SINGAPORE CHINESE GIRLS' SCHOOL
PRELIMINARY EXAMINATION 2025
SECONDARY FOUR
O-LEVEL PROGRAMME

CANDIDATE NAME

CLASS | REGISTER NUMBER

CENTRE NUMBER | INDEX NUMBER

HUMANITIES **2260/01 / 2261/01 / 2262/01**

Paper 1 Social Studies

Monday **18 August 2025** **1 hour 45 minutes**

Additional Materials: 2 Cover Sheets

READ THESE INSTRUCTIONS FIRST

Write your name, class and index number on all the work you hand in.
Write in dark blue or black pen.
Do not use staples, paper clips, highlighters, glue or correction fluid.

Section A
Answer **all** questions.

Section B
Answer **both** questions.

Start each section on a new sheet of writing paper.
Complete the Cover Sheets and attach accordingly.
At the end of the examination, fasten Section A and Section B SEPARATELY.
They will be collected SEPARATELY.

The number of marks is given in brackets [ ] at the end of each question.

This question paper consists of **7** printed pages

SECTION A (Source-Based Case Study)

Answer **all** questions.

Being Part of a Globalised World

Study the Background Information and the sources carefully, and then answer all the questions.

You may use any of the sources to help you answer the questions, in addition to those sources you are told to use. In answering the questions you should use your knowledge of the topic to help you interpret and evaluate the sources.

1 Study Source A.

What is the message of this source? Explain your answer using details from the cartoon. [5]

2 Study Sources B and C.

How similar are these two sources? Explain your answer. [7]

3 Study Sources D and E.

Having read Source D, was Source E surprising? Explain your answer. [7]

4 Study Source F.

How useful is this source in the discussion on cyber threats? Explain your answer. [6]

5 'Individual action is the best way to manage cyber threats.'

Using the sources in this case study, explain how far you would agree with this statement. [10]

How challenging is it to manage cyber threats?

BACKGROUND INFORMATION

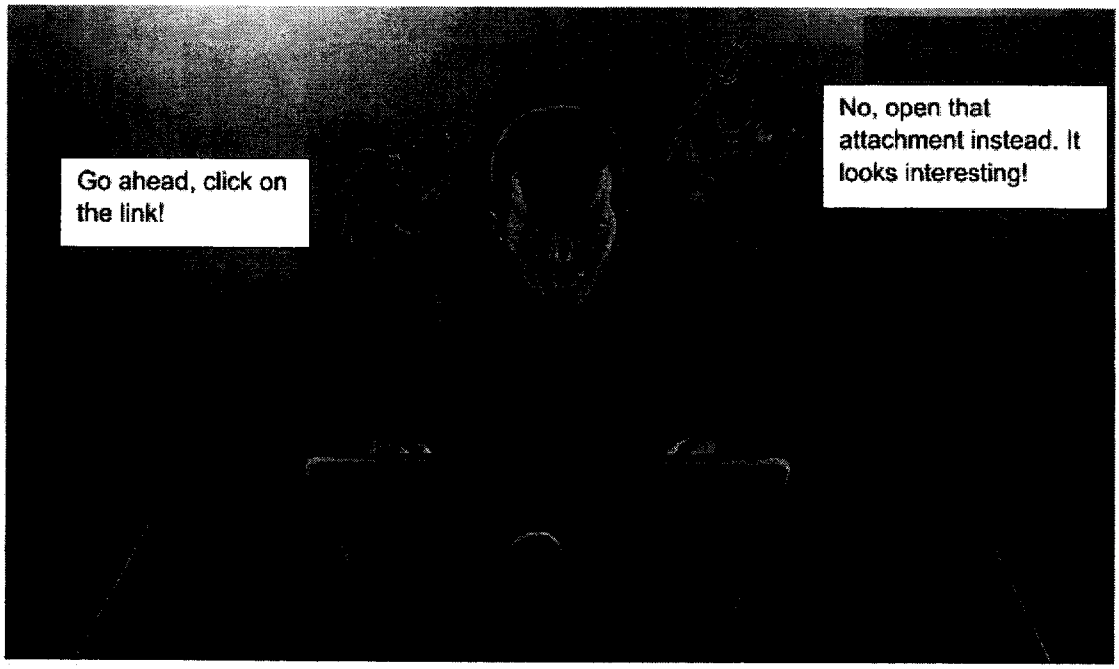
Read this carefully. It may help you to answer some of the questions.

With advancements in digital technology, many of our daily activities are carried out online. Improvements in technology have also made it easier for people to access and store information online. This digital connectedness means that cybersecurity becomes an important concern for countries, organisations and individuals.

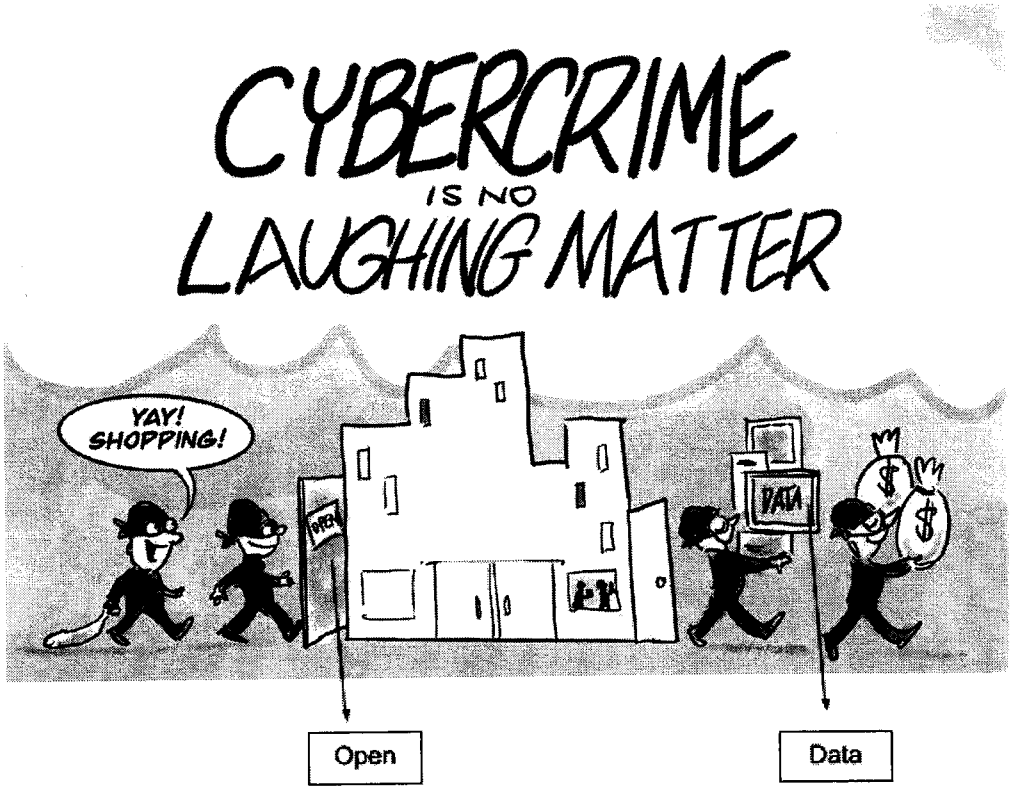
Threats to cybersecurity, also known as cyber threats, pose a significant and growing risk to the global economy, with potential damages estimated in the trillions of dollars. These threats can disrupt businesses, compromise sensitive information, and even impact national security.

Study the following sources to find out how cyber threats can be managed.

Source A: *A cartoon drawn in May 2018 about data security.*



Source B: *A cartoon by an American cartoonist, May 2021.*



Source C: *From an article on the website of a cybersecurity company published in March 2025.*

With the rapid advancement in technology, the cyber threat landscape has changed. It is more sophisticated and widespread than ever. In fact, global cybercrime costs are expected to reach $10.5 trillion annually by 2025. Cybersecurity isn't just about big enterprises and government agencies; it is something businesses of all scales have to be tuned into, including the individual who uses these digital services.

Human error remains one of the major contributing factors to cybersecurity breaches and tends to be the weakest link in organisational security defences. Poor passwords and falling for phishing remain some of the most common mistakes.

Source D: *From a reply by Minister of Education Mr Chan Chun Sing in Parliament, on 10 September 2024. He was responding to a question from a Member of Parliament about the impact of a Mobile Guardian cyberattack that affected 13,000 users from 26 secondary schools. This cyberattack took place in August 2024. Mobile Guardian is a Device Management Application that helps parents manage their children's learning device.*

It was most heartening to see many of our students step forward and proactively share their personal notes with classmates and organise study sessions to do revision for their tests and exams together.

Despite this incident, we must embrace technology in teaching and learning so that students will be digitally savvy and able to navigate digital environments. All of us can learn from this incident. It is an important reminder for all of us to practise good digital hygiene, including the regular backing up of information.

Source E: *From an article written by a National University of Singapore Professor, published on 19 September 2024. He was commenting on the same Mobile Guardian cyberattack that took place in August 2024.*

This incident with the device management app has sparked concerns about our growing dependence on technology in education. Some online reactions included calling for a return to more traditional methods as the breach disrupted students' ability to continue their studies as they normally would.

However, the real issue is not a dependence on technology. Instead, it is about our failure to equip students with skills to handle technological disruptions that are inevitable in today's world.

If students do not feel empowered by the digital tools given to them, then it is our responsibility as educators and as parents to equip them with the necessary technical and soft skills, so that they are able to gain a sense of autonomy to direct their use of digital tools.

Source F: *From an interview with Archie Norman published in a British newspaper, July 2025. Norman is the chairman of British retailer Marks & Spencer and in April 2025, there was a cyberattack against Marks & Spencer which forced them to suspend online shopping for nearly seven weeks.*

British businesses should be legally required to report cyberattacks to the authorities. We have reason to believe there've been two major cyberattacks on large British companies in the last four months which have gone unreported and this meant there was "a big deficit" in knowledge in the cybersecurity space. I don't think it would be regulatory overkill to say

if you have a cyber attack and then for companies of a certain size, you are required within a time limit to report.

SECTION B (Structured-Response Questions)

Answer **both** questions.

Exploring Citizenship and Governance

Study the extracts carefully, and then answer the questions.

Extract 1

Government agencies regularly engage citizens to receive feedback on national policies and issues of concern to them.

Extract 2

Singapore is one of the few countries in the world to maintain diplomatic relations with 190 UN member states, with the exception of Central African Republic and South Sudan.

Extract 3

Singapore must always maintain a credible and deterrent military defence as the fundamental underpinning for an effective foreign policy.

6 Extract 1 discusses how the Singapore government engage citizens to receive feedback on national policies and issues of concern.

In your opinion, what are the ways in which the Singapore government can engage with her citizens? Explain your answer with reference to **two** ways. [7]

7 Extracts 2 and 3 highlight the role the Singapore government plays in promoting and protecting Singapore's national interests.

Do you think that diplomacy or deterrence is more effective in promoting and protecting Singapore's national interests? Explain your answer [8]

End of paper

Source D	*https://www.channelnewsasia.com/singapore/mobile-guardian-cybersecurity-breach-attack-legal-action-contractors-chan-chun-sing-45977*
Source E	*https://www.channelnewsasia.com/commentary/singapore-education-digital-learning-cybersecurity-mobile-guardian-technology-4612796*
Source F	*https://www.reuters.com/business/retail-consumer/ms-cyberattack-was-carried-out-by-dragonforce-chairman-says-2025-07-08/*
Extract 1	*https://www.mfa.gov.sg/Overseas-Mission/Bangkok/About-Singapore/Foreign-Policy*

Answer scheme

Section A

1 Study Source A.
What is the message of this source? Explain your answer using details from the cartoon. [5]

L1: 1m	Describes the source / No interpretation
L2: 2-3m	**Sub-message** - Award 3m for well explained answer Sub message is about - Temptations are everywhere Eg. The message of the source is about the temptations lurking everywhere on the internet. This is evident as the source shows 2 'demons' urging a human to either open an attachment or click on a link. This indicates that humans are not strong enough to withstand the temptations lurking on the internet.
L3: 4-5m	**Valid Message is about the follow-up action that should be taken** - Award 5m for well explained answer Valid message is about - The need to increase people's awareness as they are the weakest link Eg. The message of the source is about **the need to increase people's awareness as they are the weakest link.** This is evident as the source shows 2 'demons' urging a human to either open an attachment or click on a link. This indicates that humans are not strong enough to withstand the temptations lurking on the internet. They are the ones that invite cyber attacks and hence there is a need to create more awareness and vigilance.

2 Study Sources B and C.

How similar are these two sources? Explain your answer. [7]

NOTE: Award L1 for answers that do not address the question

L1: 1m	**Details about source**
L2: 2m	**False matching**
L3: 3m	**Similarity OR/AND Difference, unsupported**
L4: 4-6m	**Similarity OR/AND Difference, supported** - Award 4m for similarity OR difference - Award 5m for similarity AND difference - Award 6m for similarity AND difference, well explained Similarity Eg. Both sources are similar in stating that the **consequences of cyber attacks can be severe.** This is evident in Source B where it shows cyber criminals taking away stash of cash and data from an unguarded company. Hence, companies not only suffer financially, they will also lose their data which will lead to more repercussions. This is also reflected in Source C where the source states 'global cybercrime costs are expected to reach $10.5 trillion annually by 2025.' Thus, the world would incurred high financial cost. Difference Eg. Both sources are different in stating **who can help to prevent cyber attacks.** Source B states that companies are responsible for preventing cyber attacks as they fail to safeguard their assets and this is evident as the source shows cyber criminals entering the company that has their doors open. Thus companies are inviting criminals to attack them. However, Source C states people are responsible as it states 'Human error remains one of the major contributing factors to cybersecurity breaches and tends to be the weakest link in organizational security defenses.' Hence, there is a need for people to step up their protection against cyber crimes.
L5: 7m	**L4 + similarity in intention of sources** Eg. Both sources are **similar in the need for people/companies to step up their cyber security measures to prevent further losses.** This is evident in Source B where it shows cyber criminals taking away stash of cash and data from an unguarded company. Hence, companies not only suffer financially, they will also lose their data which will lead to more repercussions. This is also reflected in Source C where the source states 'global cybercrime costs are expected to reach $10.5 trillion annually by 2025.' Thus, the world would incurred high financial cost. Thus, to prevent all this unnecessary cost, individuals/companies need to step up their cyber security measures.

3 Study Sources D and E.

Having read Source D, was Source E surprising? Explain your answer. [7]

NOTE: Award L1 for answers that do not address the question

L1: 1m	**Surprising / Not Surprising without stating the criteria**
L2: 2m	**False matching / Assertion of reliability of Source E** Eg. Source E is reliable because it came from a professor who is supposed to be an expert in his field, thus what he says can be believe.
L3: 3m	**Surprising OR Not Surprising, unsupported**
L4: 4-5m	**Surprising OR/AND Not Surprising, supported** - award 4m for Surprising OR Not Surprising - award 5m for Surprising AND Not Surprising Not Surprising Eg. Having read Source D, Source E was not surprising about the **need for the use of technology in education.** This is evident in Source D as the Prime Minister states 'we must embrace technology in teaching and learning so that students will be digitally savvy and able to navigate digital environments.' Thus, the use of technology must continue to prepare students for the future. Similarly, Source E also states 'then it is our responsibility as educators and as parents to equip them with the necessary technical and soft skills, so that they are able to gain a sense of autonomy to direct their use of digital tools.' Thus, the use of technology in education will remain and students must be equipped with these skills to progress. OR Eg. Having read Source D, Source E was not surprising about the **need to equip individuals with the digital skills to help them survive.** This is evident in Source D as the Prime Minister states 'we must embrace technology in teaching and learning so that students will be digitally savvy and able to navigate digital environments.' Thus, the use of technology must continue to prepare students for the future. Similarly, Source E also states 'it is about our failure to equip students with skills to handle technological disruptions that are inevitable in today's world.' Thus, the Mobile Guardian cyber attack has shown the need to equipe students with digital skills so that they would be ready for future disruptions. Surprising Eg. Having read Source D, Source E is surprising about the **reaction of the students during the cyber attack**. Source E suggests students were affected negatively as they were at a loss and this is evident as the source states 'the breach disrupted students' ability to continue their studies as they normally would.' On the other hand, Source D shows that students were able to overcome the cyber attacks and this is evident as the source states 'many of our students step forward and proactively share their personal notes with classmates and organise study sessions to do revision for their tests and

	exams together.' Students were able to overcome the inconveniences from the cyber attack and came up with solutions to help each other.
L5: 6-7m	**L4 + Assessing reliability of Source E by cross referencing to other sources** - award 7m for well explained answer Eg. Having read Source D, Source E was not surprising about the **need equip individuals with the digital skills to help them survive.** This is evident in Source E as it states 'it is about our failure to equip students with skills to handle technological disruptions that are inevitable in today's world.' Thus, the Mobile Guardian cyber attack has shown the need to equipe students with digital skills so that they would be ready for future disruptions. Source C also agrees with the need to equip individuals with digital skills to help them survive as the source states 'Human error remains one of the major contributing factors to cybersecurity breaches.' Hence, it is important to ensure individuals have the necessary digital skills to prevent cyber attacks which would help them survive.

4 Study Source F.

How useful is this source in the discussion on cyber threats? Explain your answer. [6]

NOTE: Award L1 for answers that do not address the question

L1: 1m	**Making a stand without any reasoning**
L2: 2-3m	**Useful OR Not Useful based on contents** - Award 3m for answers that show both sides Useful Eg. The source is useful in in showing **companies are responsible for cyber threats.** This is evident as the source states 'We have reason to believe there've been two major cyberattacks on large British companies in the last four months which have gone unreported and this meant there was "a big deficit" in knowledge in the cybersecurity space.' In other words, the failure to report on these cyber attacks has led to gaps in the know-how to combat against cyber threats and these threats have made companies vulnerable to more cyber threats. OR Not Useful (Typicality) Eg. The source is not useful as this is just an instance of cyber attack on a retail company in Britain and it is not representative of what is happening nation-wide or across different sectors. Not Useful (information omitted must be important) Eg. The source is not useful as it does not state the consequences of companies that failed to report cyber attacks to the relevant authorities.
L3: 4-5m	**Useful / Not useful based on cross-reference** - Award 5m for well explained answer Eg. The source is useful in in showing **companies are responsible for cyber threats.** This is evident as the source states 'We have reason to believe there've been two major cyberattacks on large British companies in the last four months which have gone unreported and this meant there was "a big deficit" in knowledge in the cybersecurity space.' In other words, the failure to report on these cyber attacks has led to gaps in the know-how to combat against cyber threats and these threats have made companies vulnerable to more cyber threats. Similarly, Source B states that companies are responsible for cyber attacks as they fail to safeguard their assets and this is evident as the source shows cyber criminals entering the company that has their doors open. Thus companies are inviting criminals to attack them. Since Source B corroborates with Source F, Source F is thus reliable and useful.
L4: 6m	**Useful based on context: author's company was a victim of cyber attack**

	Eg. The source is useful in in showing **companies are responsible for cyber threats.** The author of this source is Archie Norman, the chairman of British retailer Marks & Spencer and in April 2025, there was a cyberattack which forced them to suspend online shopping for nearly seven weeks. As his company was a victim of cyber attack, he would be aware of the implications of the attack and would want more measures to safeguard his company from further attacks. For this to happen, there must be constant updates about the methods used by cyber criminals and hence there is a need for companies to come together and share information. However, this is not happening and this is evident as he states 'We have reason to believe there've been two major cyberattacks on large British companies in the last four months which have gone unreported and this meant there was "a big deficit" in knowledge in the cybersecurity space.' Therefore, progress is lacking. What he says about cyber attacks is all the more useful as he is revealing the gaps that is preventing further cyber attacks.

5 'Individual action is the best way to manage cyber threats.'

Using the sources in this case study, explain how far you would agree with this statement. [10]

NOTE: Best Way because

- Success / positive outcome / significant role of the agent (and vice versa: Limitations or lack of positive outcome)

L1: 1m	**Writes about statement, no valid source use**
L2: 2-4m	**Yes OR No, supported by valid source use** - 1Y/N: 2m - 2Y/N: 3m - 3Y/N beyond: 4m
L3: 5-8m	**Yes AND No, supported by valid source use** - 1:1 5m - 2:1 6m - 2:2 and beyond:7-8m <u>Agree</u> **Source A** agrees and this is evident as the source shows the temptations lurking everywhere on the internet. This is evident as the source shows 2 'demons' urging a human to either open an attachment or click on a link. This indicates that humans are not strong enough to withstand the temptations lurking on the internet. Hence, the best way to manage cyber threats will be to increase individual's awareness on the dos and don'ts of cyber usage and with the knowledge, they will then be able to protect themselves. **Source C** agrees and this is evident as the source states 'Human error remains one of the major contributing factors to cybersecurity breaches and tends to be the weakest link in organizational security defenses.' Hence, there is a need for individuals to step up their protection against cyber crimes and with the knowledge, they will then be able to protect themselves. **Source D** agrees and this is evident as the source states 'students were able to overcome the cyber attacks and this is evident as the source states 'many of our students step forward and proactively share their personal notes with classmates and organise study sessions to do revision for their tests and exams together.' Students were able to overcome the inconveniences from the cyber attack and came up with solutions to help each other. <u>Disagree (no credit if agent is not identified)</u> **Source B** disagree and instead the best way to manage cyber threats is by **companies.** Source B states that companies are responsible for preventing cyber attacks as they fail to safeguard their assets and this is evident as the source shows cyber criminals entering the company that has their doors open. Thus companies are inviting criminals to attack them. Therefore the best way to manage cyber threats is by companies as they need to step up their cyber <u>security measures and this will then enable them to protect themselves.</u>

Source C disagree and instead it should be the **responsibility of the government**. The source states that 'Cybersecurity isn't just about big enterprises and government agencies.' Government agencies have a role to play as they set the laws and perimeters for others to follow. With the framework, companies and individuals will then comply.

Source E disagree and instead it should be the **responsibility of the school / family**. The source states that 'it is our responsibility as educators and as parents to equip them with the necessary technical and soft skills, so that they are able to gain a sense of autonomy to direct their use of digital tools.' As the students were the victims of cyber attacks, it is important to help them overcome the problems that arise from the attacks and hence, schools / family should play a greater role to help them since students spend most of the time there.

Source F disagree and instead it should be the **responsibility of business**. The source states that 'We have reason to believe there've been two major cyberattacks on large British companies in the last four months which have gone unreported and this meant there was "a big deficit" in knowledge in the cybersecurity space.' In other words, the failure to report on these cyber attacks has led to gaps in the know-how to combat against cyber threats and these threats have made companies vulnerable to more cyber threats, hence, companies need to be more pro-active.

Intended imbalance to cap at L3/6* (e.g. 3 : 1 / 4 : 1)
This shouldn't be a result of attempted sources but failed attempts. It should be a clear intention of imbalance sources

** To score additional 2 marks, candidates can take any one of these 3 routes:

- *Through analysing at least one source in relation to its reliability, utility or sufficiency*

Reliability:
Eg. Source C is reliable as the source came from a cybersecurity company. Since this company specialises in cyber security, it would be aware of cyber threats going on around the world. The company would also be in a better position to judge who should play a leading role in combating cyber threats as it has vast experience. Therefore, this source is more reliable as the author would have professional knowledge.

Utility
Eg. Source F is useful as the author of this source is Archie Norman, the chairman of British retailer Marks & Spencer and in April 2025, there was a cyberattack which forced them to suspend online shopping for nearly seven weeks. As his company was a victim of cyber attack, he would be aware of the implications of the attack and would want more measures to safeguard his company from further attacks. For this to happen, there must be constant updates about the methods used by cyber criminals and hence there is a need for companies to come together and share information. However, this is not happening and this is evident as he states 'We have reason to believe there've

	been two major cyberattacks on large British companies in the last four months which have gone unreported and this meant there was "a big deficit" in knowledge in the cybersecurity space.' Therefore, progress is lacking. What he says about cyber attacks is all the more useful as he is revealing the gaps that is preventing further cyber attacks. • *By sharing example (s) from their contextual knowledge* **Contextual Knowledge:** Eg. Cyber security is best dealt with through individuals and government working together. For example, in Singapore, the government has the ScamShield, which is a joint effort by the Ministry of Home Affairs, the Singapore Police Force and other government agencies where they provide monthly updates on the latest scam statistics in Singapore. They also teach Singaporeans how to possibly spot a scam and to report potential scams as well. Thus the role of the government is important, as reflected in Source C. Singaporeans are kept updated about cyber crime and hence, it is then up to them to take the necessary action to prevent scams form happening to them as individuals are vulnerable, which is reflected in Source C. Therefore, both individuals and the government have an important role to play in managing cyber threats. • *By giving a balanced conclusion / resolution* **Balanced Conclusion:** It should focus on how 1 perspective influences another or it can be about the idea of trade offs not be able to be reconciled Eg. Cyber threats can be managed by individuals as they are vulnerable due to their ignorance or the unwillingness to take the necessary precautions. This is reflected in Source A, where the carton depicts an individual undecided to either open an attachment or click on a link. This indicates that humans are not strong enough to withstand the temptations lurking on the internet. However, what individuals can do may be limited as cyber criminals are always one step ahead of enforcement agencies. Therefore individuals or even businesses may have to give up certain aspects such as their privacy online so as to enable enforcement agencies to monitor or even track online behaviour of suspicious individuals. This can be seen in Source F where the unwillingness of businesses to share certain aspects of their online behaviour has affected cyber security. Therefore, it is important to ensure all parties stay responsible for their online behaviour.

Section B (Structured-Response Question)

6	Extract 1 discusses how the Singapore government engage citizens to receive feedback on national policies and issues of concern. In your opinion, what are ways in which the Singapore government can engage with her citizens? Explain your answer with reference to **two** ways.	**[7]**
L1	**Describes the topic i.e. government agencies** *e.g. the government is busy formulating laws and policies to build a more efficient and cohesive Singapore.*	**[1]**
L2	**Identifies / describes way (s)** *Award 2m for identifying one way and 3m for two ways. Award 3m for describing one way and 4m for describing two ways.* *e.g. Governments can enhance citizen engagement through various strategies, including utilizing diverse communication channels, actively seeking citizen feedback, and fostering a sense of partnership in decision-making.* 1. Diversifying Communication Channels: **Traditional methods:** Public consultations, town hall meetings, and surveys can be effective when combined with digital tools. **Digital platforms:** Social media, online forums, dedicated government websites, and mobile apps can provide convenient and accessible means for citizens to interact with their government. **Omnichannel approach:** Offering a range of communication channels (phone, email, chat) ensures citizens can engage through their preferred method. 2. Active Feedback and Dialogue: **Encourage feedback:** Governments should actively solicit feedback on policies, services, and decision-making processes. **Two-way communication:** Going beyond one-way communication to foster a dialogue with citizens is crucial. **Address concerns:** Actively listening to and addressing citizen concerns demonstrates that their voices are heard and valued. 3. Empowering Citizens: **Participatory budgeting:** Allowing citizens to decide how a portion of the public budget is spent can increase ownership and engagement. **Community-led initiatives:** Supporting and empowering citizens to lead local projects can strengthen community bonds. **Recognizing citizen contributions:** Acknowledging and appreciating citizen participation can motivate further engagement.	**[2-4]**

	4. Making Engagement Accessible and Convenient: **Clear information:** Providing clear and concise information about government processes and decisions is essential. **User-friendly platforms:** Ensuring that digital platforms are easy to navigate and use can encourage participation. **Location and timing:** Making engagement opportunities accessible in terms of location and timing can increase participation rates.	
L3	**L2 + Explains way (s)** *Award 5-6m for explaining one way.* *Award 6-7m for explaining two ways.* **Digital Government Platforms and E-Services** **One.SG** is a digital platform in Singapore designed to serve as a unified access point for government services and citizen engagement. It integrates features from key apps like LifeSG, Singpass, and OneService to provide seamless, citizen-centric digital experiences. One.SG aims to simplify interactions with the government by personalizing services around major life moments—such as childbirth, housing, and retirement—while also offering tools for reporting municipal issues and accessing public service information. The platform effectively engages Singaporeans through a combination of user-friendly digital services, community co-creation initiatives, and targeted communication campaigns. Programs like Smart Nation Ambassadors and Tech Kaki allow citizens to test and shape digital tools, while the OneService portal empowers residents to report and resolve issues collaboratively with government agencies. Despite these successes, challenges remain in ensuring digital inclusivity for seniors and non-tech-savvy individuals. Overall, One.SG's engagement strategy reflects Singapore's broader Smart Nation vision—leveraging technology not just for efficiency, but for inclusive and participatory governance. It's important because it highlights the organisation's mission to raise public awareness about poverty and inequality in Singapore and beyond, and to take concrete actions to address these issues. ONE (SINGAPORE) also facilitates various programs and initiatives aimed at helping low-income individuals and families, promoting self-reliance, and supporting the Sustainable Development Goals (SDGs). **Analysis:** Digital platforms such as One.sg enhance accessibility and efficiency in government-citizen interactions. By reducing the need for physical presence and paperwork, they lower the barriers for engagement, especially among tech-savvy populations. In Singapore's case, it also promotes trust in the government's digital infrastructure, as high levels of cybersecurity and integration between agencies ensure convenience without compromising data security. Such endeavours of collaboration will help to build Trust and Transparency. **With these opportunities to reach out, citizens will be able to understand how they can help with decision making and contribute with formulating solutions. This will motivate them to even advocate for others to work towards a better government. By implementing these strategies, governments can create a**	**[5-7]**

more participatory and responsive environment, leading to a stronger democracy and improved public services.

OR

Civic Education and National Campaigns

Singapore integrates civic education into its national curriculum through subjects like **National Education (NE)** in schools and **Social Studies**, which teach students about governance, active citizenship, and national values. Additionally, campaigns like **"Forward Singapore"**, launched in 2022, are public engagement initiatives designed to refresh the social compact and involve citizens in conversations about future challenges and opportunities.

Analysis:
Civic education helps cultivate long-term, informed engagement by instilling a sense of responsibility and awareness in young citizens. Campaigns like "Forward Singapore" extend this engagement to adults, encouraging national dialogue. This method ensures that participation is not just reactive but rooted in shared values and sustained across generations. In Singapore's context, where social harmony and cohesion are critical, these efforts play a key role in nation-building and aligning policy directions with societal values.

OR

Youth Involvement and Leadership Platforms

The **National Youth Council (NYC)** empowers young Singaporeans through leadership programs, policy consultations, and youth dialogues. Initiatives like the **Youth Action Challenge (YAC)** invite youth teams to co-develop policy ideas with government agencies. In recent rounds, participants tackled topics like mental health, sustainability, and digital inclusion, with selected ideas receiving funding and implementation support.

Analysis:
Youth engagement is essential for fostering future-ready governance. By involving young people early, governments tap into fresh perspectives and build trust with the next generation of leaders. Singapore's approach through the NYC demonstrates a commitment to co-creation — where youth are not just consulted but actively participate in shaping solutions. This builds empowerment and encourages sustained civic participation beyond voting or feedback.

OR

Community Development and Grassroots Engagement

Another way in which Singapore government can engage is by promoting active citizen participation through the **People's Association (PA)** and its network of **Community Clubs (CCs)**. These grassroots organisations organise activities such as town hall dialogues, cultural events, volunteering initiatives, and feedback sessions. For instance, the **Our Singapore Conversation (OSC)** in 2012–2013 involved over 47,000 Singaporeans in discussions about the country's future, facilitated by PA and various community partners. It encouraged citizens from diverse backgrounds to share their views on education, healthcare, housing, and social mobility. Grassroots engagement enables the government to connect with citizens at the community level, ensuring that feedback is more localized and

	personal. This builds social cohesion and allows policies to be better tailored to residents' needs. In Singapore's case, the PA's strong infrastructure allows for sustained two-way communication, helping to foster trust and inclusivity in governance, especially among groups who may feel disconnected from national policymaking. **Note** *Accept other valid answers.*	

7	**Extracts 2 and 3 highlight the role the Singapore government plays in promoting and protecting Singapore's national interests.** **Do you think that diplomacy or deterrence is more effective in promoting and protecting Singapore's national interests? Explain your answer.**	**[8]**

L1	**Writes about the topic without addressing the question (i.e. working for the good of society)**	**[1–2]**
L2	**Describes the factors** *Award 3 marks for describing one factor.* *Award 4 marks for describing both factors.*	**[3–4]**
L3	**Explain the strategies** **Note: An explanation is showing how diplomacy and/or deterrence is effective in promoting and protecting Singapore's national interests.** Award 5-6 marks for explaining one strategy. Award 6-7 marks for explaining both strategies. Diplomacy is Singapore's most powerful tool due to its geographical and economic vulnerabilities. As a small state without strategic depth or natural resources, Singapore depends heavily on international partnerships, trade, and stability. Diplomacy allows Singapore to secure its position on the global stage, maintain friendly ties with both major and regional powers, and uphold a rules-based international order. A key example is Singapore's active role in ASEAN, where it supports regional cooperation and dialogue. Additionally, hosting the 2018 Trump-Kim summit demonstrated Singapore's reputation as a neutral and reliable diplomatic partner. By engaging constructively with global powers like the U.S., China, India, and the European Union, Singapore ensures its voice is heard and its economic interests are safeguarded. This shows that diplomacy helps Singapore influence its external environment proactively and peacefully ensures that we have strong ties, friends/allies that will come to our aid when we require, which is far more aligned with its long-term national strategy. However, diplomacy alone is insufficient without the backing of credible deterrence. Singapore has always recognised the need to complement its diplomatic efforts with a strong national defence. Through consistent investment in the Singapore Armed Forces (SAF) and the implementation of the Total Defence framework, Singapore ensures that it remains secure from both conventional and non-traditional threats. For instance, it participates in joint military exercises with countries like the United States and Australia to build readiness and international cooperation. Total Defence goes beyond military preparedness, involving civil, economic, social, psychological, and digital aspects, making it a whole-of-society approach. This robust defence posture acts as a deterrent to potential, not wanting to face the wrath if Sg's military thus reassuring international partners of Singapore's stability. Therefore, deterrence reinforces diplomacy by giving Singapore the security and confidence needed to engage internationally without fear of coercion.	**[5–7]**
L4	**Both aspects in L3 plus Explains the relative importance of each strategy** (Both examples above plus) e.g. In conclusion, while deterrence is critical to maintaining national security and supporting diplomatic credibility, **diplomacy is the more effective and sustainable strategy for Singapore to promote and protect its national interests**. Through active engagement in global and regional affairs, Singapore is able to shape its external environment in ways that deterrence	**[8]**

	alone cannot achieve. Diplomacy between nations/countries is the systemaic solution before deterrent means are employed, thus diplomacy is more effective. Nevertheless, the two must work hand in hand: **diplomacy leads, but deterrence ensures that diplomacy has weight**. Together, they form the dual pillars of Singapore's foreign and security policy.	