How to protect your institution from cyber attack

Level: Advanced (C1–C2)

Time: 60–90 minutes

Business topics: Banking and finance, business security, the threat of cyber-crime

Business language focus: Language associated with cyber-crime against banks and other financial institutions

Activities: In this lesson, students will:
- read a business article first published in the *Financial Times* and look at the language necessary to understand and talk about the article;
- learn or revise some common business collocations;
- discuss aspects of the article in greater depth;
- give advice on online security to a company that is planning to become digitalised for the first time.

Materials: One copy of the worksheet per student, internet access for Exercise 6

Group size: All of the tasks can be completed in pairs or groups, so that as much communication as possible takes place in the class. However, this lesson plan can also be used in a one-to-one teaching situation.

FT

This lesson is based on an authentic article from the *Financial Times*, republished here with its full, original text.

The article discusses how to protect businesses from cyber-attack.

Teacher's notes

1. Warmer

Write the term *cyber-crime* on the board and elicit its meaning (*crime committed online, such as stealing someone's personal information*). Ask students if they have ever been the victim of cyber-crime or if they know anyone who has.

Next they should look at their worksheet and decide which of the ways of protecting oneself online are good advice and which are bad advice. They should also put them in order from 1 (the best piece of advice) to 6 (the worst). Note that there is no single correct answer. It is a matter of opinion, so ask students to give reasons for their choice.

Key (possible answers):
- *Change your passwords regularly (good advice): If you always use the same password, it can be quite easy for criminals to find it and use it.*
- *Keep a list of all your passwords on your mobile phone (bad advice): If your mobile phone is lost or stolen, a criminal could use your passwords.*
- *Use passwords that are easy to remember, e.g. your family name, 123 (bad advice): The most common password is 123456789.*
- *Don't allow online companies to save your bank details (good advice): If you save your bank details on websites, they could be used if the websites are hacked.*
- *Use a mixture of upper-and lower-case letters, numbers and special symbols (e.g. punctuation marks) in your passwords (good advice): Mixing upper- and lower-case letters and using punctuation marks makes it harder for criminals to guess your passwords.*
- *Use the same password for several different accounts (bad advice): If one account is hacked, criminals can access all your accounts.*

2. Key words and expressions

Students search for words and expressions in the text and write them next to the definitions while noticing how the words are used in context.

Key:
1. *cyber stress test*
2. *hacker*
3. *breach (the full term is 'security breach', although the article only uses 'breach')*
4. *challenge*
5. *malware*
6. *legacy system*
7. *ramp up*
8. *spur on*
9. *phishing*
10. *fraudster*
11. *stakeholder*
12. *cyber heist*

How to protect your institution from cyber attack

3. Understanding the article

Students work individually to choose the best answers. They then compare their answers in pairs.

Key:

1. b
2. a
3. b
4. c
5. c
6. a

4. Business language – collocations

Students match the verbs with the nouns or noun phrases. They then check their answers by looking in the text and seeing the phrases in context. Note that there may be more than one possible answer in some cases but there is only one solution where each verb and/or noun phrase is only used once.

Key:

1. e
2. h
3. b
4. f
5. a
6. d
7. c
8. g

5. Discussion

In small groups, students discuss the questions which pick up on and expand on topics and quotes from the article. Hold a short whole-group feedback session and compare and contrast each group's answers and input.

6. Wider business theme – Digitalising a business

Ask students to read the short case study of a company that is not yet digitalised. Using the prompts given, they work in pairs or small groups and consider the advantages and disadvantages of digitalising the company, before coming to a final conclusion in the form of a short report to be presented to the class.

One-to-one teaching

This task can be adapted so that the student does the above as homework and then reports back (to you) in the next lesson. They should also be prepared to present their ideas as a report.

Teacher's notes

How to protect your institution from cyber attack

1 Warmer

Which of these ways of protecting yourself online are good advice and which are bad advice? Rank them from 1 (very good) to 6 (very bad).

_____ change your passwords regularly

_____ keep a list of all your passwords on your mobile phone

_____ use passwords that are easy to remember, e.g. your family name, 123

_____ don't allow online companies to save your bank details

_____ use a mixture of upper- and lower-case letters, numbers and special symbols (e.g. punctuation marks) in your passwords

_____ use the same password for several different accounts

2 Key words and expressions

Find the words or phrases in the article that match the definitions below. The paragraph numbers are given to help you.

1. a computer simulation technique used to see how well a company can function in a series of difficult situations (three words, para 2) _____
2. a person who uses a computer to connect to other people's computers secretly and often illegally to find, change or use information (para 3) _____
3. a situation in which someone discovers information that should be kept secret (para 5) _____
4. something that requires a lot of skill, energy and determination to deal with (para 6) _____
5. computing software that is designed to damage or destroy information on a computer (para 7) _____
6. a computer system that is still used although it is no longer the most modern or advanced, because it would be very expensive or difficult to replace it (two words, para 8) _____

Worksheet

How to protect your institution from cyber attack

7. to increase something, such as a rate or a level (two words, para 12)

_____

8. to encourage someone to do something or cause something to happen (two words, para 12)

_____

9. the practice of trying to trick someone into giving their secret bank information by sending them an email that looks as if it comes from their bank and that asks them to give their account number or password (para 13) _____

10. someone who commits the crime of obtaining money from people by tricking them (para 13)

_____

11. someone who has an interest in the success of a plan, system or organisation (para 13)

_____

12. an organised attempt by thieves to steal something online (two-words, para 17)

_____

Worksheet

How to protect your institution from cyber attack

How to protect your institution from cyber attack

Financial companies need to be vigilant and to share ideas, cyber experts say

BY PAUL MURPHY

FT

Paul Murphy, 25 March 2019.

1 The reach of cyber attacks on business is growing all the time. But the fight back is also under way.

2 Regulators in the UK are running war game-like cyber stress tests as well as knowledge-sharing networks to help companies boost their defences. But there is more work to do. Banks' risk managers put cyber attacks at the top of their list of concerns in a survey published by consultancy EY last year (see below).

3 The financial services industry is an obvious target for hackers. As Paul Taylor, UK head of cyber security at consultancy KPMG, says: "Criminals are lazy. They like to go to where there's lots of money, if only to reduce the workload."

4 While estimates vary, it is generally agreed that cyber crime is close to surpassing the illegal drugs trade in terms of its criminal appeal.

5 Breaches of customer data among companies ranging from mobile phone operators to credit check companies are routine topics of news reports. But breaches at banks typically cause the most alarm.

6 Cyber attacks and threats to payments systems now rank alongside terrorism and a possible pandemic as among the leading challenges in the UK's National Risk Register of Civil Emergencies.

7 The challenge is growing. "When it comes to malware," says Mr Taylor, "nothing ever goes away. The complexity of the threat just continues to grow."

8 In banking, there is a common assumption that those most at risk are the big, familiar names in the retail sector, which have clunky legacy systems prone to failure and gaping security holes. But experts say that is not necessarily the case.

9 "When it comes to the newer banking entities, the challengers and digital banks, they start with a natural advantage in that they don't have those legacy systems," says Mr Taylor. "They can start fresh in a very good security environment. But the danger is that they think first about growing their businesses quickly, and think about security second. And that's not a good idea."

10 Rob Wainwright, the former head of the EU's law enforcement agency Europol who is now a senior partner at Deloitte, echoes these concerns. For younger organisations with less resources and experience "the challenges are clear", he says.

11 "By definition, the start-up banks have a higher risk appetite. There's often a conflict of interest. You want to move quickly, but you have to build resistance quickly as well. It's a matter of how you balance that. It's a wide challenge for the sector."

12 Sir Rob adds that investment has ramped up substantially over recent years, spurred on by regulatory pressure and also the risk of bad publicity – as demonstrated by the IT meltdown suffered by UK retail bank TSB last year.

13 A botched migration of its IT systems led to an explosion of phishing attacks against TSB customers as fraudsters sought to take advantage of the chaos. The company pledged to refund any money lost in the attack and its executive chairman called for close co-operation in future between banks, the police and other stakeholders including telecoms companies.

14 When it comes to fighting back, cyber experts point to the success of the National Cyber Security Centre, established in the UK in 2016 as part of GCHQ, the country's electronic surveillance agency.

15 "They are getting the message across that, while you can't remove the threat, it can be managed," says Sir Rob. "It's about getting certain things right, following the checklists and having the right controls around the most sensitive assets."

Continued on next page

Worksheet

How to protect your institution from cyber attack

16 KPMG's Mr Taylor also cites FS-ISAC, a global finance industry body that shares cyber threat intelligence and analysis, as providing a forum for security teams across the wider financial sector.

17 The acute need for international co-operation was illustrated by the cyber heist on Bangladesh's central bank in 2016, when hackers were able to execute a series of transactions via the New York Federal Reserve to accounts in Sri Lanka and the Philippines. Though many more orders made by the hackers were blocked by the Fed, some $101m got through, the majority of which was not recovered.

18 In the UK, the Bank of England and the Financial Conduct Authority are also playing their part in guiding an industry facing complex and unpredictable threats.

19 Aside from the bank's cyber stress testing for systematically important institutions, the FCA is now quietly running an extended network of "cyber coordination groups," sharing information and experience among 175 businesses in the UK.

20 The resultant advice and checklists shared across the industry are refreshingly down to earth. They include tips on educating top executives, recruiting internal champions for cyber security at institutions and making the reporting of attacks easy for an organisation's entire staff.

21 There is a straightforward incentive. "Breaches cost money. And that's a great encouragement to getting stuff done," says Mr Taylor. For example, the FCA last year fined the banking arm of supermarket chain Tesco £16.4m for failings in the cyber heist it suffered in 2016, which saw £2.3m stolen from its customers.

22 As the UK regulator's guidance states: "Use case studies and incidents reported in the media to highlight potential risk and help executives link these risks to their business."

3 Understanding the article

Choose the best answers according to the text.

1. Why is the financial services industry 'an obvious target for hackers'?
   a Because it's easy to breach the security of financial companies.
   b Because hackers are lazy and prefer to target places where there is a lot of money.
   c Because financial services companies have old-fashioned legacy systems.

2. Data breaches at which of these types of companies cause the most alarm?
   a Financial institutions such as banks.
   b Companies whose activities are based on mobile phone use.
   c Credit check companies.

3. Why may newer banking entities such as digital banks not have an advantage when it comes to security?
   a Because they don't have clunky legacy systems.
   b Because growing their business quickly may be more important to them than security.
   c Because start-up banks have a lower risk appetite.

4. What happened to the UK retail bank TSB last year?
   a It suffered bad publicity as a result of regulatory pressure.
   b Many of its customers left the bank as a result of numerous phishing attacks.
   c Its IT systems failed and fraudsters tricked many of its customers.

5. What happened as a result of the cyber heist on Bangladesh's central bank in 2016?
   a Hackers stole a lot of money from the New York Federal Reserve.
   b $101 million was stolen but most of it was blocked and recovered.
   c More than 100 million dollars was stolen and sent to accounts in Sri Lanka and the Philippines.

Worksheet

How to protect your institution from cyber attack

6. What is the 'straightforward incentive' for UK businesses to improve their cyber security?
   a The fact that breaches of security cost money.
   b The fact that the supermarket chain Tesco was fined last year.
   c The fact that breaches of security lead to bad publicity in the media.

4 Business language – Collocations

Match the verbs in the left-hand column with the nouns and noun phrases in the right-hand column to make expressions from the text. Then find the phrases in the text to see them in context.

1.	reduce	a	investment
2.	cause	b	a business
3.	grow	c	a series of transactions
4.	highlight	d	advantage
5.	ramp up	e	the workload
6.	take	f	potential risk
7.	execute	g	intelligence
8.	share	h	alarm

5 Discussion questions

- The article states that cyber-attacks are as dangerous as terrorism and a possible pandemic in terms of risks to society. Do you agree? Give reasons for your answer.
- The article states that while the threat of cyber-attacks cannot be removed, it can be managed. In which ways do you think this threat can be managed?
- In paragraph 8, the author refers to the old-fashioned computer systems ('clunky legacy systems') and 'gaping security holes' in the retail sector. Online shopping is the preferred method for millions of people. How should they protect their security when making transactions online?
- In view of the threats that cyber-crime and malware pose, how safe do you feel when using your home computer or mobile device? What steps have you taken to improve your security online?

Worksheet

How to protect your institution from cyber attack

6 Wider business theme – Digitalising a business

Read this case study.

Rees Johnson is a small family business producing plastic packaging. The company doesn't use computers much and doesn't have an online presence. It wants to modernise, but is afraid of possible fraud and cyber-crime. Imagine that you are a member of a team of consultants hired by the company to examine the advantages and disadvantages of making the company more digital.

Here are some of the areas you could consider:

- **communication with suppliers**
- **communication with customers**
- **inventory and stock systems**
- **websites and mobile phone apps**
- **online invoicing and payments**
- **document storage**

Present your ideas to the class. Who had the best suggestions?

Worksheet