STUDENT TEST BOOKLET

READING SECTION (40 questions)

Passage 1

The digital age has ushered in an era of unprecedented connectivity and convenience, but it has also given rise to a new and ever-present danger: cyber threats. A cyber threat is any malicious act that seeks to damage data, steal data, or disrupt digital life in general. These threats are not a monolithic entity but rather a complex and evolving landscape of attack vectors, motivations, and actors. From individual hackers to sophisticated state-sponsored groups, the perpetrators of cybercrime are driven by a variety of motives, including financial gain, espionage, and political activism. The impact of these threats is far-reaching, affecting not only large corporations and governments but also small businesses and individuals.

The most common types of cyber threats include malware, phishing, and denial-of-service attacks. Malware, short for malicious software, is a broad category that encompasses viruses, worms, trojans, and ransomware. Ransomware, in particular, has become a significant threat, with attackers encrypting a victim's data and demanding a ransom for its release. Phishing attacks, on the other hand, rely on social engineering to trick individuals into divulging sensitive information such as passwords and credit card numbers. These attacks often take the form of deceptive emails or messages that appear to be from a legitimate source. Denial-of-service (DoS) attacks aim to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

The financial consequences of cybercrime are staggering. Billions of dollars are lost each year to direct theft, disruption of business operations, and the costs of remediation. Beyond the immediate financial losses, cyberattacks can also have a devastating impact on a company's reputation. A data breach can erode customer trust and lead to a loss of business. Furthermore, the theft of intellectual property can undermine a company's competitive advantage and have long-term economic consequences.

In response to the growing threat of cybercrime, organizations are increasingly turning to international standards such as ISO 27001 to guide their cybersecurity efforts. This standard provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). By adopting a systematic approach to risk management, organizations can better protect themselves against the ever-evolving landscape of cyber threats. This includes not only implementing technical controls but also fostering a culture of security awareness among employees. Ultimately, in an age where our lives are increasingly intertwined with the digital world, cybersecurity is a shared responsibility that requires a multi-faceted and proactive approach.

Questions 1-13

Questions 1-6

Do the following statements agree with the information given in the reading passage?

In boxes 1-6 on your answer sheet, write

- **TRUE** if the statement agrees with the information
- **FALSE** if the statement contradicts the information
- **NOT GIVEN** if there is no information on this*

1. Cyber threats are solely the work of individual hackers.
2. Ransomware is a type of malware.
3. Phishing attacks always involve the use of viruses.
4. The financial impact of cybercrime is limited to direct theft.
5. ISO 27001 is a mandatory standard for all businesses.
6. Employee training is an important part of cybersecurity.

Questions 7-10

*Choose the correct letter, **A, B, C** or **D**.*

Write the correct letter in boxes 7-10 on your answer sheet.

1. What is the primary motivation for most cyber attacks? A. Political activism B. Espionage C. Financial gain D. Not mentioned in the passage

2. Which of the following is NOT a type of malware? A. Virus B. Worm C. Phishing D. Trojan

3. What is the main purpose of a denial-of-service attack? A. To steal data B. To encrypt data C. To disrupt services D. To install malware

4. What does ISO 27001 provide a framework for? A. Developing new cybersecurity software B. Prosecuting cybercriminals C. Managing information security D. Training cybersecurity professionals

Questions 11-13

Complete the summary below.

*Choose **NO MORE THAN TWO WORDS** from the passage for each answer.*

Write your answers in boxes 11-13 on your answer sheet.

Cyber threats represent a significant and growing danger in the digital age. These threats are carried out by a variety of actors with different motivations, and they can have a devastating impact on both organizations and individuals. Common types of cyberattacks include malware, phishing, and denial-of-service attacks. The consequences of these attacks are not just financial; they can also damage a company's 11. _____ and undermine its 12. _____. *To combat these threats, organizations can adopt a systematic approach to risk management, such as the one outlined in ISO 27001. This involves not only implementing technical controls but also promoting a culture of 13.* _____ among employees.

Passage 2

A. The proliferation of cyber threats has necessitated the development of sophisticated defense mechanisms. One of the most critical components of a robust cybersecurity strategy is the proactive identification and mitigation of vulnerabilities. A vulnerability is a weakness in a system or its security procedures that could be exploited by a threat actor. These weaknesses can exist in a variety of forms, from unpatched software and misconfigured systems to a lack of employee awareness. Threat actors are constantly searching for these vulnerabilities, and a single unaddressed weakness can be enough to compromise an entire network.

B. The process of vulnerability management is a continuous cycle that involves identifying, classifying, remediating, and mitigating vulnerabilities. The first step is to

conduct regular vulnerability assessments to identify weaknesses in the IT infrastructure. This can be done through a combination of automated scanning tools and manual penetration testing. Once vulnerabilities are identified, they need to be classified based on their severity and the potential impact they could have on the organization. This allows security teams to prioritize their remediation efforts and focus on the most critical risks first.

C. Remediation is the process of fixing a vulnerability, which can involve applying a patch, changing a configuration setting, or implementing a new security control. However, not all vulnerabilities can be remediated immediately. In some cases, a patch may not be available, or the remediation process may be too disruptive to business operations. In these situations, organizations can implement mitigating controls to reduce the likelihood of a vulnerability being exploited. This could involve isolating the affected system from the network or implementing additional monitoring to detect any suspicious activity.

D. A key challenge in vulnerability management is the sheer volume of new vulnerabilities that are discovered every day. Security teams can quickly become overwhelmed by the number of alerts and the need to constantly patch and update systems. To address this challenge, many organizations are turning to automated solutions that can help to streamline the vulnerability management process. These tools can automate the process of scanning for vulnerabilities, prioritizing risks, and deploying patches, freeing up security teams to focus on more strategic initiatives.

E. Another important aspect of vulnerability management is the need to address the human element. Employees can be a significant source of vulnerabilities, whether through unintentional mistakes or malicious intent. To mitigate this risk, organizations need to provide regular cybersecurity awareness training to educate employees about the latest threats and how to avoid them. This should be supplemented with clear policies and procedures that govern the use of company systems and data.

F. Ultimately, vulnerability management is not just about technology; it is about creating a culture of security within an organization. This requires a commitment from all levels of the organization, from senior leadership to individual employees. By fostering a proactive and collaborative approach to security, organizations can significantly reduce their risk of a successful cyberattack and better protect their valuable assets.

Questions 14-26

Questions 14-19

*The reading passage has six paragraphs, **A-F**.*

Choose the correct heading for each paragraph from the list of headings below.

*Write the correct number, **i-viii**, in boxes 14-19 on your answer sheet.*

List of Headings

i. The role of automation in vulnerability management ii. The importance of a security-conscious culture iii. The continuous cycle of vulnerability management iv. The human factor in cybersecurity v. The challenge of prioritizing vulnerabilities vi. The nature of cybersecurity vulnerabilities vii. The process of fixing and mitigating vulnerabilities viii. The growing threat of cybercrime

1. Paragraph A
2. Paragraph B
3. Paragraph C
4. Paragraph D
5. Paragraph E
6. Paragraph F

Questions 20-23

*Choose the correct letter, **A, B, C** or **D**.*

Write the correct letter in boxes 20-23 on your answer sheet.

1. What is the first step in the vulnerability management process? A. Remediation B. Classification C. Identification D. Mitigation
2. Why might a vulnerability not be remediated immediately? A. It is not considered a serious risk. B. A patch is not yet available. C. The security team is too busy. D. The organization does not have the right tools.
3. What is a major challenge in vulnerability management? A. The high cost of security tools B. The lack of skilled security professionals C. The large number of new vulnerabilities D. The difficulty of training employees

4. What is the ultimate goal of vulnerability management? A. To eliminate all vulnerabilities B. To create a culture of security C. To implement the latest security technologies D. To comply with industry regulations

Questions 24-26

Complete the sentences below.

*Choose **NO MORE THAN THREE WORDS** from the passage for each answer.*

Write your answers in boxes 24-26 on your answer sheet.

1. A vulnerability is a weakness that can be exploited by a _____.
2. Automated solutions can help to _____ the vulnerability management process.
3. Regular cybersecurity awareness training can help to mitigate the risk of the _____.

Passage 3

The rise of the Internet of Things (IoT) has created a world of interconnected devices, from smart homes and wearable technology to industrial control systems and critical infrastructure. While this connectivity offers immense benefits in terms of efficiency and convenience, it also presents a new and complex set of cybersecurity challenges. Each IoT device represents a potential entry point for attackers, and the sheer number of these devices makes it difficult to secure them all. As a result, the IoT has become a prime target for cybercriminals, who are constantly finding new ways to exploit its vulnerabilities.

One of the biggest security risks associated with the IoT is the use of default or weak passwords. Many IoT devices are shipped with default credentials that are easy to guess, and users often fail to change them. This makes it easy for attackers to gain unauthorized access to these devices and use them to launch further attacks. In addition, many IoT devices are not designed with security in mind and lack the ability to be patched or updated. This means that even if a vulnerability is discovered, it may not be possible to fix it, leaving the device permanently exposed.

The consequences of an IoT-related cyberattack can be severe. In a smart home, for example, an attacker could gain control of a connected thermostat and use it to cause physical damage to the home. In a healthcare setting, an attacker could compromise a

medical device and put a patient's life at risk. In the industrial sector, an attacker could disrupt a critical manufacturing process or even cause a catastrophic failure of a power grid or water supply system. The potential for widespread disruption and harm is enormous, and it is a threat that we are only just beginning to grapple with.

Securing the IoT is a complex challenge that requires a multi-layered approach. First and foremost, manufacturers need to build security into their devices from the ground up. This includes using strong encryption, implementing secure boot processes, and providing a mechanism for over-the-air updates. Second, users need to be educated about the risks of the IoT and the importance of using strong passwords and keeping their devices up to date. Finally, we need to develop new security technologies and standards that are specifically designed for the unique challenges of the IoT. This includes everything from lightweight encryption algorithms to new authentication and authorization protocols.

Ultimately, the security of the IoT is a shared responsibility that requires the cooperation of manufacturers, users, and security researchers. It is a challenge that we must address if we are to fully realize the benefits of a connected world without exposing ourselves to unacceptable risks. The future of the IoT depends on our ability to build a secure and resilient ecosystem that can withstand the ever-evolving threat of cybercrime.

Questions 27-40

Questions 27-32

Do the following statements agree with the information given in the reading passage?

In boxes 27-32 on your answer sheet, write

- **YES** if the statement agrees with the claims of the writer
- **NO** if the statement contradicts the claims of the writer
- **NOT GIVEN** if it is impossible to say what the writer thinks about this*

1. The Internet of Things has more benefits than drawbacks.
2. All IoT devices can be easily patched and updated.
3. An IoT attack in a healthcare setting could be fatal.
4. Manufacturers are solely responsible for securing the IoT.
5. New security technologies are needed to address the challenges of the IoT.

6. The future of the IoT is uncertain.

Questions 33-36

*Choose the correct letter, **A, B, C** or **D**.*

Write the correct letter in boxes 33-36 on your answer sheet.

1. What is one of the biggest security risks associated with the IoT? A. Lack of user interest B. Weak or default passwords C. High cost of devices D. Limited internet connectivity

2. What is a major security flaw in many IoT devices? A. They are not compatible with each other. B. They cannot be patched or updated. C. They are too difficult to use. D. They consume too much power.

3. What is the potential consequence of an IoT attack on the industrial sector? A. Minor inconvenience B. Loss of data C. Disruption of critical infrastructure D. Reputational damage

4. Who is responsible for securing the IoT? A. Manufacturers B. Users C. Security researchers D. All of the above

Questions 37-40

Complete the notes below.

*Choose **NO MORE THAN TWO WORDS** from the passage for each answer.*

Write your answers in boxes 37-40 on your answer sheet.

Securing the Internet of Things

- Manufacturers should build 37. _____ into their devices.
- Users should be educated about the 38. _____ of the IoT.
- New security technologies and 39. _____ need to be developed.
- The security of the IoT is a 40. _____.

LISTENING SECTION (40 questions)

Section 1: Questions 1-10

Complete the form below.

*Write **ONE WORD AND/OR A NUMBER** for each answer.*

Cybersecurity Incident Report

Example	
Caller’s Name:	Anna Smith
—	—
Incident Details	
Type of incident:	Phishing email
Date of incident:	1. _____
Time of incident:	2. _____
Email subject line:	Urgent: 3. _____ Required
Sender’s email address:	4. _____@mail-services.com
Action Taken	
Did you click on any links?	No
Did you provide any personal information?	No
What did you do with the email?	5. _____ it
Further Information	
Have you received similar emails before?	Yes, 6. _____
What was the main concern?	The email asked for my 7. _____
Advice Given	
Never share personal information online.	
Always verify the 8. _____ of the email.	
Install 9. _____ software.	
Report suspicious emails to the 10. _____ department.	

Section 2: Questions 11-20

Questions 11-15

*Choose the correct letter, **A, B,** or **C**.*

1. What is the main topic of the talk? A. The history of cybercrime B. The psychology of social engineering C. The technical aspects of hacking
2. What is the primary goal of a social engineer? A. To damage computer systems B. To gain the trust of a victim C. To steal money from a bank
3. Which of the following is NOT a common social engineering technique? A. Phishing B. Baiting C. Hacking
4. What is pretexting? A. Leaving a malware-infected device for someone to find B. Creating a fake scenario to obtain information C. Sending a deceptive email to a large number of people
5. What is the best defense against social engineering? A. Using strong passwords B. Installing antivirus software C. Being cautious and skeptical

Questions 16-20

What type of social engineering attack is described in each of the following situations?

*Choose your answers from the box and write the letters **A-F** next to questions 16-20.*

Types of Social Engineering Attacks

A. Phishing B. Spear Phishing C. Whaling D. Baiting E. Quid Pro Quo F. Tailgating

1. An attacker leaves a USB drive labeled “Confidential” in a company’s parking lot.
2. An attacker sends a personalized email to a specific employee, pretending to be from the IT department.
3. An attacker calls an employee and offers to help with a technical problem in exchange for their login credentials.
4. An attacker follows an employee through a secure door to gain access to a restricted area.
5. An attacker sends a fraudulent email to the CEO of a company, attempting to trick them into transferring money.

Section 3: Questions 21-30

*Choose the correct letter, **A, B,** or **C**.*

1. What is the main topic of the discussion? A. The rise of state-sponsored cyber attacks B. The economic and social impact of cybercrime C. The challenges of prosecuting cybercriminals

2. According to the professor, what is the most significant economic impact of cybercrime? A. The cost of remediation B. The loss of intellectual property C. The disruption of business operations

3. What is the 'ripple effect' of a cyberattack? A. The direct financial losses to a company B. The long-term damage to a company's reputation C. The impact on a company's supply chain and customers

4. How does cybercrime affect individuals? A. It can lead to financial loss and identity theft. B. It can cause emotional distress and anxiety. C. Both A and B.

5. What is the 'digital divide' in the context of cybercrime? A. The gap between those who have access to the internet and those who do not B. The gap in cybersecurity knowledge between different demographics C. The difference in how cybercrime affects developed and developing countries

6. Why is it difficult to measure the true cost of cybercrime? A. Many incidents go unreported. B. The costs are often indirect and difficult to quantify. C. Both A and B.

7. What is the role of governments in combating cybercrime? A. To pass and enforce strong cybersecurity laws B. To promote international cooperation C. Both A and B.

8. What is the 'cybersecurity poverty line'? A. The inability of individuals and small businesses to afford basic cybersecurity protection B. The lack of cybersecurity infrastructure in developing countries C. The shortage of skilled cybersecurity professionals

9. What is the main challenge in international cooperation against cybercrime? A. Different legal systems and definitions of cybercrime B. Lack of trust between countries C. Both A and B.

10. What is the key takeaway from the discussion? A. Cybercrime is a complex problem with no easy solution. B. Individuals have a limited role to play in

preventing cybercrime. C. Technology alone can solve the problem of cybercrime.

Section 4: Questions 31-40

Complete the notes below.

*Write **ONE WORD ONLY** for each answer.*

The Future of Cybersecurity

Emerging Threats

- **Artificial Intelligence (AI):**
  - AI-powered attacks can be more sophisticated and 31. _____.
  - AI can be used to create more convincing phishing emails and 32. _____.
- **Internet of Things (IoT):**
  - The number of IoT devices is growing, creating a larger 33. _____ surface.
  - Many IoT devices are not secure and can be easily 34. _____.
- **Quantum Computing:**
  - Quantum computers could break current 35. _____ methods.
  - This is a long-term threat, but we need to start preparing now.

Future Trends in Cybersecurity

- **Zero Trust Architecture:**
  - Assumes that no user or device can be trusted by 36. _____.
  - Requires strict identity verification for every person and device.
- **Cybersecurity Mesh:**
  - A more flexible and 37. _____ approach to security.
  - Allows for security to be applied to individual devices rather than a central network.
- **The Role of AI in Defense:**
  - AI can be used to detect and respond to threats more 38. _____.

    - AI can also be used to automate many security tasks.
- **The Human Element:**
    - Cybersecurity is not just a technical problem; it is also a 39. _____ problem.
    - We need to invest in training and awareness to create a more security-conscious 40. _____.

WRITING SECTION

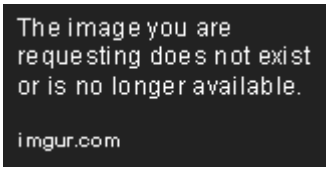
WRITING TASK 1

You should spend about 20 minutes on this task.

The chart below shows the most common types of cyber attacks reported by businesses in 2023.

Summarise the information by selecting and reporting the main features, and make comparisons where relevant.

Write at least 150 words.



(Note: A placeholder image is used here. In a real test, a proper chart would be provided.)

Common Types of Cyber Attacks Reported by Businesses in 2023

Type of Attack	Percentage of Businesses Reporting
Phishing	83%
Malware	51%
Ransomware	39%
Denial-of-Service	27%
Insider Threat	22%

WRITING TASK 2

You should spend about 40 minutes on this task.

Write about the following topic:

Some people believe that the government should be primarily responsible for protecting citizens from cybercrime, while others argue that it is the responsibility of individuals to protect themselves.

Discuss both these views and give your own opinion.

Give reasons for your answer and include any relevant examples from your own knowledge or experience.

Write at least 250 words.

SPEAKING SECTION

Part 1

The examiner asks the candidate about him/herself, his/her home, work or studies and other familiar topics.

Cybersecurity

- How much do you know about cybersecurity?
- Do you use any security software on your computer or phone?
- Have you ever received a phishing email? What did you do?
- What steps do you take to protect your personal information online?
- How important do you think it is for people to be aware of cybersecurity risks?

Part 2

You will have to talk about the topic for one to two minutes. You have one minute to think about what you are going to say. You can make some notes to help you if you wish.

Describe a time when you were concerned about your online security.

You should say:

- when this happened
- what the situation was
- how you felt about it

and explain what you did to resolve the situation.

Part 3

Discussion topics:

Cybersecurity Threats and Society

- What do you think are the biggest cybersecurity threats facing people in your country today?
- Why do you think cybercrime is increasing so rapidly?
- In what ways can companies and governments cooperate to fight cybercrime?

Individual Responsibility in Cybersecurity

- To what extent should individuals be responsible for their own online security?
- Do you think schools should teach children about cybersecurity? Why or why not?
- How can we encourage older people to be more cautious about online scams?

GRAMMAR SECTION (20 questions)

Questions 1-5: Error Correction

Identify the error in each sentence and correct it.

1. The company's data were compromised due to a lack of adequate security measure.
2. He is having a new security system installed tomorrow.
3. If I would have known about the phishing scam, I would not have clicked on the link.
4. The number of cyber attacks are increasing every year.
5. Each of the employees have to complete the cybersecurity training.

Questions 6-10: Sentence Transformation

Complete the second sentence so that it has a similar meaning to the first sentence, using the word given. Do not change the word given. You must use between two and five words, including the word given.

1. The company has to improve its cybersecurity measures. (**needed**) An improvement in the company's cybersecurity measures _____ .
2. The employees were not aware of the risks. (**little**) The employees _____ of the risks.
3. The hackers stole a large amount of data. (**was**) A large amount of data _____ by the hackers.
4. It is possible that the company will be fined. (**could**) The company _____ for the data breach.
5. The IT department is dealing with the security incident. (**by**) The security incident is _____ the IT department.

Questions 11-15: Fill in the Blanks

Fill in the blanks with the correct form of the verb in brackets, or a suitable article or preposition.

1. The company _____ (invest) in a new security system last year.
2. You should always be careful when you are _____ the internet.
3. The new software is designed to protect _____ malware.
4. He has been working _____ a cybersecurity analyst for five years.
5. _____ most important thing is to stay vigilant.

Questions 16-20: Word Formation

Use the word in capitals to form a word that fits in the gap in the same line.

1. The company is committed to the _____ of its customers' data. (PROTECT)
2. It is _____ to keep your software up to date. (ESSENCE)
3. The _____ of the new security system was a complex process. (INSTALL)

4. The company has a team of _____ cybersecurity professionals. (HIGH)
5. The government has introduced new _____ to combat cybercrime. (LEGISLATE)

LISTENING SCRIPTS

Section 1

(The phone rings)

Cybersecurity Support: Hello, Cybersecurity Support, this is Mark speaking. How can I help you?

Anna Smith: Hello, my name is Anna Smith. I'm calling to report a suspicious email I received.

Cybersecurity Support: Okay, Anna. I can help with that. Can you tell me what type of incident it is?

Anna Smith: It's a phishing email.

Cybersecurity Support: I see. And when did you receive this email? What was the date?

Anna Smith: It was on the 15th of January.

Cybersecurity Support: The 15th of January. And do you remember the time?

Anna Smith: Yes, it was at 2:30 PM.

Cybersecurity Support: 2:30 PM. Got it. And what was the subject line of the email?

Anna Smith: It said, "Urgent: Account Verification Required".

Cybersecurity Support: "Account Verification Required". Okay. And can you tell me the sender's email address?

Anna Smith: Yes, it was security@mail-services.com.

Cybersecurity Support: security@mail-services.com. Thank you. Now, did you click on any links in the email?

Anna Smith: No, I didn't.

Cybersecurity Support: And did you provide any personal information?

Anna Smith: No, I didn't provide anything.

Cybersecurity Support: That's good. What did you do with the email?

Anna Smith: I deleted it.

Cybersecurity Support: Okay. Have you received similar emails before?

Anna Smith: Yes, a few times.

Cybersecurity Support: And what was your main concern about this particular email?

Anna Smith: It asked for my password.

Cybersecurity Support: I see. Well, you did the right thing by not responding. I'd like to give you some advice for the future. First, never share your personal information online, especially your password. Second, always verify the sender of the email. And third, it's a good idea to install antivirus software on your computer. Finally, if you receive any more suspicious emails, please report them to the IT department.

Anna Smith: Okay, I will. Thank you for your help.

Cybersecurity Support: You're welcome. Goodbye.

Section 2

(Monologue)

Hello everyone. Today, I'm going to talk about a type of cyber attack that doesn't involve any complex hacking or technical skills. It's called social engineering, and it's one of the most common and effective ways that cybercriminals trick people into giving up their personal information. So, what is social engineering? In simple terms, it's the art of manipulating people into performing actions or divulging confidential information. The primary goal of a social engineer is to gain the trust of a victim so that they can then exploit that trust to their own advantage.

There are many different social engineering techniques, but some of the most common include phishing, baiting, and pretexting. Phishing, as many of you probably know, involves sending deceptive emails that appear to be from a legitimate source, such as a bank or a well-known company. These emails often contain a link to a fake website where the victim is asked to enter their login credentials or other sensitive information. Baiting is a little different. It involves leaving a malware-infected device, such as a USB drive, in a place where someone is likely to find it. The attacker is hoping that the victim's curiosity will get the better of them and that they will plug the device into their computer, thereby infecting it with malware. Pretexting is a more sophisticated technique that involves creating a fake scenario, or pretext, to obtain information. For example, an attacker might call an employee and pretend to be from the IT department, claiming that they need the employee's login credentials to fix a technical problem.

So, what is the best defense against social engineering? It's not about using strong passwords or installing the latest antivirus software, although those things are important too. The best defense is simply to be cautious and skeptical. If you receive an email or a phone call that seems suspicious, don't be afraid to question it. And never, ever give out your personal information unless you are absolutely sure that the person you are dealing with is who they say they are.

Now, let's look at a few specific examples of social engineering attacks. Imagine you're in a coffee shop and you see a USB drive on the floor labeled "Confidential". What do you do? If you're like most people, you might be tempted to pick it up and see what's on it. But this is a classic example of a baiting attack. The USB drive is almost certainly infected with malware, and if you plug it into your computer, you could be giving an attacker access to all of your personal information.

Here's another example. You receive an email that appears to be from your company's IT department. The email says that there has been a security breach and that you need to click on a link to reset your password. This is a spear phishing attack. The email is highly targeted and designed to look as convincing as possible. But if you look closely, you'll probably notice a few red flags, such as a generic greeting or a suspicious-looking URL.

What about this situation? You get a call from someone who claims to be from your bank. They say that there has been a fraudulent transaction on your account and that they need you to confirm your login credentials to resolve the issue. This is an example

of a quid pro quo attack. The attacker is offering to help you with a problem in exchange for your personal information.

And finally, imagine you're walking into your office building and someone is following closely behind you. They don't have a security pass, but they're carrying a large box and they look like they're in a hurry. You might be tempted to hold the door open for them, but this is a tailgating attack. The person is trying to gain access to a restricted area by following an authorized employee.

And a whaling attack is similar to spear phishing, but it specifically targets high-profile individuals, such as CEOs and other executives. The goal is to trick them into transferring money or divulging sensitive company information.

Section 3

(Academic Discussion)

Professor: So, we've been talking about the technical aspects of cybercrime, but I'd like to shift our focus now to the economic and social impact. What do you think is the most significant economic impact of cybercrime?

Student A: Well, I think the most obvious impact is the direct financial losses from theft and fraud. But I think the cost of remediation is also a huge factor. Companies have to spend a lot of money to fix the damage caused by a cyberattack, and that can have a big impact on their bottom line.

Professor: That's a good point. But what about the less obvious costs? What about the loss of intellectual property, for example?

Student B: Yes, I think that's a really important point. When a company's intellectual property is stolen, it can lose its competitive advantage, and that can have a long-term impact on its profitability. And then there's the ripple effect. A cyberattack on one company can have a knock-on effect on its supply chain and its customers.

Professor: Exactly. And what about the social impact? How does cybercrime affect individuals?

Student A: Well, on a personal level, it can lead to financial loss and identity theft, which can be devastating. But I think it can also cause a lot of emotional distress and anxiety. People can feel violated and unsafe, and that can have a real impact on their mental health.

Professor: That's very true. And what about the broader social impact? How does cybercrime affect society as a whole?

Student B: I think it can erode trust in our institutions. If people don't feel safe online, they're less likely to use online services, and that can have a negative impact on the economy. And then there's the issue of the digital divide. People who are less familiar with technology, such as older people or people from lower-income backgrounds, are often more vulnerable to cybercrime. This can exacerbate existing inequalities in society.

Professor: That's an excellent point. It's often said that it's difficult to measure the true cost of cybercrime. Why do you think that is?

Student A: Well, for one thing, many incidents go unreported. Companies are often reluctant to admit that they've been the victim of a cyberattack because they're worried about the damage to their reputation. And even when incidents are reported, the costs are often indirect and difficult to quantify. How do you put a price on the loss of customer trust, for example?

Professor: Precisely. So, what can be done to combat cybercrime? What is the role of governments?

Student B: I think governments have a crucial role to play. They need to pass and enforce strong cybersecurity laws, and they need to promote international cooperation to track down and prosecute cybercriminals. But I think they also have a role to play in educating the public about the risks of cybercrime.

Professor: I agree. And what about the concept of the 'cybersecurity poverty line'? What does that mean?

Student A: It refers to the inability of individuals and small businesses to afford basic cybersecurity protection. They may not have the money to buy antivirus software or to hire a cybersecurity expert, and that makes them more vulnerable to attack. It's a real problem, and it's one that we need to address.

Professor: Yes, it is. And what about the challenges of international cooperation?

Student B: I think the main challenge is the fact that different countries have different legal systems and different definitions of what constitutes a cybercrime. This can make it difficult to extradite criminals and to prosecute them effectively. And then there's the

issue of trust. Some countries are reluctant to share information with each other, and that can hamper investigations.

Professor: So, to sum up, what would you say is the key takeaway from our discussion today?

Student A: I would say that cybercrime is a complex problem with no easy solution. It requires a multi-faceted approach that involves governments, businesses, and individuals.

Student B: And I would add that technology alone cannot solve the problem. We need to invest in education and awareness to create a more security-conscious culture.

Section 4

(Academic Lecture)

Good morning, everyone. In today's lecture, we're going to be looking at the future of cybersecurity. We'll be exploring some of the emerging threats that we're likely to face in the coming years, as well as some of the future trends in cybersecurity that are being developed to combat these threats.

Let's start with the emerging threats. One of the biggest threats on the horizon is the use of artificial intelligence, or AI, in cyber attacks. AI-powered attacks can be much more sophisticated and adaptive than traditional attacks. For example, AI can be used to create more convincing phishing emails and malware that can evade detection. This is a major concern for cybersecurity professionals, and it's something that we need to be prepared for.

Another major threat is the Internet of Things, or IoT. The number of IoT devices is growing exponentially, and this is creating a much larger attack surface for cybercriminals to exploit. Many of these devices are not secure and can be easily compromised. This could have serious consequences, from the disruption of critical infrastructure to the loss of personal data.

And then there's the threat of quantum computing. Quantum computers have the potential to break many of the encryption methods that we currently use to protect our data. This is a long-term threat, but it's one that we need to start preparing for now. We need to develop new encryption algorithms that are resistant to attack from quantum computers.

So, those are some of the emerging threats. Now let's turn our attention to some of the future trends in cybersecurity. One of the most promising trends is the adoption of a zero-trust architecture. This is a security model that assumes that no user or device can be trusted by default. It requires strict identity verification for every person and device that wants to access a network or an application. This can help to prevent unauthorized access and to limit the damage caused by a successful attack.

Another important trend is the cybersecurity mesh. This is a more flexible and decentralized approach to security. It allows for security to be applied to individual devices rather than a central network. This can be particularly useful for securing IoT devices and for protecting remote workers.

Of course, AI is not just a threat; it can also be a powerful tool for defense. AI can be used to detect and respond to threats more quickly and accurately than humans can. It can also be used to automate many security tasks, freeing up cybersecurity professionals to focus on more strategic work.

Finally, I want to talk about the human element. Cybersecurity is not just a technical problem; it is also a human problem. We need to invest in training and awareness to create a more security-conscious culture. We need to teach people how to spot phishing emails, how to use strong passwords, and how to protect their personal information online. This is perhaps the most important thing we can do to improve our collective cybersecurity.

So, to conclude, the future of cybersecurity is both challenging and exciting. There are many new threats on the horizon, but there are also many new technologies and strategies being developed to combat these threats. By working together, we can create a safer and more secure digital future for everyone.

ANSWER KEY

Reading Section

1. FALSE
2. TRUE
3. FALSE

4. FALSE
5. NOT GIVEN
6. TRUE
7. C
8. C
9. C
10. C
11. reputation
12. competitive advantage
13. security awareness
14. vi
15. iii
16. vii
17. i
18. iv
19. ii
20. C
21. B
22. C
23. B
24. threat actor
25. streamline
26. human element
27. NOT GIVEN
28. NO
29. YES
30. NO
31. YES
32. NO

33. B
34. B
35. C
36. D
37. security
38. risks
39. standards
40. shared responsibility

Listening Section

1. 15th January / January 15
2. 2:30 PM
3. Account Verification
4. security
5. deleted
6. a few times
7. password
8. sender
9. antivirus
10. IT
11. B
12. B
13. C
14. B
15. C
16. D
17. B
18. E
19. F

20. C
21. B
22. B
23. C
24. C
25. B
26. C
27. C
28. A
29. C
30. A
31. adaptive
32. malware
33. attack
34. compromised
35. encryption
36. default
37. decentralized
38. quickly
39. human
40. culture

Grammar Section

1. The company’s data were compromised due to a lack of adequate security **measures**.
2. He **will have** a new security system installed tomorrow. (Original: He will has…)
3. If I **had known** about the phishing scam, I would not have clicked on the link.
4. The number of cyber attacks **is** increasing every year.
5. Each of the employees **has** to complete the cybersecurity training.

6. is needed
7. had little awareness
8. was stolen
9. could be fined
10. being dealt with
11. invested
12. on
13. against
14. as
15. The
16. PROTECTION
17. ESSENTIAL
18. INSTALLATION
19. HIGHLY
20. LEGISLATION

TUTOR GUIDE

Model Answer for Writing Task 1

The bar chart illustrates the prevalence of various types of cyber attacks as reported by businesses in the year 2023. The data is presented as percentages of businesses that experienced each type of attack.

Overall, phishing was by far the most common form of cyber attack, affecting the vast majority of businesses. The other types of attacks were significantly less common, with insider threats being the least frequently reported.

Phishing attacks were reported by a striking 83% of businesses, making it the most significant threat in the period shown. Malware was the second most common type of attack, but it was reported by a considerably lower percentage of businesses, at 51%.

Ransomware attacks were also a notable threat, with 39% of businesses reporting such incidents.

Denial-of-service attacks and insider threats were the least common types of cyber attacks, reported by 27% and 22% of businesses respectively. The figure for phishing is more than double that of ransomware, and nearly four times that of insider threats, highlighting its position as the primary cybersecurity challenge for businesses in 2023.

Model Essay for Writing Task 2 (Band 9)

In an increasingly interconnected world, the debate over who bears the primary responsibility for cybersecurity—the government or the individual—has become more pertinent than ever. While some argue that the state should provide a comprehensive shield against digital threats, others contend that personal vigilance is the most critical line of defense. This essay will discuss both perspectives before concluding that a collaborative approach is essential.

On the one hand, there is a strong case to be made for government-led cybersecurity initiatives. The state possesses the resources and authority to tackle large-scale cybercrime that is beyond the capacity of any single individual. This includes establishing national cybersecurity agencies, enacting robust legislation to prosecute cybercriminals, and engaging in international cooperation to combat cross-border threats. For instance, state-sponsored attacks and sophisticated criminal networks can only be effectively countered by the coordinated efforts of national governments. Furthermore, the government has a duty to protect its citizens from harm, and in the digital age, this responsibility extends to the virtual realm. By setting security standards for businesses and investing in critical infrastructure protection, the government can create a safer online environment for everyone.

On the other hand, the argument for individual responsibility is equally compelling. The vast majority of successful cyberattacks exploit human error, such as clicking on malicious links or using weak passwords. No amount of government intervention can completely eliminate this risk. Therefore, it is incumbent upon each person to practice good cyber hygiene. This includes using strong, unique passwords, enabling two-factor authentication, being cautious of unsolicited emails, and keeping software up to date. In essence, individuals are the gatekeepers of their own digital lives, and their actions are the first and most crucial line of defense. An informed and vigilant populace is a powerful deterrent to cybercrime, and this can only be achieved through personal effort and a commitment to continuous learning.

In my opinion, while both arguments have merit, the responsibility for cybersecurity is ultimately a shared one. The government should provide the framework, resources, and legal backing to combat large-scale threats, but individuals must take an active role in protecting themselves. It is a symbiotic relationship; government initiatives are rendered ineffective if citizens are careless, and individual efforts can be overwhelmed by sophisticated attacks without state-level support. Therefore, the most effective approach is a partnership between the state and its citizens, where the government provides the necessary tools and education, and individuals use them responsibly.

In conclusion, the fight against cybercrime requires a multi-layered approach. While the government must take the lead in tackling major threats and creating a secure digital infrastructure, individuals have an indispensable role to play in their own protection. Only through this collaborative effort can we hope to create a truly resilient and secure digital society.

Speaking Part 2 Sample Response

I'd like to talk about a time when I was quite concerned about my online security. It happened about a year ago when I received a very convincing email that appeared to be from my bank. The email claimed that there had been some suspicious activity on my account and that I needed to click on a link to verify my identity. At first, I was quite alarmed because the email looked very official. It had the bank's logo, and the language used was very professional.

I was about to click on the link, but then I remembered some advice I had read about phishing scams. I decided to take a closer look at the email, and that's when I noticed a few red flags. The sender's email address was slightly different from my bank's official address, and when I hovered my mouse over the link, the URL looked suspicious. It was a long string of random characters and didn't seem to be related to my bank at all.

I felt a mixture of relief and anger. I was relieved that I hadn't fallen for the scam, but I was also angry that someone had tried to trick me. It made me realize how vulnerable we all are to these kinds of attacks and how easy it would be to become a victim.

To resolve the situation, I immediately deleted the email and then went to my bank's official website by typing the address directly into my browser. I logged into my account and checked for any unusual activity, but everything seemed to be in order. I also reported the phishing email to my bank so that they could warn other customers. The experience taught me a valuable lesson about the importance of being vigilant

and skeptical when it comes to online communication. I'm much more cautious now, and I always double-check before clicking on any links or downloading any attachments.

Key Vocabulary List

1. **Cyber Threat:** Any malicious act that seeks to damage, steal, or disrupt digital life.
2. **Malware:** Malicious software designed to harm or exploit any programmable device, service, or network.
3. **Phishing:** A type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information.
4. **Ransomware:** A type of malware that encrypts a victim's files and demands a ransom to restore access.
5. **Denial-of-Service (DoS) Attack:** A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users.
6. **Vulnerability:** A weakness in a system or its security procedures that could be exploited by a threat actor.
7. **Remediation:** The process of fixing a vulnerability or a security flaw.
8. **Mitigation:** The action of reducing the severity, seriousness, or painfulness of a security risk.
9. **Internet of Things (IoT):** A network of interconnected devices that can collect and exchange data.
10. **Encryption:** The process of converting information or data into a code, especially to prevent unauthorized access.
11. **Social Engineering:** The art of manipulating people into performing actions or divulging confidential information.
12. **Pretexting:** A form of social engineering in which an individual lies to obtain privileged data.
13. **Baiting:** A social engineering attack where the attacker leaves a malware-infected physical device in a place where someone is likely to find it.
14. **Quid Pro Quo:** A social engineering attack in which an attacker offers a service or benefit in exchange for information or access.

15. **Tailgating:** A physical security breach in which an unauthorized person follows an authorized individual into a restricted area.
16. **Intellectual Property:** Intangible creations of the human intellect, such as inventions, literary and artistic works, designs, and symbols.
17. **Zero-Trust Architecture:** A security model that assumes no user or device can be trusted by default.
18. **Cybersecurity Mesh:** A flexible, composable architecture that integrates widely distributed and disparate security services.
19. **Vigilant:** Keeping careful watch for possible danger or difficulties.
20. **Resilient:** Able to withstand or recover quickly from difficult conditions.