Cyber Security

1.It seems with each passing month another big name is added to the growing number of organisations that have been subject to major attacks. Last month, it was revealed that hackers gained 'full functional control' to mission-critical systems at NASA's Jet Propulsion Lab, according to Inspector-General Paul Martin in a report to Congress. That followed BAE Systems admitting that computers used by engineers working on the F-35 fighter jet programme had previously been hacked, potentially compromising design and systems data.

2.It should come as no surprise then that engineering companies are vulnerable, both in terms of their intellectual property and their physical infrastructure (as the Stuxnet code that crippled Iran's nuclear centrifuges in 2010 attested).The question is what to do about it. For a sector that is notoriously technical and opaque, the solution is organic: people. Lone hackers have proved they can get into systems with little in the way of resources. The industry must therefore make sure it recruits these people before they are tempted to use their skills in altogether more sinister outlets.

3. That is the basic rationale behind the Cyber Security Challenge (CSC) – an initiative with some powerful backers, including Lockheed Martin, Qinetiq, HP Labs, Northrop Grumman, Cassidian, GCHQ, PWC and the UK government. It all started in 2011 with a series of competitions open to any amateur cyber enthusiasts not currently working in the industry. Students obviously feature heavily among the entrants, but the first overall winner, Dan Summers, was a working as a postman in Wakefield when he took part.

4. A number of top cyber-security professionals from some of the sponsor companies write the challenges, free of charge. One of the competitions – dubbed 'Secure and Control' and designed by (ISC)2 and Qinetiq – asks candidates how to ensure the security of programmes that operate security cameras, open pipes, dams or even security gates.

5. 'When we started off, we thought we'll run some competitions, we'll excite and inspire some people through,' said Baker, director of Cyber Security Challenge . 'But then it became very clear to us that we needed to do more than just run competitions.'

Surveying its own candidates, it found that 80–90 per cent with an interest and skill set in cyber security knew little or nothing about learning opportunities through the private sector or university and little or nothing about jobs in cyber security or how to get one. This contrasted with a survey by the SANS Institute, in which 90 per cent of companies said they couldn't staff to the level of cyber skills they wanted and 60 per cent said they were going to need more people in cyber security jobs over the next five years.

6.'It maps right the way back – it's not there at school; it's not there in careers sections. Universities have got spaces on their courses. Why have they got spaces on their courses? Well would you go for a course there if you didn't know what the subject was and you didn't know what the jobs were at the other end? We actually need to get the education to people from a very young age' explained Baker.

7.Clearly there are parallels with traditional engineering in terms of skills gaps and the quality of graduates, but there are also wider issues about public perceptions. Baker said, 'Most people want to get onto their computer and do whatever they want to do. They don't want to know anything about its internal workings. They don't want to have anything to do with security – it's just a bore.'

8.Speaking to candidates at the some of the award ceremonies, what appealed most to them about cyber security was the creative aspect. While the impression of cyber security might simply be geeks number-crunching and trying to crack passwords, most solutions actually require completely innovative thinking. It's not just about computer code but appreciating that systems have many different levels of vulnerability, both technological and human, and that a holistic approach is often the best way to secure them.

9.In terms of cyber security for companies and individuals, Baker also believes that manufacturers have a lot of catching up to do. 'You don't buy the car with a seatbelt in a bag and the bumper in another bag and be expected to fit them technically accurately – it's a bit like that still in the wild west of the computer world,' she said.

Cognome _____   Nome

_____

Matricola _____   Data _____

Facoltà   □ Civile e Industriale   □   Informazione,Informatica e Statistica

You must get an **overall score of more than 18** with a **minimum of 10 in Part 1** (the reading) and **5 in Part 2** (the writing section).

Part One

I. VOCABULARY (8 points)
The words in the left column (1, 2, …) appear in the text in this order. For each of them find a word with the same meaning from the right column (A, B, ….). Write your answers in the box below.

1. crippled	not interesting
1. attested	called
1. lone	tests
1. resources	have
1. outlets	make certain
1. backers	researching
1. sponsor	damaged
1. challenges	ability
1. dubbed	goes
1. ensure	equipment
1. run	help
1. surveying	spaces
1. skill	showed
1. maps	operations
1. gaps	ways
1. workings	backer
1. a bore	single

Example

1	G	2		3		4		5		6	

7		8		9		10		11		12	

13		14		15		16		17			

II. HEADINGS (4 points)
Choose the best question/title from the box for each of the paragraphs from the text.
Example: Paragraph 1   __a__

1.   Paragraph 2   _____

2.   Paragraph 3   _____

3.   Paragraph 4   _____

4.   Paragraph 5   _____

5.   Paragraph 6   _____

6.   Paragraph 7   _____

7.   Paragraph 8   _____

8.   Paragraph 9   _____

a. ~~Introduction~~
b. Job opportunities
c . An initiative
d. An image problem
e. Original thinking

f.	Types of questions
g.	A comparison
h.	The problem
i.	Lack of information

III. REFERENCE (4 points)

What do the underlined words in the sentence refer to?

Example: "That followed BAE" (par. 1) hackers gaining control of NASAs Jet Propulsion Lab

1. "their physical infrastructure" (par. 2)
_____

2. "do about it" (par.2)
_____

3. "these people" (par.2)
_____

4. "at the other end"(of what?) (par.6)
_____

IV. COMPREHENSION (4 points)

Part Two (10 points)

1. Write a paragraph about your experience of cyber activities.

Indicate if the following statements are true (T), false (F) or if there is not enough information (N) based only on the information in the text.
Example: An increasing number of computer systems have been attacked.   _T_

1.NASA and then BAE suffered cyber attacks. ____

2.Cyber experts for Lockheed Martin are involved in writing questions for CSS. ____

3. Baker argues that it's necessary to inform people about Cyber security before university age.   ____

4. Good cyber security depends on solutions which work on technological and human levels.   ____

....

....

....

....

....

....

....

....

....

2. You are interested in taking part in the next Cyber Security Challenge. Write an email to ask for further information about the next competition. (You could ask about when, where, cost, prerequisites, application process, etc)

....

....

....

....

....

....

....

....

....

....

Answers

Part One

I.
1G 2M 3Q 4J 5O 6K 7P 8C 9B 10E 11D 12F 13H
14I 15L 16N 17A

II.
1A 2H 3C 4F 5B 6I 7D 8E 9G

III.
1 engineering companies
2 security of systems
3 lone hackers
4 university course

IV.
1F (that followed BAE systems...)
2N
3T
4T