

Staying alert:
Why and how
do you deal
with it?

It's your business to be sure
Workshop on security awareness





It's your business to be sure

Security awareness for companies and institutions

This workbook is part of the workshop 'It's your business to be sure' and ties in with the film of the same name. It was commissioned by the National Coordinator for Counterterrorism (NCTb).

The workshop was developed to enhance security awareness among employees of companies and institutions.

© NCTb 2009



Introduction

After the break-in at a company someone said: You know, I thought it was a bit strange to see someone walking around there.

After two men were picked up because they were taking pictures of security cameras, it appeared that various people had already seen them.

After a demonstration by an action group, an employee remembers that a couple of weeks before then, someone was very interested in his work and asked an inordinate amount of questions.

After an incident, it often appears that people have seen something that made them wonder: 'Wait a minute, is that right?' They were Not Sure about it.

In all these situations, the repercussions are still limited. But it could also involve an incident with a tremendous impact, as in the following example.

After the attack on a train in Russia it seemed that people in the neighbourhood had noticed people hanging around the track for days. They wondered what they were doing there, but took no action in reporting it. Looking back, it appeared that terrorists had secured a bomb on the rails, which derailed the train and wounded nearly 70 people.

You, too, may see something at your workplace that appears strange or out of the ordinary. A situation, an individual, something or someone you are Not Sure about. It does not have to mean anything, but it is better to make sure that you are Sure about it. You never know beforehand whether you might be preventing something.

Why is this so important? And how do you become Sure? This will all become clear in this workshop on security awareness, 'It's your business to be sure'. This booklet is part of that workshop. It contains a short summary of what security awareness entails, examples of alert actions, and points to consider for what you can do yourself. This booklet also has three assignments that you can use for further discussion with your colleagues on security awareness in your organisation. This booklet can also be used separately from the workshop. Re-read it after you have completed the workshop.

The message of the workshop **'It's your business to be sure'** is simple:
If you are Not Sure about something, turn it around to being Sure.

Programme of the workshop 'It's your business to be sure'

Part 1 is about security awareness in general and within your organisation. It is intended to provide food for thought on the risks that could play a role. Terrorism, criminality, vandalism and extremism are addressed. What could happen at your organisation? Discuss it with colleagues after you have watched the first part of the film.

Part 2 is about your own work environment and the situations that are Not Sure for you. For example, what would you notice personally if a terrorist, a (cyber) criminal or an extremist has it in for your organisation? Think about the preparations of such individuals.

Part 3 discusses the best thing you can do for security awareness. What do you do if a situation is Not Sure? How do you turn it around to being Sure? During the workshop, you also think about concrete points of action with which you and your colleagues can get to work. What can be done to limit the chances of someone who wants to do harm?

The text has specific points to consider for companies and institutions that work with chemical, biological, radiological and nuclear knowledge and resources. See the **CBRN** marking in the text.

Information about security awareness to read through again.

It is a short summary of what you also see in the film 'It's your business to be sure'.

Security awareness, is it really necessary?

People are usually trusting. That is good and often practical, but not always justified.

Every organisation is faced with risks and threats. For some organisations, terrorism is a theme of topical interest. Others are confronted with actions by extremists (from political, religious or idealistic point of view). Some organisations risk attack from cybercriminals who hack into computer networks via the Internet. And every organisation runs the risk of 'ordinary' criminals, vandals and graffiti writers.

CBRN Potentially dangerous chemicals and viruses or radiological or nuclear materials may be stored at the institution where you work. Someone who wants to do harm may be interested in them.

Security is the work of man

"Yes, but security is not part of my work!" Security already receives the necessary attention at many organisations. Professionals provide the security; there are cameras, dogs, gates and high-tech systems.

But you also know what happens in practice. For example, a gate or a door remains open, 'since someone will be coming to deliver something any minute'.

You can think of so many systems and procedures, but everyone should participate. This is critical for the security of the organisation.

Security awareness means not giving malicious people a chance.

Alert people who use their eyes and ears are the most important element in the security of an organisation. More important than cameras, gates and any other measures and protocols.

Alert, observant people are 'security aware'.

Security awareness is not only the work of security professionals. People like you and your colleagues, who do not have 'security' as their main task, can also contribute to the security of your organisation. Simply by being observant. You help in reducing the risk that terrorists can prepare and conduct actions and help to prevent criminals, vandals and extremists from seizing their opportunity.

Security awareness is being alert to small things

In every organisation you can find examples of a key or access pass lying around, of materials/tools that are there for the taking or examples that show how easy it is to enter somewhere. People with malicious intentions take advantage of this.

You should also assume that someone who wants to do harm will make clever use of all the information on your organisation that can be found on the Internet. A terrorist, a criminal or an extremist is well-prepared. For example, by searching the Internet for corporate information about the company building and about personal information. Think about photos of a company outing, work

schedules or information about your private life. Internet sites such as Hyves, Facebook, Schoolbank and LinkedIn contain a wealth of information.

Preparation not only takes place behind the computer but also by having a look on site and taking pictures. He or she will try to get in, steal materials or tools and test the security. You might notice something about it and therefore encounter a Not Sure situation.

Security awareness is observing and taking action

You know your workplace well. Something out of the ordinary attracts attention.

Listen to your intuition that says: 'Wait a minute, something is not right here'.

Are you Not Sure? Take action. Fortunately it will often appear that nothing is wrong. Even then it is good to be Sure. If something turns out to be wrong, it is good not have to think in hindsight, 'If only I had reported that'.

Security awareness is having a healthy dose of curiosity when you see something out of the ordinary and taking action. Do not dismiss it too easily by thinking, 'I guess that's OK'.

Many people are hesitant about whether they should report something or not.

They feel uncomfortable about it or do not want to cause commotion.

That is understandable. But there is no such thing as reporting something for no purpose.

It is always useful to report something. After all, you want assurance that everything is OK.

Are you Not Sure? Always make sure that you turn it around to being Sure.

Terrorists, criminals, vandals and extremists have less of a chance with alert employees in the organisation.

Work assignment

Your organisation

How could your organisation be a target for a terrorist, criminal, extremist or a vandal? Imagine that someone has it in for your organisation. What could happen? What are the risks and threats for your organisation?

Try to look at your organisation through the eyes of a terrorist, criminal, extremist or a vandal. Is your organisation a potential target for a terrorist attack? Are there resources or information that would be of interest to them? Are there reasons to expect actions from extremists? What type of extremists (political, religious, animal rights or environmental)?

Think of at least five potential, concrete incidents of terrorism, criminality, extremism or vandalism in your organisation. Discuss with your colleagues all the potential risks, however small they may be.

- 1 _____
- 2 _____
- 3 _____
- 4 _____
- 5 _____



Work assignment

Your workplace

Mention a couple of practical situations at your workplace that you are Not Sure about. How might you have to deal with malicious people?

What do you notice of the activities of terrorists, criminals, vandals or extremists? It would be unusual to see someone lugging fifteen kilos of explosives. Think of simple situations. Someone who tries to enter somewhere or someone who tries to obtain information. Of course you do not know whether they may have malicious intentions, but you cannot rule it out.

Also describe how you would turn it around to being Sure.

1. What is the situation?
2. Why are you Not Sure?
3. How do you turn it around to being Sure?

An example:

1. What is the situation?

A man tries to get in without an access pass.

2. Why are you Not Sure?

I do not know him, he is unable to provide a good explanation of who he is coming to see and why he does not have an access pass.

3. How do you turn it around to being Sure?

I ask who he is coming to see, whether he has an appointment and what he is coming to do. If his answers make me Not Sure, I will call in security.

Examples for discussion

The following are a number of examples in which people acted attentively or should have acted attentively. The examples are largely based on true situations. Do you recognise situations that can also play a role in your organisation?

1. Credit card

Situation. A receptionist puts through a man's payment. He pays with a credit card.

What makes it Not Sure? The receptionist does not immediately trust the situation, though she cannot put a finger on why. The woman had a feeling that she should do an extra check. She followed her intuition.

How do you turn it around to being Sure? She asks the man for his passport. She then discovers that the information is incorrect. She indicates that she is unable to accept the man's credit card. The man runs away. Alert security employees go off in pursuit. The police are quickly on site and arrest the man. An international credit card fraud is uncovered and more arrests follow.

2. Baggage

Situation. At a hotel centrally located across from a large station, travellers regularly ask whether they can temporarily store their suitcases in the baggage room. The rule is that only guest baggage may be stored there. However, an employee makes an exception and accepts a suitcase from an older man.

What makes it Not Sure? Baggage from an unknown person may be a risk. The employee has not kept to the agreement.

How do you turn it around to being Sure? Just to make sure, she informs 'security'. Security checks the suitcase. A number of electrical wires are visible when the zipper is opened. The Explosives Ordnance Disposal Service is just about to perform an inspection. At that moment the owner of the suitcase returns and states that the suitcase contains one of his inventions, not a bomb.

3. Counterfeit 2 100 note

Situation. A receptionist receives payment from a customer. The man pays with a 100 euro note.

What makes it Not Sure? This man comes across as unreliable for one reason or another. He seems to be somewhat nervous. As common procedure, the employee checks the banknote for authenticity. The verification device indicates that the note may be counterfeit.

How do you turn it around to being Sure? The employee can tell the man (without immediately accusing him) what the verification device indicates. But she is hesitant to broach the subject. Moreover, it is busy and there is a long line of customers. She accepts the note. However, a further check later confirms her suspicion: the note is indeed counterfeit.

4. Bomb

Situation. A Spanish rail employee sees a long electric wire running from the track along the shrubs. He does not trust the situation. It is located at a remote spot, along the high-speed train line from Madrid to Seville. It is shortly after the bomb attack in Madrid (2004) and employees are extra alert to signals that could indicate terrorism.

What makes it Not Sure? A long electricity wire along the shrubs is out of place. His colleague tries to find an explanation and says that the wire is used to plant trees along it, but the employee still has his doubts.

How do you turn it around to being Sure? The man consults with his supervisor and informs the Guardia Civil. After some searching on site, the police find a plastic bag with a twelve-kilo bomb on the rails.

5. Microwave

Situation. An employee from a diamond dealer reports in the evening to company security. He bought a microwave during the day, forgot it, and is now coming to pick it up.

What makes it Not Sure? How often does someone forget to bring home a microwave?

How do you turn it around to being Sure? It is not turned around. Later, it is clear that security should have checked it out. However, the man was able to take the large cardboard box and walk out undisturbed. The microwave concealed 20 million guilders worth of diamonds. The robbery is spectacular news.

6. Loading up

Situation. At his building excavation, a building supervisor sees two men load materials into a lorry.

What makes it Not Sure? The building supervisor does not know the men. He has not given an order to load the materials.

How do you turn it around to being Sure? He addresses the men. They indicate that they have an order from the building supervisor (who they mention by name). Of course the building supervisor knows that there is something wrong. He continues to ask questions, to which the men get into their lorry and drive away. Theft has probably been prevented here.

7. Attaché case

Situation. At the check-in counter, a receptionist observes an unattended attaché case. None of the people on line responds when she asks who owns the attaché case.

What makes it Not Sure? It is customary for a passenger to take along an attaché case as hand luggage. It usually contains important, personal items. However, you cannot rule out in advance that it might contain explosives. Terrorists have been known to place them there before.

How do you turn it around to being Sure? The receptionist reports the unattended attaché case. A standard procedure follows. Experts establish that there is no danger.

8. Journalist

Situation. A scientific journalist is visiting and making observations in a laboratory where laboratory animals are used for research. He is extremely interested and would like to know a lot of details. That catches the attention of an employee from the laboratory.

What makes it Not Sure? The journalist is interested in matters that do not have a clear connection with his article.

How do you turn it around to being Sure? After some questioning, the journalist is unable to come up with a proper explanation. Cooperation with the journalist is suspended. It later appears that he is a member of an extremist action group against laboratory animal research.

9. Artificial fertilizer

Situation. An employee from an agrarian wholesale business receives an order for a certain type of artificial fertilizer. However, the customer refuses to be registered.

What makes it Not Sure? The customer lives on the other side of the country and makes the order at a time of the year that is unusual for fertilising the soil. Therefore, the employee does not completely trust the situation, certainly when the customer nervously responds when he is asked to register. The employee also knows that a component in artificial fertilizer (ammonium nitrate) can be used for making a bomb. Such an 'artificial fertilizer bomb' was used during the attacks at a discotheque on Bali and in Oklahoma. Therefore, as a private customer you can no longer buy certain types of artificial fertilizer without registering.

How do you turn it around to being Sure? The employee reports the order to the Home-made Explosives Reporting Centre. The police take over the case. The customer appears to have ordered artificial fertilizer from various wholesalers. Preparations for an attack may have been thwarted.

10. Hydrogen peroxide

Situation. Someone in Germany tries to buy a large quantity of hydrogen peroxide solution.

What makes it Not Sure? The customer would like hydrogen peroxide with a concentration that is unusually high for a private individual. This arouses suspicion from the seller because he knows that this concentration can be used as a raw material for explosives.

How do you turn it around to being Sure? The salesman reports it to the police. The same person had already purchased large quantities of hydrogen peroxide. The police already appear to be shadowing the buyer. He is a member of the 'Sauerland cell', a terrorist network. Ultimately the man is arrested in September 2007, along with other members of the cell.

11. Photo on the Internet

Situation. An operator of a plant that works with dangerous chemicals finds a photograph of the installation on the Internet.

What makes it Not Sure? The production installation may not be photographed. This has been stipulated for safety reasons. It is not desirable for the photo to appear on the Internet.

How do you turn it around to being Sure? The operator reports it to the security department. They investigate the origin of the photo and how it turned up on the Internet. After some detective work it appears that the photo was copied from a document and placed on the website. The webmaster immediately removes the photo upon request.

12. Photocopier CBRN

Situation. At a scientific institution, an employee sees that a foreign professor, who is working there temporarily, appears at the photocopier after working hours with reports in his hand.

What makes it Not Sure? It involves information on substances and applications that can be used as weapons. The professor makes an exceptionally large number of copies. When the employee comes to the professor's home, his suspicion that stacks of copies have been made is confirmed.

How do you turn it around to being Sure? The employee decides to report it to his supervisor. When the institute decides to ask the professor some critical questions, he returns to his homeland, where he is unreachable.

13. New colleague? CBRN

Situation. A receptionist in a laboratory sees a man walk by whom she does not know. The man introduces himself as the new janitor.

What makes it Not Sure? The receptionist is always informed about new colleagues but now knows nothing about this.

How do you turn it around to being Sure? She does not simply let the man in before making some inquiries. Ultimately it appears that the man indeed is a new colleague.

14. Revenge CBRN

Situation. After lunch in the company canteen it appears that the employees who have eaten there have all become ill. Spoiled food is suspected.

What makes it Not Sure? This does not sit well with the chef. He cannot imagine that spoiled food has come out of his kitchen.

How do you turn it around to being Sure? The chef reports his doubts. The company has an investigation carried out. It appears that employees have been poisoned with shigella dysenteriae. A frustrated employee stole it out of the lab to get even with the company. The theft had gone unnoticed at the lab.

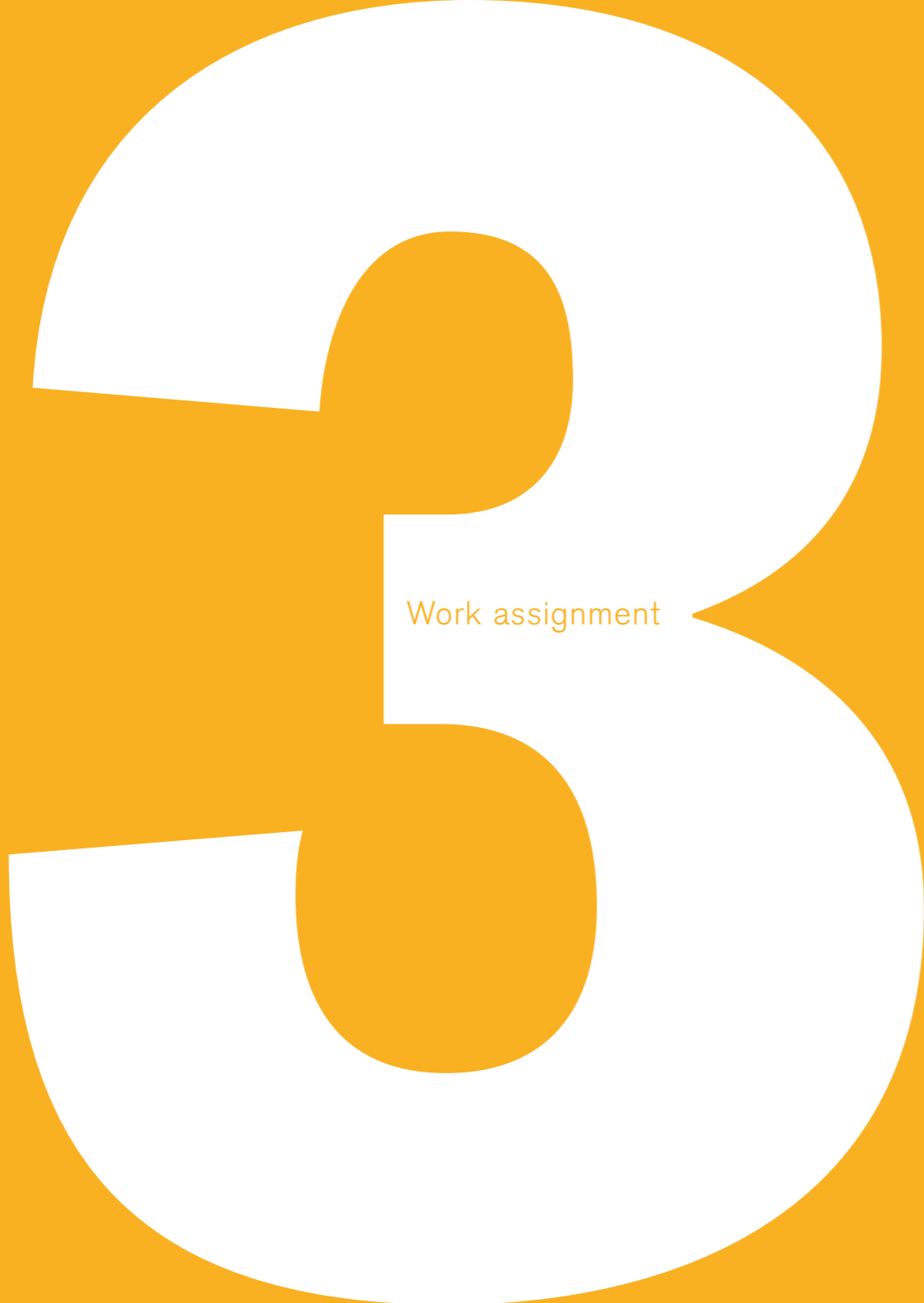
15. Delivery CBRN

Situation. An export company would like to deliver a large quantity of chemical substances to a foreign customer.

What makes it Not Sure? Chemical substances are involved, which can also be exploited to commit an attack.

How do you turn it around to being Sure? Inspectors from the Economic Investigation Service make inquiries. It appears that the export company does not know the recipient of the delivery. After the necessary intelligence work it appears that the customer did not have peaceful intentions for the chemical substances.

Do not make it too easy for people with malicious intentions.



Work assignment

What can you do?

Security awareness is keeping your eyes and ears open and taking action if you see something out of the ordinary.

You know your workplace well. You are the first to see if a situation is out of the ordinary. You immediately notice if someone behaves in an unusual way. Are you Not Sure of something? Try to figure out why you are Not Sure. Think about what you can do to alleviate that Not Sure feeling. For example, by calling someone to account or by having something checked. Report something to a colleague or supervisor. Indicate what makes you Not Sure.

It may be good that you hesitate in reporting something. During the workshop, discuss your hesitancy with your colleagues.

Have you ever reported something that you felt was not taken seriously enough? This can also be discussed with your colleagues.

With the knowledge that you now have, describe five concrete points of action that you would like to deal with. Consider things that you can do differently tomorrow. For example, how to deal with certain items or access to your organisation for strangers. Also come up with ideas on how you believe things should be arranged, even if you do not have the opportunity to implement them yourself. Your manager may be able to carry out the proposals within the organisation.

- 1 _____
- 2 _____
- 3 _____
- 4 _____
- 5 _____

Suggestions for alert action

The following are a number of suggestions for what you can do if you see something out of the ordinary.

Which tips can you use in your organisation?

People

You see someone walking around whom you do not know. It may be someone with malicious intentions, but that does not necessarily have to be the case, of course. That person may be looking for something. Simply ask: "Are you looking for someone? Can I help you?" That way, you can turn it from Not Sure to Sure for yourself. Security and customer-friendliness are closely related.

Check

There is nothing wrong with checking someone's story by simply asking. Do not immediately assume that 'it must be OK'. Ask in a friendly way: "Who are you coming to see?", "Who has given you that assignment?" "Where do you have to be exactly?" People who have a bona fide reason to be there will have no problem in providing you with an explanation. People who have malicious intentions will become nervous from these questions and will leave. Do not settle for the name of a colleague or director (that information is easy to find). Offer to accompany a visitor, if necessary.

Dealing with passes

Report a missing access pass as quickly as possible. You are Not Sure where it is now. Someone else could make improper use of it.

Lock up

Determine which cupboards, rooms and secure rooms at your workplace should be locked up. Always close them when you are finished with your work. Are cupboards or doors open when they should be closed? Check why they are open: is someone at work,

has someone forgotten to turn the key? Do not simply assume that 'it must be OK'. Report it if you cannot find an immediate explanation.

Gates

'The work should be able to continue' and therefore gates are sometimes left open. Do not take it for granted. Close gates or ask someone to stay there. Also take notice of people who are conspicuously interested in access and gates around a site. Keep an eye on them, assess the situation, ask what they are doing or report it.

Materials

Things that are out of the ordinary can be seen more easily at a tidy workplace. Stow away tools and materials. Make agreements that everyone can observe. Tidy up a workplace when finished, even if the work is to continue on another day. What you use as work material, someone else could use for an action.

On-line security

Internet criminals are increasingly skilful in hacking computer networks. Do not use the same password everywhere, do not save your password, do not hang a note with your password on your computer. Change your password regularly and do not give your password to a colleague. If you take work home with you, do not put it on a computer that is used (by children) to download and upload. Information can inadvertently appear on the Internet that way.

Make sure that you have good, legal software and a well-tested virus scanner and firewall. Make sure that updates are automatically retrieved and installed. Go to www.waarschuwingsdienst.nl for software checks and firewalls.

Personal information

It is easy to find a lot of information on social network sites, which applies to people with malicious intentions as well. Therefore, think twice about the personal information you would like to place on these sites. Protect your profile from strangers. Would you like to know what can be found about yourself (as well as colleagues and family members, for example) on the Internet? Use Google or wieowie.nl.

Information CBRN

Be aware of what certain information may be worth to someone who would like to do harm. A person who would like to conduct an action will be looking for information about your organisation. How does the security work? Where are certain items located? What are the schedules? What do the grounds look like? Who is present when and where? Where is a large stock of chemicals stored? Who are your suppliers or customers?

Talking CBRN

Everyone has talked about his or her work at some time at a party, at a sports field, at a conference, on Internet sites, perhaps even on TV. Still, it is good to realise what some information can mean for action groups, terrorists or criminals. You never know how

information reaches them. Know what you say to whom and think about how easily people can pass on the information.

Substances CBRN

Keep meticulous track of stocks of substances. File a report if certain resources are missing, even if they are residues or waste products.

Computer CBRN

Imagine that a laptop is stolen. What would actually be worse: the loss of the laptop or that certain information (for example, about your work, research or trials) might be out on the street? Be well aware that the information might be of value to someone with malicious intentions. Just to make sure, you should not only report the theft of a laptop but indicate the type of information that is on it as well.

Not Sure?

Always turn it around to being Sure.

