Unit 6

1 **Before you read, check that you know words 1–7. Match them with their definitions (a–g). Use a dictionary to help you if necessary. Then read the article to check your answers.**

1 hacking	**a** sending emails designed to gain secret information such as computer passwords
2 firewall	**b** a range of dishonest schemes
3 phishing	**c** related to computing, information technology and the internet
4 cyber	**d** gaining unauthorised access to data in a computer system
5 scams	**e** a network security system to prevent unauthorised access to computer data
6 breach	**f** an organisation or person that makes sure rules are followed
7 watchdog	**g** a breakdown in security

2 **Read the article again quickly and match the sub-headings (1–4) with the sections of the article (A–D).**

1 Tips to help a company prepare for a cyber attack ____
2 A comparison of employee and computer safety ____
3 A car company experiencing many cyber incidents ____
4 Examples of two types of computer attack ____

3 **Choose the correct option (a, b or c) to answer the questions.**

1 How many days does it take most companies to realise that a security problem has occurred?
a almost 100 **b** fewer than 60 **c** about 7

2 Who disapproved of the way Yahoo! handled the security problem?
a investors **b** customers **c** both

3 Why is it a danger to trust the security controls set by the company that supplies the computer network?
a They could already have a virus. **b** They might not be secure enough. **c** They don't have firewalls.

4 What did the hacking of San Francisco's public transit system affect?
a safety **b** health **c** payments

4 **Find words/phrases in the article with a similar meaning to the following.**

A **1** criminal _____
2 move money from one bank account to another _____
3 too trusting _____
B **4** unfriendly _____
5 main objectives _____
C **6** tidy up _____
7 paying attention and being interested _____
D **8** at the centre _____

5 **Complete the sentences with words/phrases from Exercise 4.**

1 The customer realised that he had been _____ when he gave his password and card number to a stranger, but explained that he thought that the email was from his credit card provider.
2 As a result of the security breach, the bank advised customers not to _____ money to unknown accounts.
3 Trust is _____ of a company's relationship with its clients, which is why the company must communicate quickly when data is hacked.
4 A successful business needs teams that are _____ and motivated.
5 In the meeting, we decided that the two main _____ are to review cyber security and check our staff guidelines.

FT

How to turn cyber attacks to your advantage

By Andrew Hill

A When handling hacking, the main weaknesses in most organisations are not technological – firewalls, software – but human. Since a villain pressed 'send' on the first phishing email, the human factor has played a part in cyber plots.

For example, scams where the widow of a general promises you money to help transfer their fortune – gullible people who believe the first sentence are most likely to trust the rest of the tale.

More recently, criminals have started making attacks to demand money from a company or threaten to create problems with its share price. Again, the approach uses basic human weaknesses. As a senior executive, you may well not know whether the hack is real or not – it still takes at least ninety-nine days for companies to discover a security breach, says consultancy Mandiant. So, are you prepared to risk saying that the news is fake?

B Big companies are under hostile cyber fire all the time – Volkswagen said it was facing 6,000 attacks a week – so it would be better to start thinking of the threat as an opportunity. As Amitava Dutta and Kevin McCrohan of George Mason University wrote in the early days of cyber risk, 'information security is not a technical issue; it is a management issue'. Leadership, culture and structure (or lack of them) have a 'significant impact' on what happens in an attack. So check your company's priorities.

C Spring-clean your structure. Organise files and throw out what you don't need. Find out what information you hold and where.

Update lines of communication, internal and external, and reexamine what your response will say about your attitude to different interests. For two years, Yahoo! failed to reveal a huge security breach as it tried to sell its core business, inviting criticism from customers, investors and watchdogs.

Make sure your staff are engaged. Carelessness about security may suggest reduced loyalty, risk taking, or worse, potential attacks from inside your own organisation.

Review your network. The computer security controls set by the supplier may not be secure. This could allow a virus to find a way in and infect the computers in your company.

Finally, be prepared. Executives' first reaction to a breach is often to spend time asking 'Who did this to me?', followed by a search for the 'guilty'. By contrast, when San Francisco's public transit system was held hostage by cyber attackers, managers were prepared and were able to decide quickly to open the gates and allow free travel. But if hackers had attacked safety rather than payments, the correct decision would have been to close the network.

D Good cyber security, like worker health and safety, is becoming obligatory, said Elizabeth Corley, vice-chair of Allianz Global Investors.

Hackers may be inadvertently performing a useful service: prompting executives to fix the human weaknesses at the heart of their organisations.