BUSINESS NEWS LESSONS

Cyber Security – the danger may be closer to home

1 Warmer

How many words do you know with the word *data*? Use these words to create noun or verb phrases and give a definition. Add any other expressions you know that contain the word *data*.

Nouns: bank breach file protection security

Verbs: download analyse leak mine migrate steal upload

2 Key words and expressions

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

1. a situation in which something cannot continue normally because of a problem (1) ____________________
2. to process information in large quantities automatically (2 words) (3) ____________________
3. to mention something so that people know about it (3) ____________________
4. to increase very quickly in amount or degree (6) ____________________
5. a feeling of anger towards someone because they have done something to you that does not seem right or fair (7) ____________________
6. the crime of stealing (7) ____________________
7. the activity of spying (7) ____________________
8. a responsibility or duty to do something (9) ____________________
9. becoming larger than something else (13) ____________________
10. beginning or formed recently (17) ____________________
11. acceptable (19) ____________________
12. causing unnecessary fear or worry (20) ____________________

Worksheet

Companies wrestle with growing cyber security threat: their own employees

Businesses deploy analytic tools to monitor staff as remote working increases data breach risk

BY HANNAH MURPHY

1 As cyber criminals and hackers ramp up their attacks on businesses amid coronavirus-related disruption, companies are also facing another equally grave security threat: their own employees.

2 Companies are increasingly turning to Big Brother-style surveillance tools to stop staff from leaking or stealing sensitive data, as millions work away from the watchful eyes of their bosses and waves of job cuts leave some workers disgruntled.

3 In particular, a brisk market has sprung up for cyber security groups that wield machine learning and analytics to crunch data on employees' activity and proactively flag worrying behaviours.

4 "We're seeing people say, 'I need better visibility into what my employees are doing with all of our data at home'," said Joe Payne, chief executive of cloud security group Code42, which tracks and analyses employees' activity on work devices. The group examines factors including when an employee typically works, what files they access and how much data they download.

5 "[Employers can ask] — if we have 10,000 employees, can you tell us who the most high-risk people are?" he said, adding that his company was handling a rise in cases of data theft among clients.

Insider threats

6 According to Mordor Intelligence, the $1.2bn data loss prevention market is set to balloon to $3.8bn by 2025, as many businesses migrate their data to the cloud.

7 So-called insider threats encompass employees unintentionally sharing private data outside of workplace networks, but also the deliberate stealing of data, typically motivated by financial opportunity or a grudge against an employer. Rarer, but a growing issue, is intellectual property theft and espionage on behalf of foreign governments.

8 Already more than a third of data breaches involve internal actors, according to a 2019 Verizon analysis of more than 40,000 incidents. At an exclusive meeting of top corporate cyber security heads at RSA, one of the largest cyber security conferences earlier this year, delegates labelled insider threats as their number one concern, according to one person in attendance — above nation state activity and threats from cyber criminals.

9 Traditionally, groups such as McAfee have offered tools that detect and block the exfiltration of sensitive data automatically. But there are also newer groups that seek to proactively alert employers to anomalous activity through behavioural analysis of data — which can involve screenshots and keystroke logging — and then place the onus on those employers to act in a way they see fit.

10 Falling under this category, Code42, Teramind, Behavox and InterGuard all told the Financial Times that they were seeing a rise in interest from potential clients under lockdown.

11 "There is an increase [during this pandemic] in people trying to steal intellectual property — reports or valuable HR data, client lists," said Erkin Adylov, chief executive of artificial intelligence group Behavox, which in February raised $100m from SoftBank's Vision Fund 2.

12 Its software analyses 150 data types to produce insights about employees' behaviour, including using natural language processing of email and workplace chats to assess "employee sentiment", he said. "Maybe there is uncertainty about [whether] the people are going to [keep] their job," Mr Adylov added.

Continued on next page

13 "The market is moving very fast. I would say it's probably growing at a clip of 100 per cent a year. The demand is outstripping supply," he said.

State adversaries

14 The risk of nation states opportunistically grooming employees for cyber espionage purposes is also a growing threat, several experts said. The issue was thrust into the spotlight recently when US officials last year charged two Twitter employees with mining data from the company's internal systems to send to Saudi Arabia.

15 "If I were a nation state actor [involved in cyber espionage] . . . certainly this is an opportunity to exploit some realities that exist. This is a heightened environment," said Homayun Yaqub, a senior security strategist at cyber group Forcepoint.

16 Executives at Strider Technologies, which wields proprietary data sets and human intelligence to help companies combat economic espionage, said it was seeing more recruitment of foreign spies, particularly by China, take place online under lockdown, rather than at events and conferences. "We're providing [customers] with the capability to respond to that [changing] adversary tactic," said chief executive Greg Levesque.

17 Nevertheless, critics argue that the technology is still nascent and further investment is needed to develop a more accurate understanding of what risky patterns of behaviour look like.

18 And while employers have long been able to legally monitor emails and web activity for signs of external cyber security threats, for some there is a discomfort about the privacy and trust implications of using such tools on staff.

19 "It's intrusive, it's not very culturally palatable," said former US army intelligence sergeant and former Palantir executive Greg Barbaccia. "To me, the insider threat is a cultural human problem. If someone wants to be malicious . . . you need to solve the human problem."

20 Omer Tene, vice-president of the International Association of Privacy Professionals, said: "Data breaches have been a huge issue. It's understandable why businesses would want to protect against that. I wouldn't be alarmist.

21 "But you need to be aware as a business and a technology of the creepy line," he added. "Are you doing anything . . . unexpected that will trigger backlash?"

FT

Hannah Murphy, 12 May 2020.

Articles republished from the Financial Times

Teacher's notes and worksheet: Published by Macmillan Education Ltd. © Macmillan Education Limited, 2020.

3 Understanding the article

Are these statements true or false according to the text? Correct the false statements.

1. Some companies are facing a security threat from their own employees under lockdown.
2. There is a growing market for cyber security groups that process data on employees' activity.
3. Cloud security group Code 42 tracks and analyses employees' activity on their home computers.
4. The data loss prevention market is predicted to increase its revenue from $1.2bn to $3.8bn by the end of this year.
5. People who steal data are usually doing it on behalf of foreign governments.
6. Typically, employees steal intellectual property such as reports, HR data and client lists.
7. Under lockdown, the recruitment of foreign spies takes place at events and conferences rather than online.
8. Critics of cyber security say the technology is still new and needs more investment.

4 Business language – two-word expressions

Match the words in the left-hand column with those in the right-hand column to make phrases from the text.

1.	security	a. theft
2.	machine	b. security
3.	data	c. espionage
4.	workplace	d. list
5.	cyber	e. threat
6.	client	f. problem
7.	economic	g. learning
8.	human	h. network

5 Business language – adjectives

Replace the underlined words in the sentences using these words from the text.

anomalous disgruntled grave intrusive palatable potential

1. Some companies believe that they face a serious ________________ security threat from their own employees.
2. Some employees may leak or steal sensitive data because they are annoyed ________________ after waves of job cuts.
3. Cyber security tools alert employers to unusual ________________ activity by employees online.
4. There is a rise in interest in this technology from possible ________________ clients under lockdown.
5. Critics argue that staff may find the use of this technology unwelcome ________________.
6. They also say that its use might not be culturally acceptable ________________.

6 Business language - word building

Complete the table.

	Verb	Noun
1.	survey	________________
2.	behave	________________
3.	attend	________________
4.	recruit	________________
5.	invest	________________
6.	imply	________________

7 Discussion questions

- Is it right for companies to spy on their own employees? Give reasons for your answer.
- What methods could and should companies use to protect sensitive data?
- In what ways has the lockdown contributed to attacks on businesses?

8 Wider business theme – staying safe online

1. **Staying safe online is both a problem for companies and a problem for individuals. You are the human resources manager of a small company that does most of its business online. Make a list of ways employees can say safe online (both at work and at home).**

   - Enter 'staying safe online' into an internet search engine.
   - Consult at least two websites that give tips about staying safe online.
   - Make a list of '*do's*' and '*don't's*' for all employees.

2. **Present your advice to the group.**