CYBER SECURITY AND CRYPTOGRAPHY

Name ;chandan kumar sah

Student.no ; 20210577

**Table of Contents**

[Task 1 3](#_Toc161864821)

[1. Distribution Scheme 3](#_Toc161864822)

[2. Obfuscation 4](#_Toc161864823)

[3. Command and Control Communication 4](#_Toc161864824)

[4. Ransomware Encryption 5](#_Toc161864825)

[5. Security Analysis 6](#_Toc161864826)

[6. Payment Instruction 7](#_Toc161864827)

[7. Identification of technical and compliance-related practices 8](#_Toc161864828)

[8. Product cipher implementation 9](#_Toc161864829)

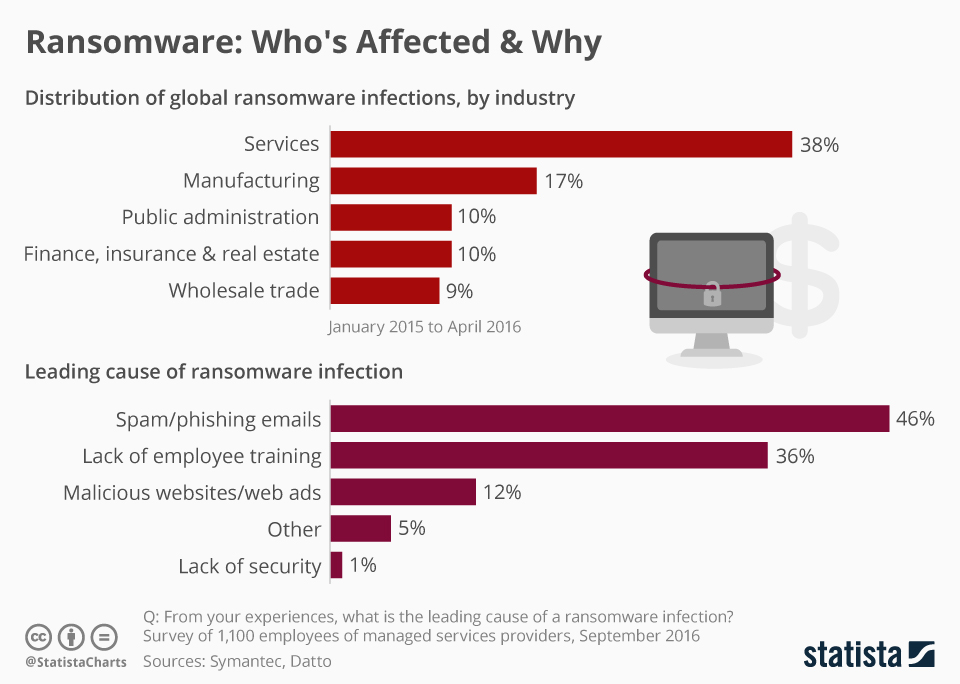
[Task 2 10](#_Toc161864830)

[References 13](#_Toc161864831)

# Task 1

## 1. Distribution Scheme

Utilizing various routes to break into imminent victims' PCs is a proposed ransomware dispersal procedure. The utilization of malicious email attachments or connections is one famous strategy. By making reasonable emails that emulate legitimate organizations or administrations, the assailant might fool beneficiaries into opening attachments or tapping on joins that send off the ransomware payload (Savant *et al.,* 2021). Normally, the download interaction involves mass phishing email dispersion to a huge number of email tends to procured through a few channels, such purchasing email records or data scraping from publically open sources. These emails incorporate spellbinding headlines and content intended to provoke the beneficiary's curiosity or need to keep moving. An email might indicate to give a pivotal record, receipt, or warning of a freight appearance, for example.



**Figure 1: Ransomware distribution to the potential users**

(Source: Kaur *et al.,* 2022)

The ransomware typically utilizes a succession of robotized tasks to spread all through the victim's PC after it has been downloaded. The ransomware look through the victim's records all through the execution cycle and encrypts them with a strong encryption method. To ensure that it keeps on working effectively, the ransomware may likewise attempt to deactivate or get around any safety efforts that are at present set up, such as antivirus programming (Kaur *et al.,* 2022). The ransomware generally advises the victim that their records have been encryptd and gives directions on the most proficient method to pay the payoff to get the decoding key on the screen in the wake of encoding the data. Generally, the payoff note has a cutoff time and undermines irreversible data misfortune in the event that the payoff isn't paid in the dispensed measure of time.

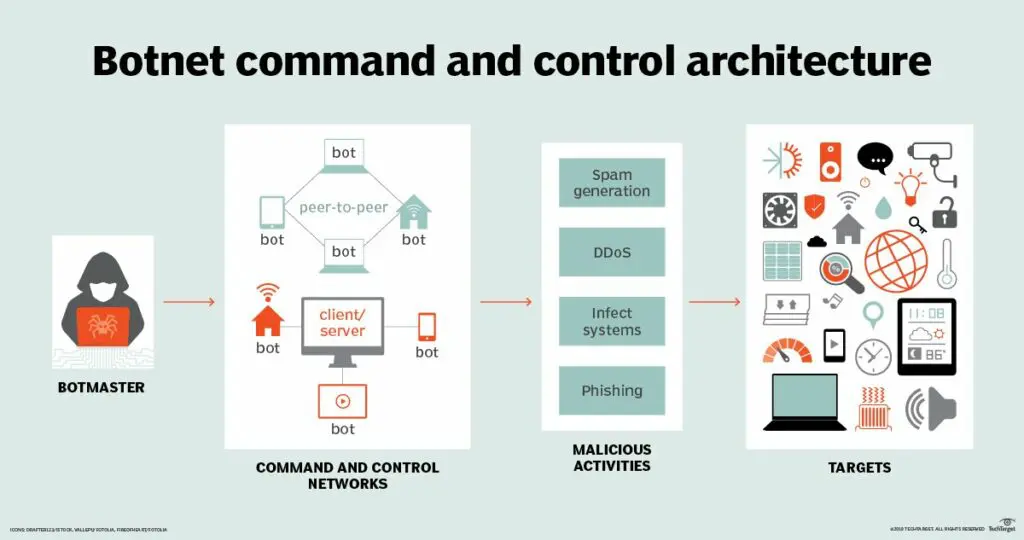
## 2. Obfuscation

There are various strategies that might be utilized to keep away from detection, stop removal, and thwart analysis to disguise ransomware all through both the disease and working stages. Utilizing fileless ransomware, which just runs in memory and leaves no proof on the circle, is one method for getting around the detection of ordinary antivirus programming. Fileless ransomware evades regular record based security components by utilizing respectable framework utilities and cycles, like PowerShell or Windows Management Instrumentation (WMI), to execute malicious code straightforwardly in memory (Dubey *et al.,* 2022). Making the ransomware code hard to decipher and recognize by antivirus programming and security scientists is another strategy. The method involved with changing ransomware code to make it extensively harder to understand and pick apart while keeping up with the functional equivalent is known as code jumbling. A few strategies might be utilized to do this, including renaming factors and works, adding superfluous code, and concealing the malicious payload through encryption and encoding.

Antivirus programming's polymorphic detection measures can likewise be avoided by the ransomware by utilizing polymorphic or transformative strategies to modify its look and mark consistently. Static mark coordinating is extremely difficult to identify with polymorphic ransomware as it makes new variants with each contamination, while transformative ransomware changes its code structure with each redundancy. Besides, Cobalt Strike and other comparative projects have complex avoidance abilities and may impersonate refined enemy ways of behaving to get around security shields (Katsikeas *et al.,* 2021). Moreover, the ransomware code can be clouded and the payload encrypted utilizing cryptos and packers like Themida and Conundrum Defender, which expands the payload's protection from analysis and detection by antivirus programs.

## 3. Command and Control Communication

During ransomware tasks, correspondence between the compromised framework and the Command and Control (C&C) server is fundamental for various reasons, including key creation, stockpiling, and the execution of additional commands. The trading of payment notes, file encryption, and contact between the aggressor and the victim are totally made conceivable by this network. The C&C server is typically the site of key creation, when the assailant makes a particular encryption key pair for each compromised framework (Katsikeas *et al.,* 2021). While the confidential key is securely kept on the server, the public key is shipped off the compromised gadget. With this awry encryption strategy, data encrypted with the public key can't be unencrypted by anyone other than the aggressor who has the confidential key.



**Figure 2: Command and control communication between infected system and server**

(Source: Katsikeas *et al.,* 2021)

The infected device lays out a network with the C&C server to get the public key expected for encoding the items in the victim. Subsequent to accessing the key, the ransomware encrypts the files, keeping the victim from getting to them. For safekeeping, the encryptd data are then sent back to the C&C server or held on the compromised gadget. To send the victim the payoff note and guidelines, the ransomware likewise trades messages with the C&C server. Normally, this payment letter incorporates dates and punishments for rebelliousness alongside subtleties on the most proficient method to pay the payoff, including Bitcoin wallet locations or payment gateways (Vaishnavi *et al.,* 2021). Alongside ensures that the victim's files will be returned after payment, the payoff letter could likewise contain decoding directions. Ransomware utilizes various protocols and strategies, for example, peer-to-peer (P2P) networks, DNS, and HTTP(S), to complete these interchanges. These protocols diminish the likelihood that security arrangements will see the compromised PCs and permit data to be traded among them and the C&C server.

## 4. Ransomware Encryption

A ransomware assault generally focuses on an enormous number of files on the victim's framework to encode significant data and boost impact. Files like papers, photos, motion pictures, databases, and more that are frequently used and have a ton of significant worth for the victim are the objectives of the ransomware. The ransomware may utilize recursive file traversal procedures to search for files on both local and network devices (Easttom, 2022). This involves recursively going through directories, for example, the root directory of an organization share or the client's home directory, starting with a given root directory. By checking each file's expansion against a foreordained rundown of upheld file types, the ransomware may identify files and directories utilizing working framework libraries or APIs.

The malware utilizes strategies to find files and then, at that point, recovers and encrypts them. Adding each file's items to memory, encoding the data with a key and encryption strategy that are provided by the C&C server, and then overwriting the first file with the encrypted variant are the typical strides in this methodology. To hold the victim back from getting to the actual files, the ransomware may possibly eliminate or rename them (Al-Amri *et al.,* 2023). Ransomware might encrypt a more extensive scope of data by explicitly focusing on files with specific expansions, which raises the likelihood that victims would consent to pay the payoff to restore admittance to their significant files. It's important to keep in mind that the exact file augmentations designated could change in view of the sort of ransomware and the aggressor's objectives.

## 5. Security Analysis

***Brute Force***

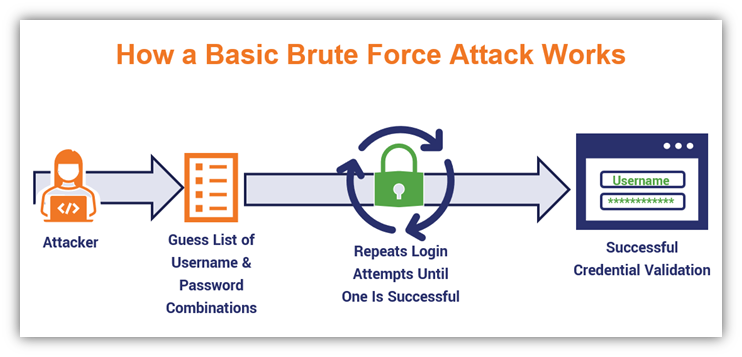
Brute force attacks involve purposefully endeavouring each vital mix until the right one is found. Brute force attacks might be conceivable on account of ransomware assuming that the encryption method and key used are inadequate or ineffectively planned. Notwithstanding, on the grounds that there are so many likely keys, brute force attacks are delivered inconceivable if the ransomware utilizes powerful encryption techniques and safely stores encryption keys (Ahmad *et al.,* 2023). Frequency analysis concludes data about the plaintext by involving factual examples in encrypted data. By the by, accurately carried out current encryption calculations yield ciphertext that appears to be random, delivering frequency analysis futile for decoding.

***Meet-in-the-middle***

Meet-in-the-middle attacks exploit how a few cryptographic calculations are intended to minimize how much computing power is expected to break them. Meet-in-the-middle attacks, in any case, are not important if the ransomware utilizes contemporary encryption strategies like AES with a sufficiently long key length (e.g., 128, 192, or 256 bits) and applies it properly.

***Methods for decryption***

The victim can recuperate their files without having to pay the payoff in the event that they have a new reinforcement of them securely kept offline. Creating normal reinforcements of your data is one of the most incredible ways of protecting yourself from ransomware attacks. Antivirus programming suppliers and security scientists could make decoding tools that could open files encoded by specific ransomware strains (Tsochev *et al.,* 2020). Although not all ransomware forms have freely open decoding techniques, victims can use these tools to open their files without having to pay the payment. It is feasible to distinguish and eliminate ransomware flare-ups before they encode files by serious areas of strength for implementing and antimalware programs.



**Figure 3: Cyber attack analysis for security purposes**

(Source: Taylor *et al.,* 2020)

In order to remain protected from steadily changing ransomware attacks, standard redesigns and it are significant to ongoing monitoring. The implicit framework restore and recuperation tools in victims' operating frameworks permit them to return their PCs to a period before the ransomware infestation. By doing this, the assault's belongings might be decreased and admittance to encrypted data might be restored. Policing ought to be informed of the ransomware attack, and network protection experts can offer additional assets and help for unscrambling and removal activities (Taylor *et al.,* 2020). Despite the fact that ransomware is a significant risk to the two individuals and networks, there are ways of lessening its belongings and get the encrypted information back without having to pay the aggressor. Through the execution of solid safety efforts, reliable reinforcement methods, and the utilization of decoding tools and abilities, individuals may capably balance ransomware and shield their valuable data from any expected intrusion.

## 6. Payment Instruction

Ransomware attackers normally supply victims with payment instructions that include explicit methodology they should take to fulfill the payoff demand and secure the decoding key expected to recover their encrypted data. The motivation behind these instructions is to help the victim in the payment strategy and assurance that the payoff is effectively communicated to the aggressor's picked wallet or record.

The ransom note outlines the amount of cash the attacker is requesting to be sent in kind for the decoding key. This total can contrast fundamentally founded on various factors, including the kind and intensity of the ransomware attack, the aggressor's judgment, and the assessed worth of the victim's data. To empower namelessness, the payment might be mentioned in cryptocurrencies like Bitcoin, Ethereum, or Monero as well as in regular monetary forms like US dollars or euros. The attacker gives the victim a particular cryptocurrency wallet address to which they are told to make the payoff payment in request to get it secretly (Aggarwal *et al.,* 2022). The payoff cash is shipped off this wallet address, which additionally empowers the attacker to monitor incoming payments and affirm fruitful exchanges without disclosing their personality. The payoff letter as a rule contains deadlines for the victim to pay the payoff in request to forestall super durable data misfortune or an increase in the payment total, among other irreversible repercussions. The victim feels under the gun to follow the attacker's demands because of these deadlines. Assuming the deadline is missed, there may be more dangers or an increase in the payment demand.

The victim is encouraged to caution the attacker by means of a predefined correspondence channel, such email or a Tor-based messaging administration, subsequent to transferring the payment cash to the preset wallet address. Assuming that the victim needs affirmation that the payoff has been paid effectively, they can be approached to submit proof of payment, such an exchange ID or screen capture (Althobaiti *et al.,* 2020). The attacker should supply the unscrambling key or tool expected to open the encoded data after the payment has been checked. In certain instances, the payoff letter could give a contact rundown or guidelines for getting in touch with the attacker to demand help or participate in discussions. This could involve utilizing email accounts provided by the attacker or encoded messaging administrations.

## 7. Identification of technical and compliance-related practices

The two technical controls are described as follows

***Endpoint protection solution***

Ransomware attacks might be distinguished and stopped at the endpoint level by serious areas of strength for implementing security arrangements, for example, antivirus programming, hostile to malware tools, and endpoint detection and reaction (EDR) frameworks (Choithani *et al.,* 2022). These arrangements include social monitoring, machine learning calculations, and modern heuristic analysis to recognize uncommon actions that could be an indication of ransomware movement. These arrangements can recognize and stop ransomware episodes before they encrypt files and mischief the organization's frameworks and data by continually monitoring and analyzing endpoint conduct.

***Network Segmentation***

Putting access limitations and organization division into place lessens how much ransomware spreads all through the organization of the organization. networks have some control over ransomware infestations and stop them from spreading all through the organization by segmenting the organization into more modest, disengaged areas and limiting access between them using the least honour principle (Švábenský *et al.,* 2021). To further brace the network's safeguard against ransomware attacks, intrusion detection and prevention systems (IDPS) and next-generation firewalls (NGFW) can be utilized to recognize and obstruct ransomware traffic.

The compliance-related practices are described as follows

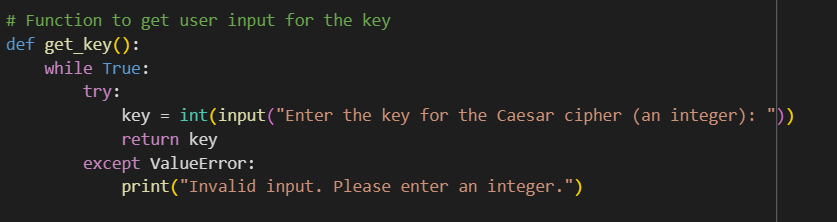
***Security related training***

Customary security training illuminates staff individuals about the risks and repercussions of ransomware attacks. It likewise shows them how to detect and respond to phishing emails, questionable links, and other regular ransomware assault vectors. networks might empower staff individuals to effectively partake in avoiding ransomware attacks and lessening their impacts on the organization by increasing representative information and fostering a culture of network safety mindfulness and sharpness.

***Data recovery policies***

It is guaranteed that fundamental data is routinely upheld and safely kept in offline or offsite places by areas of strength for putting reinforcement and recuperation techniques set up. Networks might minimize disturbance and data misfortune for the situation of a ransomware assault by restoring encoded information from reinforcement duplicates without having to pay the payment (Faragallah *et al.,* 2020). Networks should set up solid data reinforcement and recuperation systems in request to follow data security regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). This will protect classified data and assurance business continuity in case of ransomware attacks.

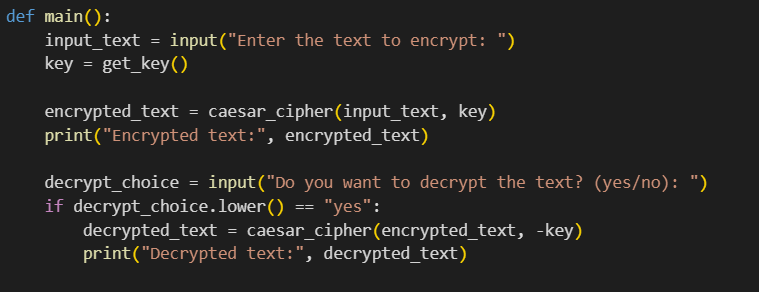
## 8. Product cipher implementation



**Figure 4: Function for encryption**

(Source: Google Colab)

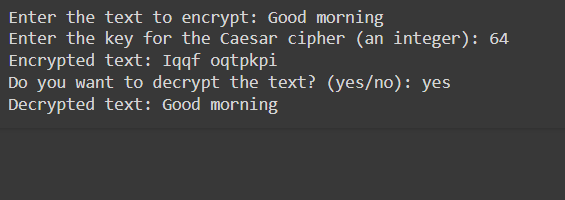
The Caesar figure requires an integer key, which the get\_key capability requests that the client enter. ValueError errors for non-integer inputs are handled, and the client is prompted until a right integer is provided. Finally, it offers back the genuine key so the program might continue to run.



**Figure 5: Function for decryption**

(Source: Google Colab)

The main function requests that the client enter text to encrypt and a Caesar figure key. The text is then encoded using the given key, printed, then, in the event that the client decides, alternatively decoded.



**Figure 6: Encrypted and decrypted text**

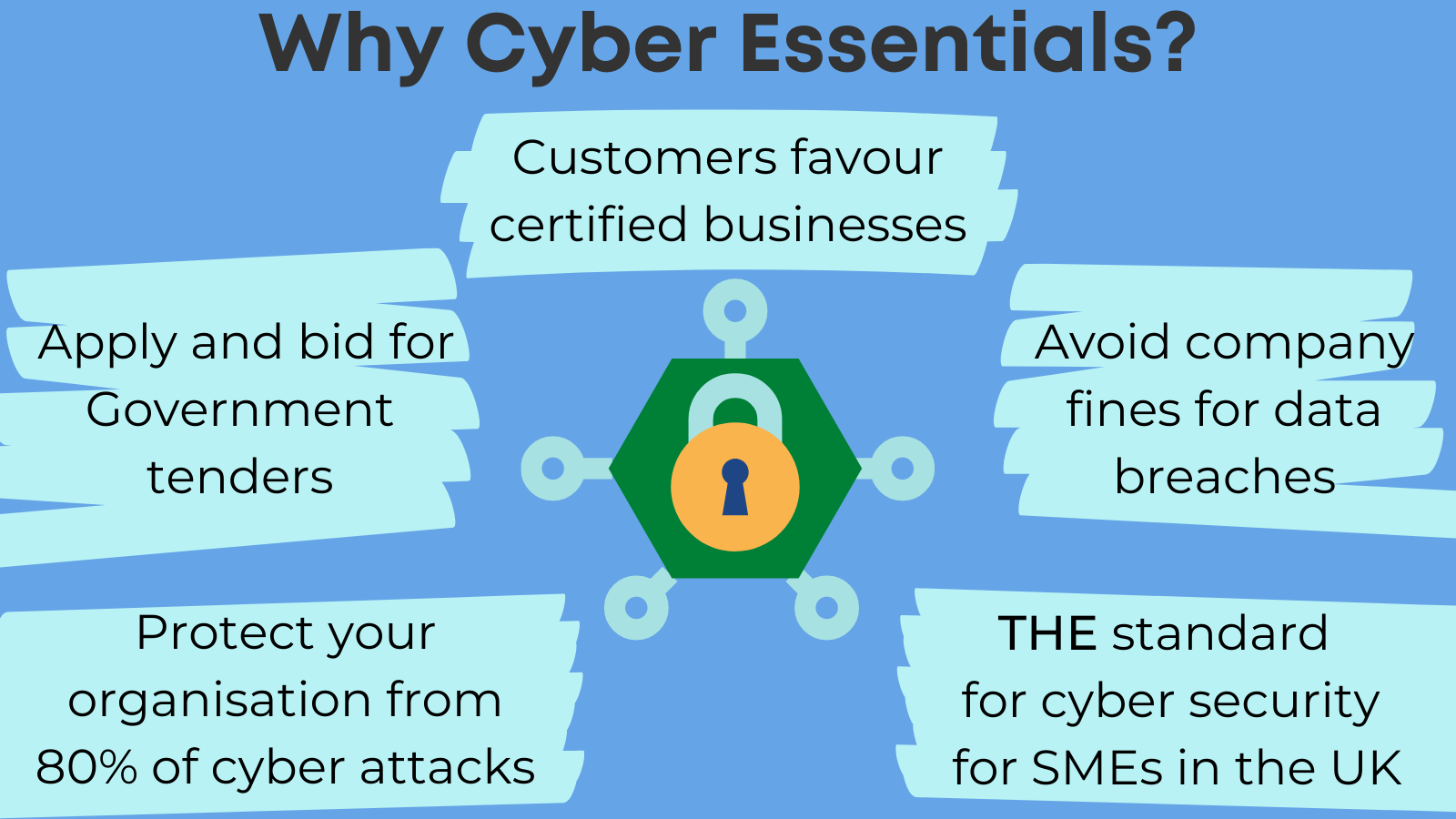
(Source: Google Colab)

A text has been encrypted with a Caesar cipher key and the output hs been came according to the encryption funcion mentioned in the input code. The encrypted text can again be decrypted and option for decryption has shown to decrypt the text. The encrypted text has been decrypted with the hashing function after the positive input ‘yes’ in the output section.

# Task 2

***Cyber Essentials***

A program called Cyber Essentials, upheld by the UK government, expects to help businesses in defending themselves against continuous cyberattacks. Associations might show their devotion to cybersecurity best practices, for example, safe design, line firewalls, access control, fix management, and malware avoidance, by earning the Cyber Essentials affirmation. Associations might decrease their weakness to typical cyberthreats including malware infections, phishing attacks, and unapproved access by putting the Cyber Essentials controls into place and establishing a baseline level of cybersecurity strength (Chivukula *et al.,* 2021). Having the Cyber Essentials confirmation might assist a business with standing out from the opposition by showing accomplices, buyers, and other partners that it views cybersecurity in a serious way and has set areas of strength for up measures to get basic information and frameworks. Associations might attain consistence and stay away from fines connected with data breaches and security slips by obtaining the Cyber Essentials confirmation, which is in line with a few industry standards and regulatory necessities including GDPR and ISO 27001.



**Figure 7: Cyber essentials in the cyber security process**

(Source: Chivukula *et al.,* 2021)

***ISO 27000 Series Standard***

International standards that give proposition and best practices for information security management frameworks (ISMS) make up the ISO 27000 series. ISO 27001 is a conscious method for dealing with risk management to assist relationship with recognizing, survey, and relieving information security risks. A wide cluster of safety dangers and weaknesses may be tended to by relationship through the execution of measures.

Associations should make, execute, maintain, and continuously improve their ISMS in request to consent to ISO 27001. This supports a culture of continuous improvement. Through predictable assessment and modification of safety arrangements, protocols, and controls, foundations might conform to changing landscapes of dangers and develop ideal methodologies (Jaffray *et al.,* 2021). It indicates to clients, partners, and experts that the organization has set up universally acknowledged security protocols to defend private data.

The ISO 27001 access is seen as the international standard for information security management and is for the most part perceived all over the planet. Obtaining an ISO 27001 permit is an indication of an affiliation's obligation to putting into influence internationally recognized security methods and safeguard private data. The affiliation gains trust and certainty from buyers, accessories, and regulators due to this affirmation, which chips away at the affiliation's standing and acceptability in the business place. International business trades are further worked with by ISO 27001 credentials, which extends comfort that the association has set solid areas for up measures to defend fragile data and diminish information security risks.

***General Data Protection Regulation***

Associations are expected by GDPR to set up important hierarchical and mechanical shields to safeguard individual data from unapproved access, revelation, adjustment, and obliteration. Associations might carry major areas of strength for out assurance measures including encryption, access limitations, and data decrease by complying with GDPR guidelines (Anwar *et al.,* 2020). Strengthening data security and protection means bringing down the chance of data breaches and unapproved data processing. GDPR expects associations to give data subjects clear and direct information about how their own data is gathered, handled, and handled. It puts major areas of strength for on responsibility and receptiveness in data processing tasks. Associations might lay out great associations and entrust with customers, labourers, and other partners by granting individuals more control over their own data, gaining express assent for data processing exercises, and posting noticeable security exposures. Increased responsibility and receptiveness support an organization's standing and put it aside as a mindful steward of individual information.

# References

Aggarwal, B.K., Gupta, A., Goyal, D., Gupta, P., Bansal, B. and Barak, D.D., 2022. A review on investigating the role of block-chain in cyber security. *Materials Today: Proceedings*, *56*, pp.3312-3316.

Ahmad, A.Y.A.B., Kumari, S.S., MahabubBasha, S., Guha, S.K., Gehlot, A. and Pant, B., 2023, January. Blockchain Implementation in Financial Sector and Cyber Security System. In *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)* (pp. 586-590). IEEE.

Al-Amri, R.M., Hamood, D.N. and Farhan, A.K., 2023. Theoretical Background of Cryptography. *Mesopotamian Journal of CyberSecurity*, *2023*, pp.7-15.

Althobaiti, O.S. and Dohler, M., 2020. Cybersecurity challenges associated with the internet of things in a post-quantum world. *Ieee Access*, *8*, pp.157356-157381.

Anwar, F., Khan, B.U.I., Olanrewaju, R.F., Pampori, B.R. and Mir, R.N., 2020. A comprehensive insight into game theory in relevance to cyber security. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *8*(1), pp.189-203.

Chivukula, R., Lakshmi, T.J., Kandula, L.R.R. and Alla, K., 2021, November. A study of cyber security issues and challenges. In *2021 IEEE Bombay Section Signature Conference (IBSSC)* (pp. 1-5). IEEE.

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D. and Shah, M., 2022. A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, crypto currency and banking system. *Annals of Data Science*, pp.1-33.

Dubey, H.A.R.S.H.I.T., Kumar, S.U.D.H.A.K.A.R. and Chhabra, A.N.U.R.E.E.T., 2022. Cyber Security Model to Secure Data Transmission using Cloud Cryptography. *Cyber Secur. Insights Mag*, *2*, pp.9-12.

Easttom, C., 2022. Quantum computing and cryptography. In *Modern Cryptography: Applied Mathematics for Encryption and Information Security* (pp. 397-407). Cham: Springer International Publishing.

Faragallah, O.S., Afifi, A., El-Shafai, W., El-Sayed, H.S., Alzain, M.A., Al-Amri, J.F. and Abd El-Samie, F.E., 2020. Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications. *IEEE Access*, *8*, pp.103200-103218.

Jaffray, A., Finn, C. and Nurse, J.R., 2021. Sherlocked: A detective-themed serious game for cyber security education. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15* (pp. 35-45). Springer International Publishing.

Katsikeas, S., Johnson, P., Ekstedt, M. and Lagerström, R., 2021. Research communities in cyber security: A comprehensive literature review. *Computer Science Review*, *42*, p.100431.

Kaur, J. and Ramkumar, K.R., 2022. The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), pp.5766-5781.

Savant, V.B. and Kasar, R.D., 2021. A review on network security and cryptography. *Research Journal of Engineering and Technology*, *12*(4), pp.110-114.

Švábenský, V., Čeleda, P., Vykopal, J. and Brišáková, S., 2021. Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, *102*, p.102154.

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R., 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), pp.147-156.

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S. and Pavlova, G., 2020, October. Cyber security: Threats and challenges. In *2020 International Conference Automatics and Informatics (ICAI)* (pp. 1-6). IEEE.

Vaishnavi, A. and Pillai, S., 2021, July. Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042002). IOP Publishing.

**Video File**



**Code File**

