Companies wrestle with growing cyber security threat: their own employees

FT FINANCIAL TIMES

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 cybercriminals.

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.

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?"

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. to increase the rate or level of something (2 words) (1)
2. telling private or secret information to journalists or to the public (1)
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. spying (7)
7. unusual or unexpected (9)
8. to do something in order to stop something bad from happening or a bad situation from becoming worse (16)
9. beginning or formed recently (17)
10. becoming involved in something in a way that is not welcome (19)
11. acceptable (19)
12. a strong, negative and often angry reaction to something that has happened (21)

3 Understanding the article

Choose the best answer according to the text.

1. Why are companies particularly worried about their employees under lockdown?
a. because they don't know how much work their employees are doing when they are working from home
b. because employees who are not under supervision might be leaking or stealing sensitive data
c. because cyber criminals and hackers have increased their attacks on businesses during the coronavirus pandemic

2. What does the writer predict will happen to the cyber security industry?
a. It will make data loss prevention much more expensive by 2025.
b. It will see the turnover of the data loss prevention market increase by over 200% in the next five years.
c. It will see more employees sharing private data outside workplace networks.

3. How do newer data protection groups alert employers to unusual activity?
a. They inform employers when data is accessed and filtered, and stop the access automatically.
b. They inform employers and help them take appropriate action.
c. They detect when data is being accessed by analysing the behaviour they observe, such as the number of screenshots and keystrokes.

4. What kind of intellectual property are people trying to steal during the pandemic?
a. Financial information such as bank details.
b. Human resources data and client lists.
c. Information about new products.

5. What, in particular, has increased during the pandemic?
a. More data is being mined from internal systems to send to Saudi Arabia.
b. More adversary tactics are based on human intelligence.
c. More foreign spies are being recruited online than face-to-face.

6. What problem does Greg Barbaccia highlight?
a. He says that the threat to companies from their own employees is a cultural human problem.
b. He says that it is not alarmist for businesses to protect against internal data breaches.
c. He says that using technology tools to monitor staff has privacy and trust implications

4 Business language – collocations

Match the verbs in the left-hand column with the nouns or noun phrases in the right-hand column.

1. face	a. data
2. flag	b. a backlash
3. access	c. economic espionage
4. steal	d. a threat
5. trigger	e. intellectual property
6. combat	f. worrying behaviour

5. Business language - word building

Complete the sentences using the correct form of the word in brackets at the end of each sentence.

1. Employees might _____share private data outside of workplace networks even if they do not mean to do so. [INTENTION]
2. Some tools can detect and block the exfiltration of sensitive data_____ . [AUTOMATIC]
3. Newer groups are making use of_____ analysis of data. [BEHAVE]
4. Demand is_____ supply in the data analysis market. [STRIP]
5. More_____ of foreign spies is taking place under lockdown. [RECRUIT]
6. Using surveillance tools on staff is_____ and not very culturally palatable. [INTRUDE]

6. Grammar Infinitive or Gerund?

Look at the following sentences.

- Companies suggest changing passwords regularly.
- In most offices, staff are allowed to choose their own passwords.
- We recommend using a variety of characters in your password.
- You are warned not to store your password as plain text.
- You must avoid using the same default password.

Consider the underlined verbs. What do you notice? Why? Try the exercise on elearn (for Homework)

7. Cyber security Conversation Questions (if you finish before the others!)

Discuss the following questions. Use conditionals

1. Would you trust the cloud to keep your company's data safe? Why or why not?
2. Have you received training on cyber security at the IUT? If so, what did you learn? If not, do you think this would be a good idea?
3. What kind of software can help keep your computer systems safe?
4. What are the different motivations behind cybercrime?
5. How can cyberattacks lead to a company's reputation being damaged? Can you think of any examples when this happened?
6. Which governments are involved in cyberattacks? How could these attacks affect businesses?
7. Will new technology lead to better cyber security in the future, or will this new technology lead to Cybersecurity problems? Why?
8. What would happen if all the data in the world were made public? How would this change the world as we know it?