computers, even cars will remain secure and not leak data, become unreliable/unresponsive, or make sudden incorrect adjustments for vehicles, leading to catastrophic accidents.

As a result, those who have such perceived cybersecurity skills benefit from a seller’s market. Those who need people with cybersecurity skills pay higher prices or have unfilled positions. Within the U.S. federal government (e.g., within the Department of Defense [DoD]), the rising demand for cybersecurity skills cuts more sharply because government salaries are very difficult to change in the short term (it usually takes a promotion or a time-in-grade increase) and tend to be inflexible (in comparison to private salaries) even in the medium and long term. Thus, even as many proclaim the advent of cyberwar as a decisive component of modern warfare, others argue that DoD has a difficult time acquiring the people to wage that kind of war.[1]

Those pursuing a career in this field will need to have a broad set of technical, professional, and functional skills, as well as the specific cybersecurity skills and key soft skills in demand by employers that will set you apart from the competition. We've created a list of top cybersecurity skills to help you see what it takes to be a professional in the cybersecurity field. As a cybersecurity professional, problem-solving will play a major role in your day-to-day work. Those in the field need to find creative ways to take on and address complex information security challenges across a variety of existing and emerging technologies and digital environments.

As the name implies, cybersecurity is a technology-focused field: you will be likely be tasked with responsibilities such as troubleshooting, maintaining, and updating information security systems; implementing continuous network monitoring; and providing real-time security solutions. Being technologically savvy is essential in order to perform the daily activities of a cybersecurity professional.

As with any technical field, cybersecurity is fast-changing. Anyone who works in the field will need to be committed to keeping current with best practices and emerging industry trends, and will always need to be learning and self-educating - both on and off the clock.[2]

The global cybersecurity skills shortage has fallen for the second consecutive year, but the size of the workforce is still 65% below what it needs to be, according to the latest figures from (ISC).The non-profit accreditations body’s 2021 (ISC)2 Cybersecurity Workforce Study was compiled from interviews with 4,753 cybersecurity professionals and IT workers who dedicate at least 25% of their time to security tasks. It revealed the shortfall of skilled workers in the industry had sunk from 3.12 million last year to 2.72 million. That’s down in part to 700,000 new entrants joining the sector since 2020 and lower demand for workers from APAC, where a slower economic recovery impacts small businesses and those in the IT services sector.

However, despite the global workforce growing to nearly 4.2 million, there are several persistent causes for concern. APAC has the most significant regional workforce gap despite faltering demand, at 1.42 million, while the workforce gap in every other region increased since last year. It’s now around 402,000 in North America and 199,000 in Europe, including 33,000 in the UK.[3]

***Part B***

Downloaded Sonarlint and JShint which are both programs for testing and identifying security flaws in code. They both uncover any flaws the developer may not have noticed.

SonarLint pointed out 7 flaws/problems that may make my program less secure

Text

Description automatically generated

Jshint on the other hand uncovered 41 flaws/problems in my program, however they were mainly coding preferences.

Text

Description automatically generated

***Part C***

**+**: Force exact-match on a single phrase. Deprecated with the launch of Google+.

Examples: +cars

**-:** Put minus (-) in front of any term (including operators) to exclude that term from the results.

Example: Tesla -motors

**~** : Include synonyms. Seems to be unreliable, and synonym inclusion is default now.

Example: ~cars

**.** : a single-character wildcard

Example: m.trix

**\*** : An asterisk (\*) acts as a wild-card and will match on any word.

Example: Tesla “rock \*roll”

**“”** : Put any phrase in quotes to force Google to use exact-match. On single words, prevents synonyms.

Example: “nikola tesla”

**|** : The pipe (|) operator is identical to "OR". Useful if your Caps-lock is broken :)

Example: Tesla | edison

**OR** : Google search defaults to logical AND between terms. Specify "OR" for a logical OR (ALL-CAPS).

Example: Tesla OR edison

**Allintext**: Search the body text for every individual term following "allintext:". Same as multiple intexts:'s.

Example: allintext: orbi eero google wifi

**Allintitle** : Search the page title for every individual term following "allintitle:". Same as multiple intitle:'s.

Example: allintitle: tesla vs edison

**Allinurl** : Search the URL for every individual term following "allinurl:". Same as multiple inurl:'s.

Example: allinurl: amazon field-keywords nikon

**Cache**: Returns the most recent cached version of a web page (providing the page is indexed, of course).

Example: cache:apple.com

**Define**: A dictionary built into Google, basically. This will display the meaning of a word in a card-like result in the SERPs.

Example: define:entrepreneur

**Filetype** : Match only a specific file type. Some examples include PDF, DOC, XLS, PPT, and TXT.

Example: "tesla announcements" filetype:pdf

**Info** : to bring back information about a certain domain.

Example: Info:tesla.com

**Intext** : Search for a word or phrase (in quotes), but only in the body/document text.

Example: intext:"orbi vs eero vs google wifi"

**Intitle** : Search only in the page's title for a word or phrase. Use exact-match (quotes) for phrases.

Example :intitle:"tesla vs edison"

**Inurl** : Look for a word or phrase (in quotes) in the document URL. Can combine with other terms.

Example: tesla announcements inurl:2016

**Link:** Find pages that link to the target domain. This operator was deprecated in early 2017.

Example: link:nytimes.com

**Related :** Return sites that are related to a target domain. Only works for larger domains.

Example: related:nytimes.com

**Site :** Get results from certain sites or domains

Examples : olympics site:nbc.com Olympics site:nbc.com OR site:.gov

**Numrange :** for searching numbers within a desired range.

Example: numrange:1200-1230

**Daterange** : Return results in the specified range. Can be inconsistent. Requires Julian dates.

Example: tesla announcements daterange:2457663-2457754

Search Engines:

1. **Yahoo**

Advantage: Yahoo offers thorough organic results, and it has better shopping search features than other search engines.

Disadvantage: undated search results, along with unclear labelling of ads which can make it difficult to know which results are ads and which are organic results.

1. **Baidu**

Advantages : offers amazing features and high-quality search results.

Disadvantages : government censorship which leads to integrity questions of the search results

1. **Yandex**

Advantages : delivers relevant search results locally, has a unique image search option, and can abe customized for different countries.

Disadvantages : reaching people out of the before mentioned countries and collecting data from users just like other search engines.

1. **DuckDuckGo**

Advantage : doesn’t track or keep user’s data, it delivers fast results, and has a clean user-friendly interface.

Disadvantage : results are not personalized because of the no data usage, and in that sense are quite limited.

1. **Ask.com**

Advantage: takes help from an unnamed third party search engine.

Disadvantage: the answers might not be as current as those on the other search engines which is one of the biggest disadvantages.

1. **Ecosia**

Advantage: helping to plant those trees for real according to their financial statements so you can contribute to the planet with simple info searching.

Disadvantage: it takes you straight to Google Maps which in my opinion is better than trying and failing to compete with Google. it takes you straight to Google Maps which in my opinion is better than trying and failing to compete with Google.

1. **AOL.com**

Advantage: gives out the safest search result

Disadvantage: heir task bar looks tacky

1. **Internet Archive**

Advantage: digitally preserves more than 1.4 million books and historical documents

Disadvantage: suspicious and maybe unsafe.

1. **Twitter**

Advantage: Best search engine for searching for current news

Disadvantage: has a character limit on the posts

1. **Wiki.com**

Advantage: is a free content, multilingual online encyclopaedia written and maintained

Disadvantage: Academics discredit the website for several reasons: articles can be written by anyone, not necessarily a world expert; editing and regulation are imperfect and a reliance on Wikipedia can discourage students from engaging with genuine academic writing.

***Part D***

1. **Spyware** – Malware that spies on user activity, stealing data, monitoring activity, and collecting keystrokes to access passwords.
2. **Viruses** – Capable of copying itself and spreading, these can steal information, steal money from accounts, shut down computers, and other harmful actions.
3. **Ransomware** – Malware that encrypts your files or locks down your system until you pay a ransom to the hacker to unlock it.
4. **Bots** – Software programs designed to perform specific functions.
5. **Adware** – Advertising-supported software that automatically causes pop-up ads. Often, adware is bundled with spyware on free software and free applications.
6. **Worms** – Computer worms are a type of malware that spreads from computer to network without user intervention. The most famous example is the Morris worm which infected more than ten per cent of computers connected to the internet in 1988.
7. **Trojans** – A trojan is a type of malware that is disguised as something benign. A trojan horse will often make its way onto your computer when you download a program or open an email containing a malicious attachment. Trojan horse is often used to steal information such as passwords from your computer.
8. **Ransomware** – Ransomware is a form of malicious software designed to block access to files or directories on an infected computer and demand that the user pay money. It encrypts the user data and prompts the user to pay the ransom to decrypt their data.
9. **Logic Bombs** – A logic bomb is a malicious code that triggers to execute once it detects specific conditions have been met. In other words, the code does not activate until certain criteria are met and then executes in full force. Logic bombs can be used as weapons against computer networks or databases.
10. **Rootkits** – Rootkits are a type of spyware. They stay hidden on your computer, but they are active. Rootkits give criminals the ability to control your computer remotely. Some rootkits might give them the ability to steal your passwords or track which keys you tap on your keyboard, so be careful!

[1] http://goo.gl/c5zikq

[2] <https://online.champlain.edu/blog/top-cybersecurity-skills-in-high-demand>

[3] https://www.infosecurity-magazine.com/news/global-security-skills-shortage/