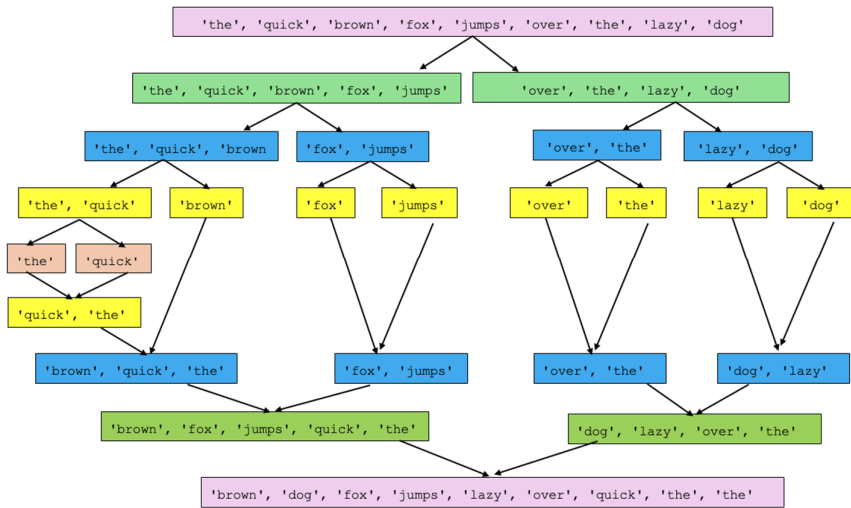


## 2024 YIJC H2 Compting JC2 Prelim Paper 1 – Suggested Solutions

Qu	Suggested Solutions									Mark Scheme
1(a)	Conditions									4m
	Amount < Account balance	N	N	N	N	Y	Y	y	y	
	Amount < Daily withdrawal limit	N	N	Y	Y	N	N	Y	Y	
	Amount < ATM amount	N	Y	N	Y	N	Y	N	Y	
	Actions									
	Cash will be dispense								Y	
	Offer amount available							Y		
	Cancel transaction	Y	Y	Y	Y	Y	Y			
1(b)	Conditions									2m
	Amount < Account balance	N	-	y	y					
	Amount < Daily withdrawal limit	-	N	Y	Y					
	Amount < ATM amount	-	-	N	Y					
	Actions									
	Cash will be dispense				Y					
	Offer amount available			Y						
	Cancel transaction	Y	Y							
1(c)	<pre>Amt = input('Enter the requested amount of money: ')  if Amt &gt; AccBal:     print("Transaction cancelled") else:     if Amt &gt; DailyLimit:         print("Transaction cancelled")     else:         if Amt &lt; AmtATM:             print("ATM will dispense the requested", Amt)         else:             print("ATM can only dispense", AmtATM)</pre>									4m
2(a)	<p>A successful recursive function typically exhibits the following key features:</p> <p><b>1. Base Case</b> - The base case is the condition that stops the recursion by returning a value without making further recursive calls.</p> <p><b>2. Recursive Call</b> - The recursive case is where the function calls itself with a modified argument, moving towards the base case.</p> <p><b>3. Progress Towards the Base Case</b> - Each recursive call should work towards making the problem simpler or smaller, reducing the difference between the current state and the base case.</p>									3m
2(b)	<p>Each recursive call of the function <math>X(n)</math>, the parameter <math>n</math> reduces by 1 and eventually becomes 0 which is the base case and it will return the value 0, hence terminating the recursive calls.</p>									<p>1m – recursive call</p> <p>1m – reduces to 0</p>

2(c)	Each time the function is called, a new frame is added into the call stack. When the number of frames exceeds the maximum allowed by the system (the recursion depth limit), the program can no longer allow further recursive call, hence it raises the error message.	1m – a new frame created for each call  1m – max depth allowed by system
2(d)	Use iteration instead of recursion.	1m
2(e)	<pre>def X(n):     total = 0     for i in range(n+1):         total = total + n     return total</pre>	1m – iterative loop  1m – sum from 0 to n (inclusive)
3(a)	<ul style="list-style-type: none"> <li>Assume the <u>first item is sorted</u>. This forms the <u>sorted part</u> of the list.</li> <li>Take each <u>subsequent item from the unsorted part</u>, and insert it into the <u>correct position within the sorted part</u>."</li> </ul> <p>Continue this process <u>until all elements from the unsorted part</u> are inserted into the sorted part.</p>	1  1  1
3(b)	<ul style="list-style-type: none"> <li>The list is <u>recursively split into two halves</u></li> <li>until each list contains <u>1 item</u>.</li> <li>The <u>two sublists</u> are merged by <u>comparing elements</u> and arranging them in the <u>correct order</u>.</li> <li>This merging process <u>continues recursively</u> until <u>all sublists are combined into a single sorted list</u>.</li> </ul>	1  1  1  1
3(c)	 <p>1 mark: correct split 1 mark: correct merging 1 mark: correct output</p>	
3(d)	<p>Insertion: <math>O(n^2)</math> Merge: <math>O(n \log n)</math></p> <p>Merge Sort is <u>more efficient for large datasets</u> due to its <math>O(n \log n)</math> complexity, whereas Insertion Sort may be <u>preferred for small or nearly sorted datasets</u> due to its simplicity and lower overhead.</p>	1  1

4(a)	<p>A class is a <u>blueprint or template that defines the attributes (properties) and methods (functions)</u> that the objects created from the class will have. It represents the general concept or idea of what an object can be, but it does not represent an actual object itself.</p> <p>An object is <u>an instance of a class</u>. When a class is used to create an object, the object is a <u>specific realization of that class with its own set of values</u> for the attributes defined in the class.</p>	<p>1</p> <p>1</p>
4(b)	<p>Inheritance is a OOP feature that allows a class (known as the <u>child class</u> or subclass) to inherit attributes and methods from another class (known as the <u>parent class</u> or superclass).</p> <p>This enables code reuse and allows the child class <u>to extend or modify the functionality of the parent class by adding additional attributes or methods</u>.</p> <p>Consider a <code>Rectangle</code> class that has attributes like <code>length</code> and <code>width</code> and a method to calculate the area. A <code>Square</code> class can be created as a child class that inherits the properties and methods of the <code>Rectangle</code> class. However, since a square has equal sides, the <code>Square</code> class can override the constructor to take a single attribute, <code>side</code>, and assign it to both <code>length</code> and <code>width</code>.</p>	<p>1</p> <p>1</p> <p>1 (any relevant eg with specifics)</p>
4(c)	<p>Polymorphism is a OOP feature that allows methods in a child class to have the <u>same name as methods in the parent class but perform different actions</u>. This means that the same method name can be used in different classes to perform various tasks depending on the specific object that invokes the method.</p> <p>Polymorphism <u>enables code generalization</u> because a <u>single method can work with different types of objects</u>, allowing for more flexible and reusable code.</p>	<p>1</p> <p>1</p>
4(d)	<p>A Binary Search Tree (BST) is a data structure that stores elements in a hierarchical order. <u>Each node in a BST contains a value, and has at most two child pointers, one to the left child and one to the right child.</u></p> <p>For any node in the BST, the <u>values of all nodes in its left subtree are less than the value of the node</u>,</p> <p>and the <u>values of all nodes in its right subtree are greater than the value of the node</u>.</p>	<p>1</p> <p>1</p> <p>1</p>
4(e)	<ol style="list-style-type: none"> <li><b>Start at the Root:</b> Begin at the root of the BST.</li> <li><b>Traverse the Tree:</b> Compare the value to be inserted (new) with the current node's value: <ol style="list-style-type: none"> <li><b>If new is less than the current node's value</b>, move to the left child.</li> <li><b>If new is greater than the current node's value</b>, move to the right child.</li> </ol> </li> <li><b>Insert the Node:</b> <ol style="list-style-type: none"> <li>If you reach a position where the left or right child is None (i.e., the position is empty), insert the new node at that position.</li> </ol> </li> </ol> <p><b>Recursion/Base Case:</b> The process repeats recursively until the correct position is found and the new node is inserted.</p>	<p>1</p> <p>1</p> <p>1</p>
4(f)	<pre>&lt;A&gt; current = self.root &lt;B&gt; current = current.getLeft() &lt;C&gt; current = current.getRight() &lt;D&gt; return False</pre>	<p>1</p> <p>1</p> <p>1</p> <p>1</p>
4(g)(i)	Root, Left, Right	

	10, 8, 2, 1, 6, 4, 3, 5, 11, 14, 13, 16 Minus 1 mark per error	
<b>4(g)(ii)</b>	Left, Right, Root 1, 3, 5, 4, 6, 2, 8, 13, 16, 14, 11, 10 Minus 1 mark per error	
<b>5(a)</b>	Advantages of hash table over array: 1. Efficient for search – Time complexity for hash table is $O(1)$ and $O(n)$ for unsorted array or $O(\log n)$ for sorted array.  2. Efficient for delete and insert – Deletion and insertion for hash table removes or insert an element based on the index position obtained with the hash value, it is not dependent on the table size; for unsorted array, it requires shifting the existing elements.	2m  2m
<b>5(b)(i)</b>	Separate Chaining – when collision occurs, all the elements with the same hash value will be added to another data structure so that they occupy the same location in the hash table.  Open Addressing (Linear Probing) – when collision occurs, the algorithm will search sequentially from the point of collision for the next available slot to insert the element.	1m  1m
<b>5(b)(ii)</b>	One disadvantage of:  Separate Chaining – increase memory usage due to additional data structure and slow down the search function.  Open Addressing (Linear Probing) – may lead to clustering of the data and degrade the insert, delete and search procedures.	1m  1m
<b>5(c)</b>	State any one advantage and disadvantage:  Dynamic Data Structures: Advantages: <ul style="list-style-type: none"> <li>- Memory flexibility: allocate memory as needed at runtime; no memory wastage.</li> <li>- Scalability: ideal for applications where the amount of data is unpredictable or changes frequently.</li> <li>- No limited by predetermined memory size.</li> </ul> Disadvantages: <ul style="list-style-type: none"> <li>- Memory fragmentation: free memory is split into small non-contiguous blocks and large data need to be fragmented which lead to slower performance.</li> <li>- Additional overhead for pointers and memory management to implement the dynamic structure.</li> <li>- Slower access since it uses pointers to link the elements.</li> </ul>	1m  1m  1m

	<p>Static Data Structures:</p> <p>Advantages:</p> <ul style="list-style-type: none"> <li>- Simpler memory management: memory is allocated at compile time, less chance of runtime errors due to memory allocation.</li> <li>- Faster access: data are stored in contiguous block of memory and can be accessed directly using their memory addresses.</li> </ul> <p>Disadvantages:</p> <ul style="list-style-type: none"> <li>- Inefficient memory use: If allocated memory is larger than needed, the extra memory is wasted.</li> <li>- Limited by predetermined memory size: the data cannot be larger than the allocated size.</li> </ul>	1m
<b>6(a)</b>	<p>State and explain any two advantages:</p> <p>Centralized Resources: A server can centrally store files, applications, and other resources like printers, internet access, making them easily accessible to all clients on the network. This reduces redundancy and ensures that everyone has access to the same, up-to-date information.</p> <p>Collaboration and Communication: Server-based systems often include tools for collaboration, such as email servers, instant messaging, and file sharing services, which can enhance communication and teamwork within the organization.</p> <p>Improved Security: Centralized control allows for better security management. The server can enforce security policies, control access to sensitive data, and ensure that antivirus software and updates are consistently applied across all clients.</p> <p>Backup and Recovery: Data on the server can be regularly backed up, ensuring that important information is not lost. In case of a hardware failure on a client machine, the data can be easily restored from the server.</p>	<p>2m – state the advantages</p> <p>2m - explain</p>
<b>6(b)</b>	<p>State and explain any two of the following ways to prevent unauthorised remote access:</p> <p>1. Strong Authentication Mechanisms: Ensuring that only authorized users can access servers by requiring robust authentication methods, for example, use multi-factor authentication (MFA) that combines something the user knows (e.g., password), something they have (e.g., security token), and something they are (e.g., biometrics).</p> <p>2. Firewalls with Access Controls: A firewall acts as a barrier that controls traffic between your internal network and external threats, filtering out unauthorized access. Configure firewalls to block unauthorized access to servers by allowing only specific IP addresses or ports. Use access control lists (ACLs) to define which users or systems can connect to the servers and monitor traffic for suspicious activities.</p>	<p>2m – state</p> <p>2m - explain</p>

	<p>3. Virtual Private Network (VPN): VPNs create a secure tunnel for data transmission, encrypting traffic between remote users and the LAN. Implementation: Require remote users to connect via a VPN, which authenticates users and encrypts all data being transmitted, ensuring that unauthorized parties cannot intercept or access sensitive information.</p>	
<b>6(c)</b>	<p>State and explain any three of the following authentication methods:</p> <ol style="list-style-type: none"> <li>1. Password-Based Authentication: Users enter a username and password to gain access to the network.</li> <li>2. Two-Factor Authentication (2FA): Users provide two different types of credentials, typically something they know (a password) and something they have (a mobile device for OTP).</li> <li>3. Biometric Authentication: Uses unique biological characteristics such as fingerprints, facial recognition, or iris scans to authenticate users.</li> <li>4. Token-Based Authentication: Users authenticate using a physical token, such as a smart card, or a virtual token generated by an application.</li> <li>5. Multi-Factor Authentication (MFA): Extends 2FA by requiring additional forms of identification, such as biometrics, security tokens, or even a user's location.</li> <li>6. Certificate-Based Authentication: Users or devices are authenticated using digital certificates issued by a trusted Certificate Authority (CA).</li> </ol>	<p>2m – state</p> <p>2m - explain</p>
<b>6(d)</b>	<p>State and explain any three of the following methods to ensure security during transmission:</p> <ol style="list-style-type: none"> <li>1. Encryption: Encryption converts data into a coded format that can only be deciphered by someone who has the correct decryption key. Using protocols like TLS (Transport Layer Security) or SSL (Secure Sockets Layer) ensures that data transmitted over the network is encrypted, making it unreadable to unauthorized parties even if intercepted.</li> <li>2. Virtual Private Networks (VPNs): A VPN creates a secure tunnel through which data is transmitted, encrypting all traffic between the user's device and the VPN server. This ensures that data remains secure, especially when using public or unsecured networks.</li> <li>3. Secure Protocols: Using secure communication protocols, such as HTTPS for web traffic, FTPS for file transfers, and SSH for remote access, helps protect data during transmission by ensuring that the communication channel itself is secure.</li> <li>4. Digital Signatures and Certificates: Digital signatures verify the authenticity and integrity of transmitted data, ensuring that it has not been tampered with during transmission. Digital certificates, issued by trusted Certificate Authorities (CAs), confirm the identity of the parties involved in the communication.</li> </ol>	<p>2m – state</p> <p>2m - explain</p>

7	<p>State and explain any three advantages:</p> <ol style="list-style-type: none"> <li>1. Scalability - Horizontal Scaling: NoSQL databases are designed to scale out by adding more servers to distribute the load, making them more suitable for handling large-scale data and high-traffic applications. This contrasts with relational databases, which typically scale vertically (by adding more power to a single server).</li> <li>2. Flexibility Schema-less Design: NoSQL databases allow for flexible, schema-less data models, meaning data structures can evolve without the need for extensive database migrations. This is particularly useful in environments where the data model changes frequently. Diverse Data Models: NoSQL databases support various data models, such as key-value, document, column-family, and graph, allowing developers to choose the model that best fits their application's needs.</li> <li>3. Handling Unstructured Data: Support for Unstructured Data: NoSQL databases can efficiently store and manage unstructured and semi-structured data, such as JSON documents, which are cumbersome to handle in relational databases.</li> <li>4. High Availability and Fault Tolerance: Many NoSQL databases are built on distributed architecture systems, which provide built-in replication and redundancy. This leads to high availability, fault tolerance, and resilience against data loss in the event of hardware failures.</li> <li>5. Cost-Effectiveness: NoSQL databases often run on clusters of commodity hardware, reducing the cost of scaling compared to the more expensive hardware often required for high-performance relational databases.</li> <li>6. Simplified Automated Data Sharding: NoSQL databases often provide automatic sharding (splitting and distributing data across multiple servers), simplifying the process of distributing data and improving scalability.</li> </ol>	<p>3m – state</p> <p>3m - explain</p>
8(a)	<p>Any 2 (1 mark to ID, 1 mark to explain, max 4 marks)</p> <p><b>Responsible Disclosure</b></p> <ul style="list-style-type: none"> <li>• Alex adhered to the ethical principle of responsible disclosure by <u>informing CyberCorp about the vulnerability</u> in GuardOn promptly.</li> <li>• This shows commitment to protecting users and <u>preventing potential harm by giving the company an opportunity to fix the issue</u> before it could be exploited by malicious actors</li> </ul> <p><b>Professional Integrity</b></p> <ul style="list-style-type: none"> <li>• Alex demonstrated professional integrity by <u>providing detailed information on the nature of the exploit</u> and how it could be addressed.</li> <li>• This reflects <u>honesty and transparency in reporting security issues</u>, ensuring that the <u>company has sufficient information to address the problem effectively</u>, adhering to the professional responsibility to act in the public interest.</li> </ul>	<p>2</p> <p>2</p>

	<p><b>Public Interest:</b></p> <ul style="list-style-type: none"> <li>Alex acted in the public interest by <u>prioritizing the safety and security of the broader community over personal gain.</u></li> <li>By reporting the vulnerability to CyberCorp <u>instead of exploiting it or selling the information</u>, Alex demonstrated a commitment to <u>protecting users</u> and preventing harm to the public.</li> </ul> <p><b>Confidentiality:</b></p> <ul style="list-style-type: none"> <li>Alex maintained confidentiality by <u>not publicly disclosing the vulnerability before CyberCorp had a chance to address it.</u></li> <li>This adherence to confidentiality respects the professional responsibility to <u>avoid unnecessary panic or exploitation of the vulnerability</u> before a solution is available.</li> </ul> <p><b>Professional Competence:</b></p> <ul style="list-style-type: none"> <li>Alex demonstrated professional competence by <u>thoroughly researching and understanding the vulnerability</u> and then <u>providing detailed information to CyberCorp on how it could be fixed.</u></li> <li>This reflects the ethical principle of <u>ensuring accuracy and expertise in work</u>, showing that Alex not only identified the issue but also <u>contributed to its resolution.</u></li> </ul> <p><b>Avoiding Harm:</b></p> <ul style="list-style-type: none"> <li>By reporting the vulnerability to the company <u>instead of exploiting it</u>, Alex took steps to <u>avoid harm to users.</u></li> <li>This is a demonstration of the ethical principle of <u>minimizing harm in professional practice</u>, ensuring that the <u>vulnerability would not be used to compromise user data.</u></li> </ul>	
8(b)	<p>Any 2 (1 mark to ID, 1 mark to explain, max 4 marks)</p> <p><b>1. Failure to Act Promptly (Violation of Ethical Principle: Responsibility, Legal Obligation: Duty of Care)</b></p> <ul style="list-style-type: none"> <li><b>Explanation:</b> <u>CyberCorp's five-week delay in acknowledging the vulnerability report from Alex demonstrates a breach of the ethical principle of responsibility.</u> Computing professionals are <u>ethically obliged to act promptly to address security issues, especially when they could lead to significant harm to users.</u> This delay shows a lack of diligence and a disregard for the potential risks to users.</li> <li><b>Legal Requirement:</b> Under data protection laws such as Singapore's Personal Data Protection Act (PDPA), companies are required to <u>take reasonable steps to safeguard personal data.</u> By not addressing the vulnerability in a timely manner, CyberCorp failed in its legal duty to protect the data of its users, potentially exposing them to unauthorized access and data breaches.</li> </ul> <p><b>2. Lack of Transparency (Accountability, Notification)</b></p> <ul style="list-style-type: none"> <li><b>Explanation:</b> CyberCorp's <u>refusal to provide additional details or confirmation of the steps taken to fix the vulnerability violates the ethical principle of accountability.</u> Computing professionals and organizations must be <u>transparent about how they handle security issues to maintain trust and ensure accountability.</u> CyberCorp's lack of communication undermines this trust and fails to demonstrate accountability.</li> <li><b>Legal Requirement:</b> Legally, <u>organizations are often required to notify affected parties and authorities about security breaches, especially when personal data is compromised.</u> CyberCorp's lack of transparency may also be a violation of legal obligations to inform stakeholders about the measures taken to address the vulnerability and the status of their data security.</li> </ul>	<p>2</p> <p>2</p>



	<p><b>3. Neglecting User Safety (Avoiding Harm, Data Protection)</b></p> <ul style="list-style-type: none"> <li>• <b>Explanation:</b> CyberCorp's handling of the vulnerability neglects the ethical principle of avoiding harm. By <u>not addressing the vulnerability promptly and effectively, they exposed thousands of users to significant risks, including data loss and unauthorized access to personal information.</u> Ethical principles dictate that computing professionals should <u>prioritize user safety and take proactive measures to prevent harm.</u></li> <li>• <b>Legal Requirement:</b> Under data protection laws, organizations have a <u>legal obligation to ensure the security of personal data.</u> CyberCorp's failure to fix the vulnerability in a timely manner led to a data breach, which could be considered a violation of these legal obligations. This negligence could result in penalties or legal action against the company.</li> </ul> <p><b>4. Inadequate Incident Response (Professional Competence, Breach Notification)</b></p> <ul style="list-style-type: none"> <li>• <b>Explanation:</b> CyberCorp demonstrated a lack of professional competence in their incident response. <u>The delayed acknowledgment and insufficient communication about the vulnerability indicate that the company was not adequately prepared to handle security incidents, which is a breach of the ethical principle that professionals must maintain high standards of competence in their work.</u></li> <li>• <b>Legal Requirement:</b> Many jurisdictions require that organizations <u>notify affected individuals and relevant authorities about data breaches within a specified timeframe.</u> CyberCorp's inadequate response and lack of timely communication could be seen as a failure to meet these legal requirements, further compounding the legal consequences of the breach.</li> </ul> <p><b>5. Failure to Protect Confidential Information (Confidentiality, Data Security)</b></p> <ul style="list-style-type: none"> <li>• <b>Explanation:</b> By not addressing the vulnerability promptly, CyberCorp allowed confidential user information to be accessed and sold on the dark web. This violates the ethical principle of <u>confidentiality, which requires professionals to protect sensitive information and prevent unauthorized access.</u></li> <li>• <b>Legal Requirement:</b> Data protection laws mandate that <u>companies implement appropriate security measures to protect confidential information.</u> CyberCorp's failure to do so, leading to a breach of user data, could be considered a violation of legal data security requirements, potentially exposing the company to legal penalties.</li> </ul>	
8(c)	<p><b>Social Impact (Any 2 points, 1 mark each):</b></p> <p><b>1. Loss of Trust in Technology Companies:</b></p> <ul style="list-style-type: none"> <li>• The breach can lead to a <u>significant loss of trust in CyberCorp and similar technology companies.</u> Users may become <u>more hesitant to use such services,</u> fearing that their personal data is not secure. This erosion of trust can have long-term effects on how people interact with technology and rely on digital services.</li> </ul> <p><b>2. Privacy Violations and Psychological Impact:</b></p> <ul style="list-style-type: none"> <li>• Users whose data has been compromised may face <u>severe privacy violations, such as identity theft or unauthorized access to personal information.</u> This can lead to psychological stress, anxiety, and a feeling of vulnerability among affected individuals, especially if sensitive personal information is involved.</li> </ul> <p><b>3. Impact on Vulnerable Groups:</b></p>	2

	<ul style="list-style-type: none"> <li>• <u>Certain groups, such as elderly users or individuals with less technical knowledge, might be more severely affected by the breach.</u> They could struggle with the consequences of identity theft or data misuse, exacerbating social inequalities in access to security resources and support.</li> </ul> <p><b>4. Erosion of Digital Participation:</b></p> <ul style="list-style-type: none"> <li>• The breach could lead to a <u>wider societal reluctance to engage with digital platforms, particularly those involving sensitive data.</u> This might slow down the adoption of digital services, hindering societal progress in areas like online education, e-commerce, and e-government services.</li> </ul> <p><b>5. Stigmatization and Social Discrimination:</b></p> <ul style="list-style-type: none"> <li>• If personal information such as health data or social behaviors are exposed, <u>affected individuals may face stigmatization or discrimination in their communities or workplaces.</u> This can lead to long-term social isolation or reputational damage.</li> </ul> <p><b>Economic Impact (Any 2 points, 1 mark each):</b></p> <p><b>1. Financial Loss for Users:</b></p> <ul style="list-style-type: none"> <li>• Users may <u>suffer direct financial losses due to fraudulent activities, such as unauthorized transactions or theft of assets.</u> They may also incur costs related to securing their data and recovering from identity theft, such as legal fees or credit monitoring services.</li> </ul> <p><b>2. Economic Consequences for CyberCorp:</b></p> <ul style="list-style-type: none"> <li>• CyberCorp <u>may face significant financial repercussions, including legal penalties, compensation claims from affected users, and loss of business.</u> The company could also suffer a decline in stock value, loss of customers, and increased costs for implementing enhanced security measures in the aftermath of the breach.</li> </ul> <p><b>3. Costs to Government and Public Services:</b></p> <ul style="list-style-type: none"> <li>• <u>Governments might have to invest in additional resources to deal with the aftermath of the breach,</u> such as funding for cybersecurity initiatives, legal investigations, or social support programs for victims of the breach. This represents an economic burden on public services.</li> </ul> <p><b>4. Broader Economic Instability:</b></p> <ul style="list-style-type: none"> <li>• <u>If CyberCorp is a major player in its industry, the breach could create instability within the market.</u> Competitors may also suffer from reduced consumer confidence, leading to decreased investment in the tech sector and potential job losses.</li> </ul> <p><b>5. Loss of Productivity:</b></p> <ul style="list-style-type: none"> <li>• <u>Both CyberCorp and affected users may experience a loss of productivity.</u> Users might spend time resolving issues related to the breach, while CyberCorp may need to divert resources from other projects to address the breach, slowing down innovation and business operations.</li> </ul> <p><b>6. Impact on Insurance and Cybersecurity Costs:</b></p>	<p>2</p>
--	---	----------

	<ul style="list-style-type: none"><li>• The <u>breach might lead to increased insurance premiums for companies in similar industries, as insurers adjust to the heightened risk.</u> CyberCorp itself might face higher costs in securing its systems post-breach, which could impact its profitability and pricing strategies.</li></ul>	
--	---	--