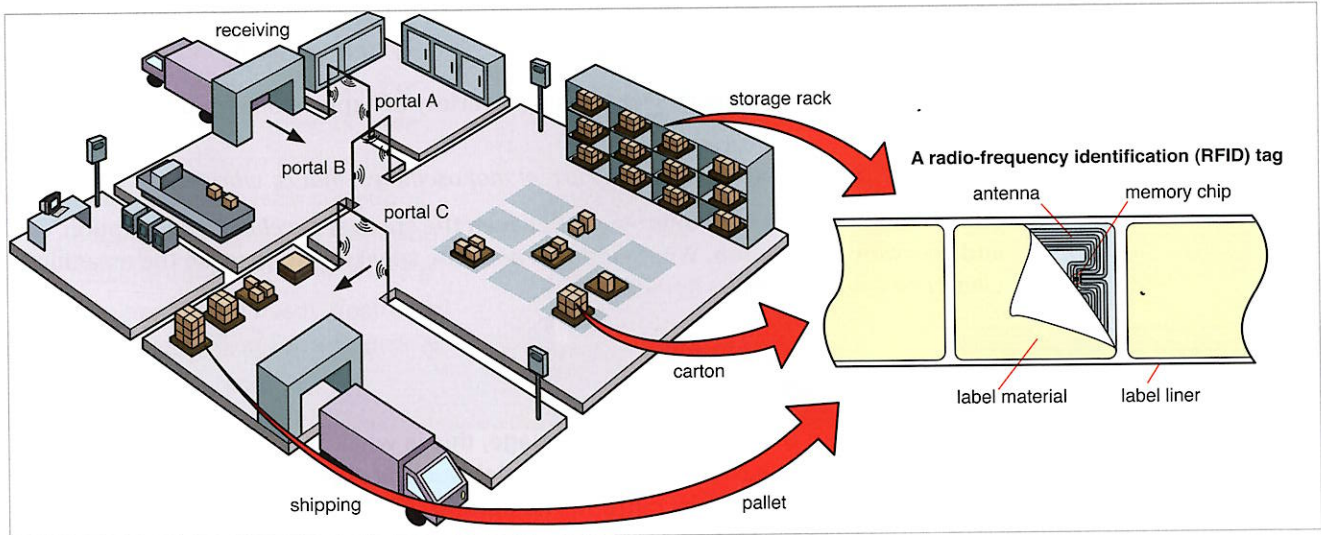


1 Theft

Start here 1 Work in groups. Discuss the main threats to security in a typical warehouse. What security measures are needed?



Reading 2 A theft has occurred at a warehouse. Read this memo about it and mark the following locations on the illustration above.

- 1 the place where RFID tags were first attached to the cartons
- 2 the faulty RFID scanning portal
- 3 the only two possible locations of the theft

TO: Head, Inventory Dept
FROM: Manager, Warehouse
SUBJECT: Missing cartons: preliminary thoughts

INCIDENT

The three cartons were taken from three pallets. The plastic film over the pallets was torn. There were no signs of a break-in to the warehouse from the outside.

CAUSES

We know for certain that (1) the cartons were RFID-tagged on receipt, (2) all carton tags scanned positive during put-away and picking and (3) one RFID scanning portal (portal C, between the warehouse and staging area) was faulty at the time of the incident.

1 Possibilities:

- goods stolen after picking from storage rack and before staging ☐
- theft occurred in staging area ☐

2 Things we can definitely rule out:

- cartons taken during receiving stage ☒

- cartons removed from storage rack prior to picking stage ☐

3 Assumptions we can safely make:

- theft carried out by insider (warehouse worker) ☐
- incident took place 08.30–09.25 ☐

4 Some mistakes identified:

- faulty portal C left out of action for two weeks ☐
- hand scanning not carried out at portal C ☐

RECOMMENDATIONS

- immediately review all CCTV footage in relevant areas ☐
- don't inform police until more information available ☐

NEXT STEP

As soon as the staff have been interviewed (by end of today), I'll brief you on the outcome. Other investigations are in hand. Can we meet first thing tomorrow?


- 3 Read the memo again and put the stages of the warehousing process in the correct order.

put-away <input type="checkbox"/>	storage <input type="checkbox"/>
staging <input type="checkbox"/>	shipping <input type="checkbox"/>
picking <input type="checkbox"/>	receiving <input type="checkbox"/>

- 4 Briefly explain what happens in a warehouse, changing the nouns in 3 into passive verbs.

Begin: *Immediately after the goods have been received, they are put away on racks ...*

Listening

- 5  21 Listen to this discussion and write the numbers 1–10 in the boxes in the memo, according to the order in which the points are mentioned.
- 6 Next to each numbered box in the memo in 2, write the modal form which was used in the discussion. The headings in the memo will help you work this out. Use each of the following modal forms once only. Then listen again and check your answers.

must have	can't have	should (have)	ought to (have)	couldn't have
might have	could have	has to have	shouldn't (have)	ought not to (have)

Language

Speculating about possibilities in the past: *The cartons **may / might / could have been** stolen here.*

Speculating about impossibilities in the past: *The cartons **can't / couldn't have been** taken out during the receiving stage.*

Speculating about probabilities or near certainties in the past: *The theft **must have / has to have been** carried out by an insider.*

Expressing regrets or criticisms about the past: *Hand scanning **should (not) have / ought (not) to have been** carried out*

Recommending an action for the future: *The police **should (not) be / ought (not) to be** informed yet.*

- 7 Change these sentences to give the same meaning using a variety of modals from the box in 6. Don't use the phrases in italics.

Example. 1 *The thieves can't have ...*

- It's not possible that* the thieves stole the cartons from the truck before they were received.
- It's certain that* the incident took place in the morning, but it's impossible that it happened before 08.30.
- It's possible that* the goods were stolen in the warehouse, and *another possibility* is that they were taken in the staging area.
- It's recommended that* we have another look at CCTV footage and that all security procedures are tightened up generally.
- It's virtually certain that* someone disabled the scanning portal deliberately.
- One mistake, which we regret, is that* the faulty portal was not checked on a daily basis and repaired as soon as the fault was discovered.

Speaking

- 8 Work in pairs. Question each other about the numbered items 1–4 in the memo. Respond using the appropriate modal.

A: *Were the goods stolen after picking and before staging?*

B: *Yes, that's a possibility. They could have been stolen at that point.*

2 Security

- Start here** 1 Discuss the situation below in pairs. What might / must / can't have happened? If you were the security administrator, what would you like your security system to be able to do?

At 08.12 the Sales Manager of Avantis plc can't find his company-issued mobile phone (which has an SD card containing sensitive company data). He immediately phones his office to report the loss. Meanwhile, over at Avantis HQ, the Security Administrator sees a security alert on her computer screen, indicating that someone is making repeated multiple incorrect password attempts to connect to the internet from the mobile phone.



- Reading** 2 Read part of a memo sent after the incident from the security director to the security administrator, and make a list (in note form) of what the security system can do, or allows you to do. Compare the list with your ideas in 1.

but at this point I'm not interested in what *might* have happened, what *must* have taken place or what *couldn't* have occurred. I want to know what *actually happened*. Specifically I need to know:

- | | |
|--|--|
| 1 how and when you first discovered that an unauthorised user (UU) was trying to use the device to go online, what action (if any) you took in response and your reasons for such action | 3 whether this response was successful |
| 2 at what point you realised that the UU was attempting to install software to download company files, what action(s) you took to counter this and | 4 whether you attempted to take over control of the mobile device remotely, whether or not such attempts were successful and why |
| | 5 whether or not you attempted to wipe company data from the device (including the SD card) remotely and if so, how you did it, and which methods (if any) proved successful |
| | 6 if you were able to determine where the mobile was located and in which direction it was moving, if any |

Language
page 104

- 3** Make direct questions.

Example: *I Who was the authorised user of the stolen mobile device?*

- 1 I would like to know who the authorised user of the stolen mobile device was.
- 2 Next, I need to find out why our employee was carrying a company mobile with him to a private party.
- 3 It's important that we determine how often he accessed company files that evening.
- 4 We've got to discover whether or not he downloaded sensitive data onto his SD card.
- 5 Tell me how much data the IT department allows employees to carry around.
- 6 Please check what kind of memory stick is currently being issued by the company.
- 7 Do we know if the mobile device was fitted with a GPS and camera?

- Speaking** 4 Work in pairs, A and B. Use the indirect questions in the memo in 2 to ask direct questions to each other to find out about the incident. Make complete notes: you will need them later.

Student A: You are the Security Director at Avantis. Ask the Security Administrator questions based on the memo and make notes of the answers.

Student B: You are the Security Administrator at Avantis. Turn to page 114 and use the information there to answer the Security Director's questions.

Then switch roles. Student A's material is on page 111.

LOCKDATA



LOCKDATA mobile security solutions can help you protect your sensitive corporate data against unauthorised access and data theft. Did you know that LockData allows your security administrator to take remote control of a stolen mobile phone, wiping (i.e. completely removing) all data from the device *and* from any connected storage devices such as SD cards and memory sticks? LockData achieves this using five methods:

- 1 on-demand wipe, in which the administrator can send a command to an online device to wipe all data instantaneously from device and storage card
- 2 pre-scheduled wipe on sight, where the device is programmed to wipe all data the next time the device is detected online
- 3 programmed time-based wipe, where an offline or out-of-contact device is programmed beforehand to wipe all data if it does not appear online for a specified number of hours
- 4 pre-set event-based wipe, where a wipe action is triggered by a specified action, such as multiple incorrect password entry attempts or installation of an unauthorised program
- 5 wipe by text message, which permits the administrator to send an encrypted SMS message to the offline device to execute a wake-up-and-wipe command

Which of the five methods ...

- 1 must be programmed in the mobile device in advance, before the device has been stolen?
- 2 can be executed during the incident itself, for example while the thief is using the phone to access data?
- 3 can be executed only while the device is connected to the internet?
- 4 operate if the thief carries out an operation specified in advance, such as trying to log in more than three times using the wrong security information?
- 5 can be executed even when the device is disconnected from the internet?

- Vocabulary** 6 Find the seven hyphenated word combinations in the brochure. Then match them with these phrases with the same or similar meaning. Each hyphenated combination acts as an adjective.

Example: *1 out-of-contact*

- 1 which cannot be contacted
- 2 dependent on a specified action being carried out
- 3 dependent on the passage of a fixed time
- 4 executed when it is requested
- 5 which makes the device switch on and remove all data
- 6 fixed or planned beforehand
- 7 planned beforehand to happen at a specific moment

- 7 Find words in the brochure with the same or similar meaning as the following.

- | | |
|-----------------------------|--------------------------|
| 1 needing to be kept secure | 4 from a distance |
| 2 illegal or not allowed | 5 immediately |
| 3 entry | 6 written in secret code |

- Writing** 8 You are the Security Administrator at Avantis. Write a concise report to your Security Director giving the main points of the data theft incident you worked on in 4. Write the report in five sections, as shown below. Summarise information from your scenario in 4 for sections 1–3. Select one item from the brochure for sections 4 and 5.

- 1 The incident
- 2 The security response
- 3 Outcome
- 4 Weaknesses in our security system
- 5 Recommended improvements to the system