

S security incidents: definition and analysis

Purpose:

Learning how to recognise and respond to security incidents.

What is a security incident?

Put simply, a security incident can be defined as **any fact or event which you think could affect your personal or organizational security.**

Security incidents can be incidental or provoked intentionally or unintentionally.

Examples of security incidents could include seeing the same, suspicious vehicle parked outside your office or home over a number of days; the telephone ringing at night with nobody at the other end; somebody asking questions about you in a nearby town or village, a break-in to your house, etc.

But not everything you notice will constitute a security incident. You should therefore **register** it, by writing it down, and then **analyse** it, ideally with colleagues, to establish if it really could affect your security. At this point you can **react** to the incident. The sequence of events is as follows:

You notice something ⇒ you realise it might be a security incident ⇒ you register it / share it ⇒ you analyse it ⇒ you establish that it is a security incident ⇒ you react appropriately.

If the matter is pressing, this sequence should still take place, just much more quickly than usual to avoid delay (see below).

How to distinguish between security incidents and threats:

If you are waiting for a bus and somebody standing next to you threatens you because of your work, this - apart from being a threat - constitutes a security incident. But if you discover that your office is being watched by a police car from the opposite side of the street, or your mobile phone is stolen, these are security incidents, but not necessarily threats. However, while incidental and/or unintentional security incidents (i.e. to be in the crowd and/or to have lost one's keys) can clearly be distinguished from the threats, remember that intentionally provoked security incidents have got an

objective and not necessarily the same as threats (see Chapter 1). The minimum objective of an intentionally provoked incident is to gather information about the defenders regardless if it is going to be used against them.

Establishing a clear distinction is important at least for the mental health of the defenders.

**All threats are security incidents, but
not all security incidents are threats.**

Why are security incidents so important?

Security incidents are crucial in handling your security because **they provide vital information about the impact your work is having, and about possible action which may be planned or carried out against you.** Likewise, such incidents allow you to change your behaviour or activities and avoid places which could be dangerous, or more dangerous than normal. Security incidents can therefore be seen as indicators of the local security situation. If you couldn't detect such changes it would be difficult to take appropriate and timely action to stay safe.

For instance, you may realize that you are under surveillance after noticing several security incidents: now you can take action about surveillance.

**Security incidents represent "the minimum unit" of
security measurement and indicates the
resistance/pressure on your work.
Do not let them go unnoticed!**

When and how do you notice security incidents?

This depends on how obvious the incident is. If it could potentially go unnoticed, your ability to recognise it depends on your security training and experience and your level of awareness.

**The greater your awareness and training,
the fewer incidents will escape your attention.**

Security incidents are sometimes overlooked or briefly noticed and then brushed to one side, or people sometimes overreact to what they perceive as security incidents.

Why might a security incident go unnoticed?

An example:

A defender experiences a security incident, but the organisation s/he works with does not react at all. This could be because...

- the defender isn't aware that a security incident took place
- the defender is aware of it but dismisses it as unimportant

- the defender hasn't informed the organisation (s/he forgot, doesn't believe it necessary, or decide to keep quiet because it happened because of a mistake on their part)
- the organisation, having done a team evaluation of the incident after the defender registered it in the incident book, does not judge action necessary

Why do people sometimes overreact to security incidents?

For example:

A colleague might be constantly telling stories about some security incident or other, but on further examination they prove not to have substance or merit the definition. The actual security incident in this instance is the fact that your colleague has a problem which makes him/her see non-existent security incidents. S/he might be feeling very afraid, or suffering from stress, and should be offered support to resolve the problem.

Do not forget that that security incidents are overlooked or dismissed to often: be careful about this!

Dealing with security incidents

There are many ways to react rapidly to a security incident. The following steps take into account the moment and the type of reaction from the moment the security incident has been reported, while it is happening and after it has happened.

Three basic steps to deal with security incidents:

- 1 • **Register them.** All security incidents noticed by a defender must be registered, either in a simple, personal notebook or one accessible to the whole group.
- 2 • **Analyse them.** All registered security incidents should be properly analysed straight away or on a regular basis. It is better to analyse them as a team rather than individually because this minimises the risk of missing something. Someone should be put in charge of making sure this is done.

Decisions must also be made about whether or not to maintain confidentiality about specific incidents (such as threats). Is it ethical and realistic to keep a threat hidden from colleagues and other people you work with? No single rule applies to every situation, but it is often best to be as open as possible in terms of sharing information and addressing logistical concerns, as well as fears.

- 3 • **React to them.** Given that security incidents give feedback on the impact of your work, they could lead to the following:
 - Reaction to the incident itself;
 - **Feedback**, in security terms, about how you work, your work **plans** or your work **strategy**. **For example:**

Example

of an incident which provides **feedback** on working more securely:

For the third time somebody from your organisation has had problems passing through a police checkpoint because they frequently forget to carry the necessary documents. You therefore decide to compile a checklist which all staff members must consult before leaving the city. You might also change the route for these types of journeys.

Example

of an incident which providing feedback on how you **plan** for security:

At the same police checkpoint, you are detained for half an hour and told that your work is poorly regarded. Thinly veiled threats are made. When you ask for an explanation at police headquarters, the scene is repeated. You call a team meeting to revise your work plans, because it seems clear that changes have to be made in order to continue working. You then plan a series of meetings with Interior Ministry civil servants so that checkpoint police is instructed to refrain from harassing you, change some aspects of your plans and arrange weekly meetings to monitor the situation.

Example

of an incident which provides feedback for your security **strategy**:

When you start work as defenders in a new area, you immediately receive death threats and one of your colleagues is physically assaulted. You did not anticipate such opposition to your work, nor provide for it in your global strategy. You will therefore have to change your strategy in order to develop tolerance of your work locally and deter further attacks and threats. To do this you may have to suspend your work for a while, withdraw from the area and reconsider the entire project.

Reacting *urgently* to a security incident

There are many ways of responding promptly to a security incident. The following steps have been formulated in terms of when and how to react from the moment a security incident is reported, while it is happening, and after it is over.

Step 1: Reporting the incident.

- ◆ What is happening/has happened (try to focus on the actual facts)?
- ◆ Where and when did it take place?
- ◆ Who was involved (if it can be established)?
- ◆ Was there any injury or damage to individuals or property?

Step 2. Decide when to react. There are three possibilities:

- ◆ An **immediate reaction** is required to attend to people with injuries or stop/prevent an attack.
- ◆ A **rapid reaction** (in the next few hours or even days) is necessary to prevent possible new security incidents from arising (the incident is over).
- ◆ A **follow up action** (in several days, weeks or even months): if the situation has stabilised, an immediate or rapid reaction may not be necessary. However, any security incident that requires an immediate or rapid reaction must be followed by a follow-up action in order to restore or review your working environment.

Step 3. Decide how to react and what your objectives are.

- ◆ If the reaction has to be immediate, the objectives are clear: attend to injuries and/or prevent another attack.
- ◆ If the reaction has to be quick, the objectives will be established by the person in charge or a crisis team (or similar) and **focus on restoring the necessary security for those affected by the incident.**

Subsequent actions/reactions will take place through the organisation's normal decision-making channels, with the objective of restoring a safe working environment externally, as well as re-establishing internal organisational procedures and improving subsequent reactions to security incidents.

Any reaction also has to take into account the security and protection of other people or organisations or institutions with which you have a working relationship.

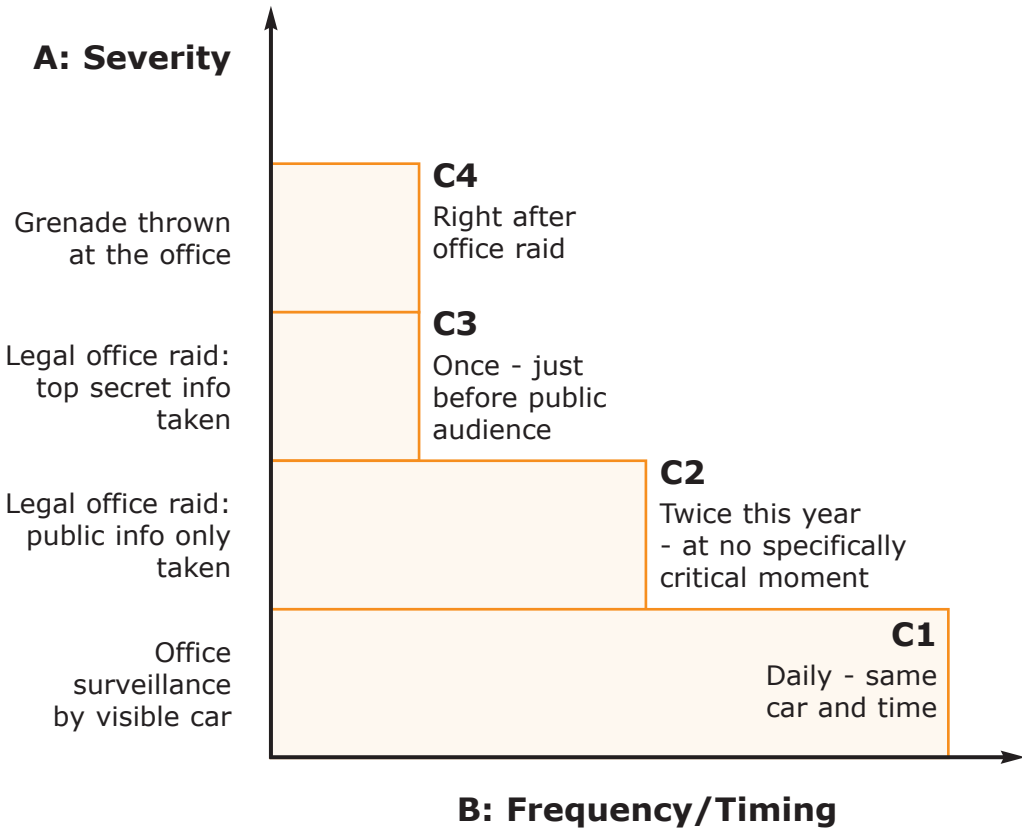
Establish your objectives before taking action.

Prompt action is important, but knowing why you are taking action is more important. By first establishing what you want to achieve (objectives), you can decide how to achieve it (course of action).

For instance:7

If a defenders' group receives news that one of their colleagues has not arrived at her destination in a town, they may start a reaction by calling a hospital and calling their contacts in other NGOs and a nearby UN Office and police. But before starting those calls, it is very important to establish what you want to achieve and what you are going to say. Otherwise you may generate unnecessary alarm (imagine that the defender was just delayed because they missed a bus and forgot to call the office) or a reaction opposite to the one intended.

Logging security incidents (and threats) helps analysing them from the perspective of anticipating them at specific moments. For example, if the log reports security incidents around pre-electoral periods, it is likely that they will occur again at the following pre-electoral period. The log can also help assessing the likeness of an action against the HRD by the potential aggressor or, in case of security incidents due to the carelessness of HRD, it will contribute to assess how security is being managed by HRD themselves.



C: Probability of imminent more severe action against HRD from Potential Aggressor

C1: VERY LOW (A1: office surveillance by visible car + B1: daily same car and time)

C2: LOW: (A2: legal office raid: public information only taken + B2: twice this year at no specifically critical moment)

C3: High: (A3: legal office raid: top secret information taken (top secret witnesses names taken) + B3: Once just before public audience)

C4: Very high : (A4: grenade thrown at the office + B4: Right after office raid C3)

(...)

Summary

A security incident is any fact or event which you think could affect your personal or organizational security.

Security incidents can be incidental or provoked intentionally or unintentionally.

Security incidents measure security and the impact of defenders' work on others' interests.

All defenders have security incidents. The contrary would imply that:

- The impact of the defenders' work is insignificant either because the work is not carried out properly and/or because nobody's interest is being affected. In other words: no one is interested in them.
- The potential aggressor has already got all information about the defenders and doesn't need to bother: the defenders were not able to spot the provoked security incidents then (surveillance, information gathering...).

A security incident is not a threat, however it needs attention.

Three steps to deal with security incidents:

- 1 • Register them
- 2 • Analyse them
- 3 • React to them

