

Security
awareness,
how do you
deal with it
together
with your
employees.

It's your business to be sure
Management guide





It's your business to be sure

Workshop on security awareness for companies and institutions

This guide for supervisory staff and security managers is part of the materials for the workshop, 'It's your business to be sure.'

A DVD and a workbook are also included.

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

It was commissioned by the National Coordinator for Counterterrorism (NCTb).

© NCTb 2009



Introduction

The workshop 'It's your business to be sure' gives you a positive approach to bringing security awareness to the attention of your employees.

You will clearly see why this workshop was developed by the National Coordinator for Counterterrorism (NCTb). Alert employees are indispensable in nipping (the preparation of) potential terrorist activities in the bud. But security awareness provides even more. It also helps in preventing criminal activities, vandalism and extremist actions.

Your organisation benefits in various ways. Security awareness prevents disruption of business processes, saves money, is in the best interest of company continuity, helps to avert a tarnished image and contributes to customer friendliness and service.

This workshop is a starting point. You and your staff adapt it to your specific work situation by interpreting security awareness in a way that is relevant for your organisation. As supervisor and workshop manager, you play a critical role.

With this guide, you are well-prepared in thirty minutes to go through the workshop 'It's your business to be sure' with a team. With your commitment and enthusiasm, security awareness can develop constructively, which is in the best interest of the security of your company, your organisation and each individual employee.

I wish you a lot of success in giving the workshop.

Erik Akerboom

National Coordinator for Counterterrorism (NCTb)

Contents

1. What is the purpose of the workshop 'It's your business to be sure'?
2. How do you achieve security awareness?
3. What is your role in the workshop?
4. Explanation of the three parts of the film and accompanying work assignments
5. Management information security awareness

What is the purpose of the workshop 'It's your business to be sure'?

A frequently asked question from employees (and perhaps yourself) is:
Why should we be on the alert if we already have security professionals,
protocols, gates, cameras, access passes, etc.?

Experience has shown that alert employees are indispensable. Their eyes and ears are the most important elements for the security of an organisation. With a relatively small investment, companies can profit greatly from the security awareness of its employees.

'It's your business to be sure' is not about technology and protocols, but about the mindset of your employees. During the workshop, you will enhance the security awareness of your employees. In other words, they will become aware that:

- the company or the institution may be struck by the activities of malicious people;
- a deviant work situation ('something is not quite right') may be caused by the activities of malicious people;
- taking action can make a difference.

When we refer to malicious people during the workshop, we usually mean people who are engaged in terrorism, criminality, vandalism and extremism.

Terrorism is a realistic threat. Even if the risk of a terrorist attack is small, it cannot be ruled out. Consider, for example, our presence abroad or statements from certain politicians that can provide a reason for making the Netherlands a target. Attacks in Madrid and London show that public transportation is vulnerable to attacks and that other targets are conceivable. The NCTb has involved various business sectors in its Counterterrorism Alert System so that quick measures can be

taken in the event of a heightened threat. For more information go to www.nctb.nl. Moreover, some organisations are not a target in themselves, but can provide resources for a terrorist. Examples include organisations that have chemical, biological, radiological and/or nuclear knowledge and resources in house.

Extremism can come from various directions, from people with right-wing extremist sympathies, religious factions, such as Muslim extremists, or (violent) animal rights extremists. In all cases, small factions that use violence in demanding attention for their views are involved.

Criminality can take many forms, ranging from theft of data and information to sabotage, blackmail and espionage. The Monitor Criminaliteit Bedrijfsleven 2008 [Monitor Crime in the Business Sector 2008], which limits itself to five sectors in the Netherlands, estimates the damage from criminality at close to EUR 700 million.

Security awareness helps to prevent terrorists, criminals, vandals and extremists from being able to strike at your company or institution or being able to strike with resources obtained from your company or institution.

How do you achieve security awareness?

During the workshop 'It's your business to be sure', your employees receive the simple but important message: Not Sure? Turn it around to being Sure.

Security awareness means being alert to situations that are out of the ordinary. Whether it is a person who enters your company for equipment or resources, or for information, it always involves a situation in which an employee has a sneaking suspicion that something is not quite right.

That intuitive feeling is very important. Your employees learn to recognise such a situation as Not Sure. They also learn to turn it around to being Sure.

Fortunately, it will often turn out that nothing was actually out of the ordinary. But then, too, it is good to be Sure about it.

Workshop Programme

The programme takes approximately 1-1^{1/2} hours. The film on the enclosed DVD is the basis for the workshop.

The film consists of three parts that you watch with your employees. At the end of each part of the film you hold a discussion with your employees based on an assignment that can be found in the employee workbook. The ideal group size for the discussion is a maximum of 10.

Part 1 of the film starts with general information about security awareness. What makes your organisation a target for terrorists, criminals, extremists? What risks play a role in your organisation?

Part 2 of the film shows what an employee might personally notice from (the preparation of) the activities of a terrorist, a (cyber) criminal or an extremist. Which Not Sure situations can be prevented?

Part 3 of the film focuses on the action perspective. What should you do if a situation is Not Sure? How do employees turn it around to being Sure? You then work together on drawing up concrete action items.

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.

What is your role in the workshop?

Particularly important are the discussions with your employees after each film part, based on the assignments in the workbook. They help you to apply the general information in the film to the specific situation in your organisation. Make sure that you also consider the cultural aspects in your organisation. For example, are you accustomed to calling each other to account for undesirable behaviour?

Ask your employees for a reaction after each part of the film. Does that also apply to us? What could also play a role in our organisation? How easy is it to enter our company? What situations do we recognise? What could we do about it? As the supervisor, make sure that the discussion is constructive. Have your employees think and relate as much as possible themselves. Only come up with additional questions and/or examples if the discussion stagnates.

What is the best way to prepare yourself for giving the workshop? Watch the film again, if possible. In any case, think about the assignments in the workbook. The next explanation will clarify the purpose of each part of the film and the accompanying assignment.

Each assignment also has a practical list with points of reference to talk about in the joint discussion.

Explanation of the three parts of the film and accompanying work assignments

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

Explanation of part 1

Content of the film. General information about security awareness. Three experts explain. The National Coordinator of Counterterrorism Erik Akerboom briefly sheds some light on the theme of terrorism. Technical University Professor Ben Ale talks about various types of extremism. Jos Meekel, director of a private company detective agency, provides information about criminality at companies. A Spanish railway worker who prevented a new drama in Madrid, thanks to his alertness several weeks after the bomb attacks also has a role in the film.

Learning objective. Your employees become aware that their (and your) organisation may be a target for terrorists, criminals and/or extremists.

It could happen to you too! The risk that your organisation will be affected may be small, but no one can rule it out.

Discuss with your colleagues after part 1 of the film.

How could our organisation be a target for terrorists, criminals and extremists? See assignment 1 in the workbook. The question is, what could happen to the organisation (talk in the 'we' form; part 2 of the film is about the personal level).

Give employees the opportunity to respond spontaneously. If necessary, use the list below to keep the discussion going. What could happen in your organisation?

- Theft of data.

- Theft of an employee's personal property (e.g. wallet).
- Theft of information.
- Industrial espionage/loss of a patent.
- Hacking of a computer network.
- Vandalism and graffiti/sabotage/destruction of administrative work.
- Intimidation or threat of personnel and family.
- Blackmail.
- An attack/arson.
- An action designed to get media attention.
- ..
- ..
- Have employees complete on their own.

CBRN

- Theft of radiological materials.
- Theft of chemicals.
- Theft of viruses.
- Theft of bacteriological materials.
- Theft of (research) equipment or instruments (or knowledge about it).
- Theft of research data.
- Blackmail of (family of) investigator.
- ..
- ..
- Have employees complete on their own.

Something to talk about. If your company is affiliated with the

Counterterrorism Alert System (ATb) of the NCTb, explain why to your employees. If you work at a CBRN institution, explain why there is contact between your organisation and the NCTb within the framework of improving resilience.

If necessary, make inquiries with the contact for security in your organisation.

Explanation of part 2

Content of the film. We make the acquaintance of six employees from different companies. They have a discussion that is led by the presenter and a trainer from the Police Academy.

Learning objective. Your employees learn to recognise a Not Sure situation in their own work environment and link it to a potential action from someone who wishes to do harm.

Discuss with your colleagues after part 2 of the film. Which Not Sure situations do they recognise in their daily workplace? See assignment 2 in the workbook. Try to have employees describe something similar to what is described in the workbook in three parts:

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

Initiate the discussion. The purpose is not for every employee to take notes on individual situations; make sure that experiences are exchanged. Have employees come up with suggestions for one another and describe situations together.

If you wish, you could first have them read the examples of employees who took action through alert behaviour. They can be found in the workbook on page 14, 'Examples for discussion'.

Something to talk about.

- How easy is it to enter your workplace? How does a person behave? Where? At what point in time? Might that be deviant behaviour?
- Is there something unusual about a person's curiosity (asking for information, taking photos, taking notes)?
- If you see someone walking around at your workplace whom you do not know, do you address this person?
- How does someone react when called to account?
- Do you keep talking when someone is very interested in your work and tries to obtain information? What can someone do with certain information if he or she wants to do harm?
- What happens, for example, if an access pass, a key or industrial clothing is stolen? What could someone do with them?
- Someone tries to find out personal information about certain employees. What do you do?
- How do you know if someone is actually who he says he is?
- How useful is certain information for someone who wants to do harm?
- How is security sometimes at odds with the continuity/speed of work processes?
- What is deviant behaviour? It is important to talk with your employees about preconceptions, for example, based on a person's external features. Someone who dresses differently or conspicuously does not necessarily exhibit deviant behaviour.
- Do you have a situation that you would like to bring up yourself?

Explanation of part 3

Content of the film. The six employees in the film indicate how they now view security awareness after the discussion.

This part of the film contains various recommendations.

The trainer from the Police Academy summarises what you and your colleagues can do for security awareness.

Learning objective. Have employees see how they can take simple measures to make a difference in security awareness.

Discuss with your colleagues after part 3 of the film. Talk about how you turn a Not Sure situation around to being Sure. See assignment 3 in the workbook. To start, discuss with your employees the best place to report a Not Sure situation. Indicate which internal department of the organisation they should go to. The police are the logical contact point for an acute threat. In some situations it is sufficient to talk to a colleague or supervisor. It is important to review with your employees: What do I report where? Make agreements about this. If your organisation has still not agreed on a procedure for reporting Not Sure situations, broach the subject with your contact person for security.

Moreover, have employees think about the possible points for improvement for the security of the organisation. What can improve tomorrow, now that you have thought about security? Think about simple matters such as: from now on, we will visibly wear a pass and we will call each other to task about that. More suggestions appear in the workbook on page 20, 'Suggestions for alert action'.

It is important to have the employees come up with ideas themselves.

As the workshop leader, collect all suggestions and set priorities: What are quick wins and which ideas require more time? Also indicate, if necessary, the points you can take up immediately with your employees and those that must be presented to the management team or the management board.

The jointly prepared list with concrete actions offers a basis for discussing security awareness again after some time. Since it is necessary, of course, to keep the subject on the agenda. Discuss the results with your management team.

Management information security awareness

The workshop 'It's your business to be sure' is a starting point. To keep security awareness in the limelight, it will have to be implemented in the company's operations, coordinated to your employees and geared to activities within your company.

To assure permanent security awareness, it is important to keep the subject under employee attention on a regular basis, for example, during work planning. Your commitment is also needed.

To start, a positive attitude is needed from management, from high to low in the organisation. An employee who reports a Not Sure situation must be able to count on confirmation that he or she took the proper action, by receiving a compliment, a reward and/or feedback about what was done with the report. It's better to be safe than sorry.

Besides, nothing is more demotivating for an employee than having his or her report received with indifference or, even worse, made to look foolish. If management does not emphasise the benefit of security awareness, there will be no security awareness among employees.

This workshop is focused on security awareness within your company.

It is important that your employees know where and to whom they can report a Not Sure situation. Of course your organisation should have internal agreements from the start. It is important to notify your employees about internal procedures for reports and about the telephone numbers that should be used for this. If necessary, use simple but effective means of communication (for example, a card,

key cord, a placemat in the canteen, etc.) to bring and keep this under the attention of your employees.

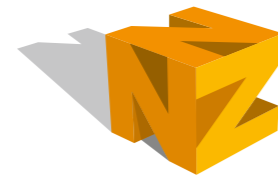
In practice, feedback appears to be very important for employees to be permanently willing to be security aware.

'We never heard about it again', is an often-heard complaint from people who reported something at one time. However, it is not always possible to provide feedback. But information always comes to the right specialist police departments, where certain information can provide a piece of the puzzle in a larger whole. That is not always immediately clear. In some cases, in the interests of a pending investigation, the police are wary of making any statements about what has been done with certain information. Nevertheless, it is good to seek opportunities to give attention to an employee. Let the employee know that he or she took the proper action, indicate why actions were or were not taken as a result of the report and let the employee know what phase the investigation is in, if applicable.

Ultimately your organisation can also use reports as an indication of the degree of security awareness among the employees.

By registering the results, you can evaluate the present situation within your company. This evaluation can then apply as a starting point for placing a specific topic of security awareness on the agenda.

Moreover, with the list of concrete action items you made with Assignment 3 during the workshop, you have a point of reference to return to the subject of security awareness on a regular basis. Which action items have already been implemented, which action items are still open and what happens with them?



Want to know more?

Finally, we wish you a lot of success in giving the workshop 'It's your business to be sure'. We trust that you now have a positive approach for bringing security awareness to the attention of your employees.

Do you have any questions as a result of the workshop materials or general questions about security awareness? For more information you can contact the security manager in your own organisation. You can find more information about counterterrorism at www.nctb.nl.

Not Sure?

Always turn it around to being Sure.

