Unit 7

1 **Read the definitions of risk types below. Then read the text quickly and tick the risk types mentioned in it.**

1 cybercrime (= criminal activity carried out by means of the internet)
2 hacking (= an attempt to secretly gain access to someone's computer)
3 fraud (= the crime of obtaining money from someone by tricking them)
4 non-compliance (= failing to obey laws)
5 ransomware (= software that blocks your computer until a sum of money is paid)
6 phishing (= sending fake emails in order to get information such as passwords and credit card numbers)
7 malware (= software that is designed to cause harm to a computer)
8 denial-of-service attack (= where hackers try to make a network crash by flooding it with traffic)

2 **Read the text again. Match the people or companies (1–6) with the information (a–f) to make sentences.**

1	Deloitte	**a**	says that spending on risk management has grown due to both compliance issues and cybercrime.
2	Nicola Crawford	**b**	show the dangers of hacking by organising fake phishing attacks.
3	Wendy Tran	**c**	provides information that hackers can use to trick people in phishing attacks .
4	LinkedIn	**d**	showed the dangers of hacking by getting employees to plug unsafe items into their computers.
5	Trustwave	**e**	organised a survey to get statistical information about how companies manage risk.
6	KnowBe4	**f**	was a victim of phishing and identity theft.

3 **Decide which sentence (a or b) has a similar meaning to sentences (1–8) from the text.**

1 Institutions across the business world now have board-level risk committees.
a Many companies now have teams of people at the highest level to control risk.
b In every company the online meetings of senior managers are at risk of hacking.

2 Institutions now spend large amounts of money on third-party specialist advice.
a Companies now spend a lot of money asking three experts about what to do.
b Companies now spend a lot of money asking outside experts about what to do.

3 Hackers had filed fake tax returns on her behalf.
a Hackers pretended to be the government and got her to pay tax to them.
b Hackers pretended to be her and gave the government false tax information.

4 Hackers understand human psychology and play on greed, fear and curiosity.
a Hackers exploit feelings like being careful about money, taking risks and trusting people in authority.
b Hackers exploit feelings like the desire for money, worries that something bad might happen and the desire to know about things.

5 They sent modified keyboards, pretending they were rewards for good performance.
a They sent keyboards that had been slightly changed, and tried to trick people into thinking they were gifts because of their good work.
b They sent better quality keyboards, telling people that if they used them they would be able to work more efficiently.

6 Insurance companies spot a growth market.
a Insurance companies notice a market that is growing.
b Insurance companies are part of a market that is growing.

4 **Complete the sentences (1–8) with a phrase from the box. Be careful: some phrases are similar.**

assess risk	manage risk	minimise risk	potential risk	reduce risk	risk officer

1 If you _____ then you deal successfully with the problems associated with risk.
2 If you _____ then you make a risk smaller.
3 If you _____ then you make risk as small as possible.
4 A(n) _____ is the job title of the person in an organisation whose job it is to manage risk.
5 A(n) _____ is a possible risk in the future.
6 If you _____ then you decide how risky something is after thinking carefully about it.

Cybercrime and hacking – the modern face of risk

In 2008, at the height of the financial crisis, 73 percent of financial institutions had a Chief Risk Officer in their organisation to attempt to minimise risk. That figure is now 92 percent, according to a survey by consultants Deloitte. More and more institutions across the business world now have board-level risk committees.

The cost of managing risk has gone up considerably. Nicola Crawford, Chair of the UK's Institute of Risk Management, says that spending has increased 30–50 percent since the financial crisis. 'The main driver of this is the significant increase in banking regulations, as well as managing the increasing threats of cyber risk and fraud,' she says. Institutions now spend large amounts of money on third-party specialist advice, and there is a shortage of risk professionals.

In the decade after the financial crisis of 2008, the greatest risk to companies was non-compliance – the failure to obey complex laws introduced to reduce the risk of another crisis. But now the greatest risk is the threat from cyber criminals. According to the Deloitte survey, only 42 percent of respondents thought their company was extremely or very effective at managing cyber risk. Respondents viewed cyber security as one of the dangers that would increase most in the next two years.

Take the example of phishing (so called because the criminals 'fish' for data and passwords in the sea of internet users). These attacks trick staff with fake emails, with results that include loss of sensitive data, locking down of computers with malware that demands a ransom and even the transfer of funds to criminals' bank accounts.

Wendy Tran, an employee at a US company, discovered that hackers had filed fake tax returns on her behalf, hoping to get the refund that the government would pay to her. Her tax data and that of her colleagues had been sent to cyber criminals by an innocent HR employee. The HR member of staff, seeing an email request that looked like it was from someone with authority, attached Ms Tran's data and sent them off to the cyber criminals.

Many company boards are giving extra funds for cyber security technology, but experts warn that humans are the weak point when protecting companies from attack. Hackers understand human psychology and play on greed, fear and curiosity. They usually use a company's own website, or recruitment sites such as LinkedIn or Glassdoor, to discover who a target's manager is and then send an email pretending to be from that person. It can be something like 'we've seen there's this conference you might want to check out,' or 'this invoice doesn't look right, can you take a look?'. The recipient clicks on a link or downloads an attachment and their computer is infected.

There are many other ways to play on human weakness to gain access to networks. Karl Sigler, threat intelligence manager at cyber security specialist Trustwave, gives an example. He says many people are curious if they see a USB stick lying around in the workplace. They plug it in just to see what is on it. At that point their computer, and the whole network, is at risk. Trustwave have testers who act like hackers to show companies where their weaknesses are. In one test they sent modified keyboards to employees in an organisation, pretending they were rewards for good performance. Most people were suspicious and asked questions first, but five people plugged in the keyboards straight away. In a real situation this would have allowed hackers easy access to the company's network.

A similar company, KnowBe4, trains employees to be more careful of potential cybercrime. For example, they send fake phishing emails to an entire workforce to see how many people are tricked. Employees become aware of the dangers, and then take an online course to learn what to watch out for. They are told they will be tested with fake emails again in the future.

For the insurance industry, the growing number of cyberattacks is an opportunity. They spot a growth market as companies of all types increase their demand for cyber insurance. The market is estimated to be growing at about 28 percent annually at a time when other specialist insurance lines are shrinking. However, it is hard for insurance companies to assess levels of risk as the risks themselves are constantly evolving.