"Co Funded by The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union"

PSOPHIA GUIDELINES FOR CRITICAL INFRASTRUCTURE (CI) EMPLOYEES

WP4.1 (GI)

Project reference number : HOME/2012/CIPS/AG/4000003789
Project title : *Increasing Security Awareness of Critical Infrastructure OPerators introducing Intelligence Techniques and focusing on Psycho-social and Human factors- PSOPHIA*
Project duration : 18 months **Start Day:** 01.04.2013
Funding Scheme: CIPS 2012
Author: Olivia Gualda
Responsible of the document: 
Due date of the deliverable: 01.09.2014

PSOPHIA GUIDELINES FOR CI EMPLOYEES

'The project has being funded by the EU under the CIPS Programme (EC DG Home) The Commission is not responsible for any use that may be made of the information contained therein, the sole responsibility lies with the authors.'

Table of Contents

Towards a Culture of Personnel Security 1

I. Introduction 1

Deliberate actions 2

Unintended actions 4

II. Methods 5

A. Gathering Information – Passive Ways 5

B. Gathering Information – Direct Approach 6

C. Cover Stories – Dispersed Approach (Establishing the relationship) 8

III. Principles 9

IV. Recommendations 10

PSOPHIA

Increasing Security Awareness of Critical Infrastructure OPerators introducing Intelligence Techniques and focusing on Psycho-social and Human factors

Towards a Culture of Personnel Security

These Guidelines respond to PSOPHIA's main goal of increasing security awareness of Critical Infrastructure (CI) security operators, with a special focus on the human vulnerabilities of CI personnel that can jeopardise the general security of infrastructures, people and assets. The Guidelines are a result of previous research and activities in the project, where the need of paying better attention to psycho-social factors and specially those areas where personal, social and working lives interact have been stated, as well as the field for improvement towards a more accomplished personnel security culture and conduct.

In the present times, not only systems, information, networks and services, but also people need to be reliable if they are part of the staff or they are temporary workers, contractors, etc. of a CI. Only an approach that takes due account of all aspects of security and nature of risks can provide effective security.

Each person is an important actor for ensuring security. CI employees, as appropriate to their roles, should be aware of the relevant security risks related to their own personal vulnerabilities, as well as the existing preventive measures and therefore, assume responsibility and take steps to enhance the security of their organisations.

Furthermore, the promotion of a culture of personnel security requires leadership, management commitment and extensive participation and should result in a heightened priority for security planning and management, as well as an increased awareness of the need for security among all staff. Personnel Security issues should be topics of concern and responsibility at all levels of business and for all participants.

PSOPHIA Guidelines constitute a foundation for working towards a holistic concept of security throughout CI, where the human factor is not left behind or given less importance. They propose that all participants adopt secure habits and behaviours inside and outside the workplace and always consider and assess potential risks before acting in everyday life.

These Guidelines aim to provide a useful complement to existing (personnel) security procedures in CI and shed light into the consideration of the insider threat as part of security regimes, as well as the risks of potential exploitation of the staff's personal vulnerabilities for malicious purposes.

I. Introduction

Most of the times, we tend to think that we are ordinary people, unimportant, and with nothing to hide. Therefore, we do not realise that our personal vulnerabilities, behaviour and mistakes can be the only or easiest gate for criminals and terrorists to access and damage our organisation…

Moreover, damages caused to organisations like yours can result in impactful incidents, catastrophes, massive loss of life, and great economic damage.

Why? Because your organisation provides an essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities. Attacks against Critical Infrastructures can cause hazards such as electricity supply cuts, contamination of drinking water, floods or… even, the destruction of an entire country's nuclear programme.

That was the case of the computer worm STUXNET *that ruined Iran's nuclear production capabilities. The only way it got into the facilities was through a contractor working in the plant, the Stuxnet attack exploited his human vulnerability of natural curiosity by simply dropping a bunch of USB flash drives around the facility*, one of which ended later plugged to the contractor's PC.

This is just one of the examples that prove that human factors are so important in security…

You are a key element to the security of your organisation.

PSOPHIA Guidelines for Critical Infrastructure employees help you understand how you can contribute to the security of your organisation, resisting and neutralising threats originated by human factors. First, pay attention of these categories of threats and attackers:

Deliberate actions

From the human perspective, **intentioned** attacks can be performed by **any** person who gets access to assets and premises.

But why should anyone want to damage your organisation?

The majority of attacks from **INSIDERS** are motivated by employee's disgruntlement, radicalised beliefs, terrorism, or financial greed. These motivations don't need to be there from the start, the change in behaviour can happen at any time during the employees' working life.

The insider threat can come from '**anyone**' with access to the organisation, whether for:

A few hours	A day
A month	Every working day

Therefore, a threat can emanate from:

A permanent member of staff	A contractor
A consultant	Temporary staff

And be aware! They can get access to traditional office or site settings but also via a remote means of working. (PLC, IED, hackers to operating systems…)

INSIDERS

According to the British CPNI: An **Insider** is defined as 'a person who exploits, or has the **intention** to exploit, their legitimate access to an organisation's assets for unauthorised purposes. The insider threat can come from '**anyone**' with access to the organisation'. Recognising this is a very important step for the management but also for the employees.

An insider can:

Disclose sensitive information;	Corrupt processes
Facilitate third party access to an organisation's assets	Perform physical sabotage; and electronic or IT sabotage

Studies show the most frequent types of insider activity to be the disclosure of sensitive information (47%) and process corruption (42%).[1]

Detecting insiders with malicious intentions is hard, but you can contribute, firstly if you:

- Do not assume it's not going to happen to you or your organisation, as this is a common blunder. **Don't suffer from NIMO! ('not in my organisation')**
- Do not assume you can always trust people just because you are familiar with them or because they are in senior positions

Your security and HR managers are in charge of spotting related indicators but:

- Do not be blind to what you see

U.S. Army Major Nidal Hasan expressed his radicalised and violent beliefs for years, openly justifying suicide bombers, and showing devotion to Osama bin Laden, and Sharia law over the U.S. Constitution. He did it in front of colleagues and supervisors In November 2009, he shot a group of soldiers, killing thirteen and wounding twenty-nine in Fort Hood, Texas, on the US largest military bases.

Many reasons may stop people to report red flags, and indicators of insider security problems are systematically underreported.

- Find what channels your organisation offers for discreet reporting and report changes, and suspicious or alarming behaviours.

[1] CPNI: Insider data collection study - report of main findings (PDF, 407.22 KB) - See more at: http://www.cpni.gov.uk/advice/Personnel-security1/Insider-threats/#sthash.sQAv07As.dpuf

Insiders are often linked with motivation, **intention**, capability and opportunity

Insiders might NOT have the intention to harm or attack, but there is a danger that they might be **recruited by** or **become sympathetic** to a malicious outsider person or group.

Unintended actions

There are

TWO WAYS of recruiting an employee such as you, two ways of getting a person to do what malicious people want: **COERCION** and **DECEPTION**

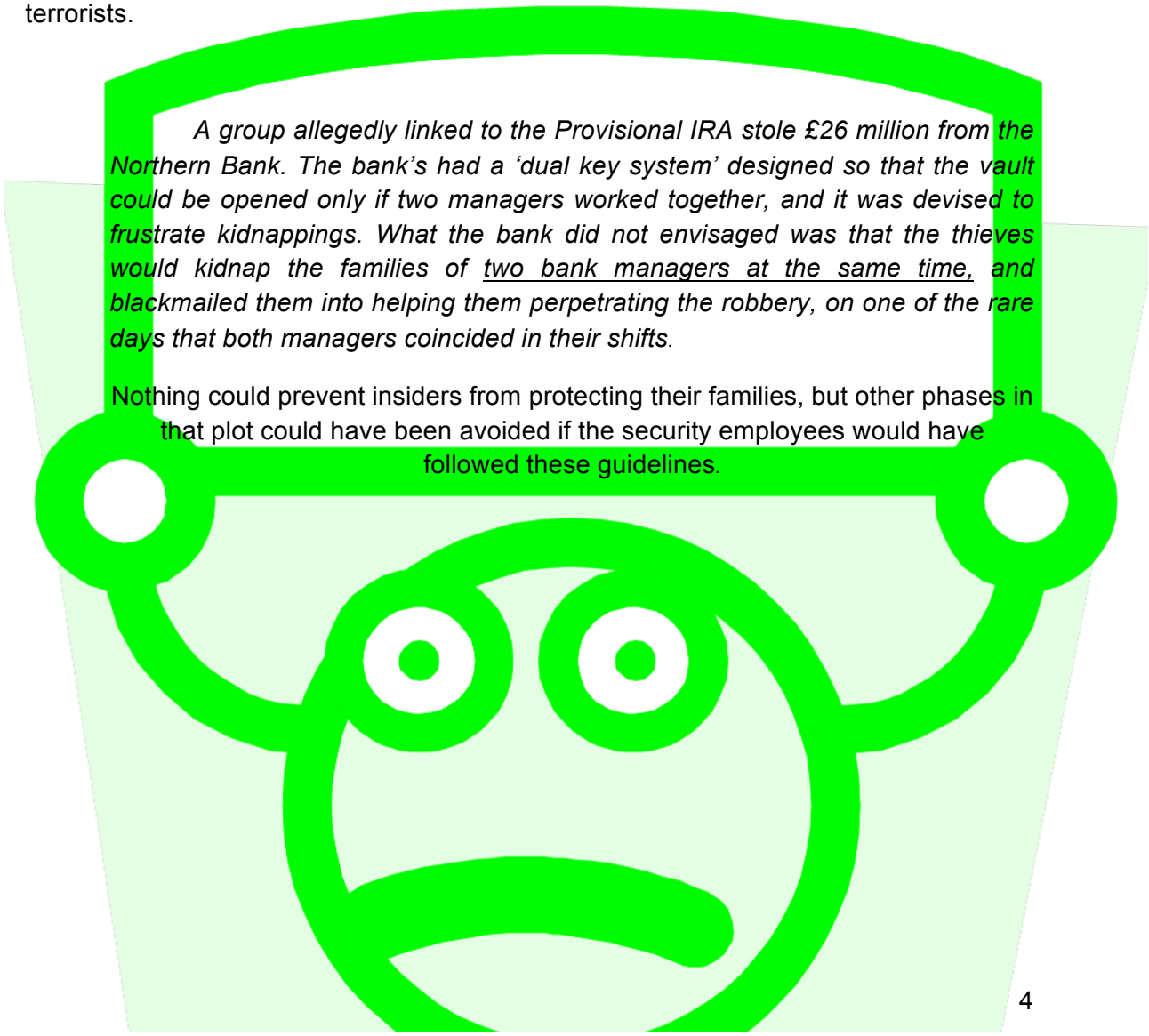
1. Coercion

Coercion is a strong tool that may put employees in a position they don't desire to be, and may be the key to recruit otherwise highly reliable insiders at an organisation.

Blackmailing and threatening are long standing methods used by criminals and terrorists.

A group allegedly linked to the Provisional IRA stole £26 million from the Northern Bank. The bank's had a 'dual key system' designed so that the vault could be opened only if two managers worked together, and it was devised to frustrate kidnappings. What the bank did not envisaged was that the thieves would kidnap the families of two bank managers at the same time, and blackmailed them into helping them perpetrating the robbery, on one of the rare days that both managers coincided in their shifts.

Nothing could prevent insiders from protecting their families, but other phases in that plot could have been avoided if the security employees would have followed these guidelines.



2. Deception

Deception

PSOPHIA project focusses on employees who may be **unconsciously** used as attack facilitators, people who may be manipulated and deceived for malicious purposes.

The techniques that spies have always used to gather information or for infiltration, those used in marketing campaigns to persuade people, or the arts of seduction as well as all aspects related to Social Engineering exploit, not only human vulnerabilities but also natural human tendencies and characteristics, in order to take advantage of them in their favour.

The art of manipulation involves two aspects:

- concealing real intentions and

- knowing the vulnerabilities of the victim well enough

All forms of influence that seek control over people can appear in different interpersonal and social relations. **And take good notice**: They are used **inside** and **OUTSIDE** your organisation… in all backgrounds: private, public, family, corporate, educational, institutional, mediatic, religious and politic.

If the Critical Infrastructure where you work becomes a target for terrorists or criminals, you could be used to get information, access and cause damage. So, first, they will try to gather as much information the can about you.

Remember: the more information people have about you, the easiest to use it against you.

"We know who you are. We know everything about you. We know who your family is. We know everything about them and we're here about your job." [2] Anatomy of a Bank Robbery, the Northern Bank Case

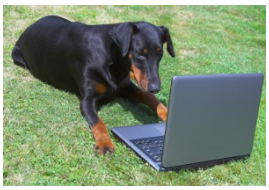
II. Methods

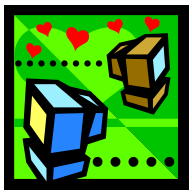
A. Gathering Information – Passive Ways

Before approaching people directly, there are many **passive ways of Gathering Information** (and ways you might be exposing yourself and your family):

- Social Media (Facebook, Linked In…)

[2] http://irishaires.blogspot.com.es/2005/01/011205-anatomy-of-bank-robbery.html





- Personal/Company website
- Online (Dating sites, Fora…)
- Email
- Other Internet tools like Google Street View
- Spotting people at tradeshows, symposia, conferences
- Surveillance, monitoring, study of habits and routines…

Studies have also shown how many details on the organisations' systems, services and people, that can help designing a Social Engineering attack or other plots, are published and available in the company website, tender documents, specialised articles or supplier success cases.

If an aggressor gets to know you inside out, he/she will know your **needs**, **fears, insecurities, core beliefs, sensitivities, level of conscientiousness**, **personality traits**… gaining great power to use and manipulate you.

Bear in mind that:

. everyone needs something and

. even good values can be exploited as vulnerabilities

B. Gathering Information – Direct Approach

Gathering information is always the first step, it might serve on its own or be used as part of a bigger plan. We have mentioned passive ways but it can also be done through many other techniques that involve technology and, from the human factor, directly approaching people.

1. ***Elicitation:*** is a technique used to gather information in an unsuspicious way

REMEMBER: Elicitation attempts will ALSO take place in your private life, OUTSIDE your workplace, It occurs at social gatherings, at conferences, over the phone, on the street, on the Internet, or in your home. It works where your defences are lower. Through ordinary conversations, surveys, questionnaires, personal questions…

As there are many elicitation techniques[3], let us mention some frequently used ones[4]:

1. **Assumed Knowledge:** Someone pretends to have information, know details or have associations in common with a person or company to make the victim think automatically the attacker is someone to trust and maybe share more information.

2. **Can you top this?** Someone tells an extreme story in hopes the person/victim will want to top it.

[3] http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques
[4] For illustrating examples, see WP2.2 Annex 2

3. **Confidential Bait:** Someone pretends to divulge confidential information in hopes of receiving confidential information in return.
   It normally starts with: “Just between you and me…” “Off the record…”

4. **Make False Statements deliberately:** Someone says something wrong in the hopes that the victim corrects the false statement with true information.

5. **Feigned Ignorance:** Someone pretends to be ignorant of a subject in order to make the victim explain or expand on the subject, exploiting the person’s tendency to educate, show off….

These and other numerous tricks for covertly eliciting information, try most of the time to exploit other people’s:

Ego through flattering, praising	Natural need to feel clever, superior, show knowledge	Natural tendency to flirt
Tendency to educate, to correct others	Natural tendency to trust	Naivety
	Gossip habits	

Also very important to be considered are the techniques named by the FBI as:

6. **Oblique Reference:** A way of talking about one subject in order to get information about a complete different topic.

For instance: A question about comfort, temperature or AC at work may get an answer with insight into window accesses, security, locked doors…

7. **Targeting the Outsider:** To ask friends, family, clients, or competitors who may know a lot of information but may not be as sensitised.

1.1 Countermeasures

How can you resist the direct approaches that seek to steal information from you?

- Know the value of information, including personal information about you, your family, or your colleagues.

- Be ready to use refutational arguments and avoid the extraction of information by:

▪ **Changing the subject**
▪ **Referring people to open sources like websites or press releases**
▪ **Saying that you do not know**
▪ **Telling them that you have to check with your managers or security officer**
▪ **Stating politely that you are not allowed to respond**
▪ **Mentioning Data Protection Laws**
▪ **Answering with more questions**
▪ **Responding with "Why do you ask?"**
▪ **Giving a nondescript answer**
▪ **Avoiding gossip**
▪ **Being discreet**

- Always remember that even innocent conversations in theory can pose a threat

C. Cover Stories – Dispersed Approach (Establishing the relationship)

But the approaches are not always so simple, sometimes, they involve feigned identities, impersonation, clothing, logos, websites… everything in order to build a credible character…

Cover Stories or Pretexts are the fictitious storylines that malicious people might develop in order to deceive their target and obtain information, access or other goals, without raising suspicions. They can be used at a given moment, or be the story used to establish a longer relationship.

Traditionally, the most common cover stories used by criminals, fraudsters or terrorists have been:

Journalism: pretending to be a reporter… in order to be able to ask all sort of questions with a good excuse.
Surveys: Explaining a benign purpose for the survey, including the key questions among other logical ones... Or only using a survey to get people to talk with you.

	Master or Doctoral thesis: it has been found how real thesis disseminate a lot of real sensitive data, so using it as an instrument for data gathering about an organisation could be good but it would require good planning and backup
	Pretending to be customers, the will to sell makes people collaborate and give information away
	Pretending to be the gas man, a technician…policemen… the need for things to be repaired, the familiarity with the logos and labels, the respect for authority are used to get access to places and information from victims
	NGOs, charities: based on the need for support, help, and exploiting humanity and the desire to help others
	Job recruiting, headhunting: as job seekers are willing to give information away in order to impress

In the so called '**mosaic attacks**', little pieces of information are gathered by one or more people posing as a **co-worker, new employee, delivery person** or **workman** who have innocent conversations. The information collected may not be useful in isolation but can be be highly valuable when it is put together like in a jigsaw.

But any credilble story would work!

Once the malicious person has the information he or she needs, the aggressor is ready to establish the relationship, gain trust, obtain collaboration and **exploit the relationship**.

III. Principles

Some of the main principles of persuasion identified by Robert Cialdini[5] are a constant in the techniques that potential deceivers may use in the PSOPHIA context, such as:

- The **Principle of Reciprocity**, that focusses on the natural tendency of human beings to return favours and pay back debts, and also, to treat others as they have been treated. It will always be easier to get collaboration from someone whom we have already given something or done a favour.

- The **Principle of Social Proof**: we are more likely to be influenced by people who are similar to us. We also tend to look and do what others do.

- The **Principle of Liking**, it seems very obvious but people are also more likely to favour those who are physically attractive, who give them compliments or who are similar to themselves.

- The **Principle of Authority**: rather than to authority itself, we get automatic responses to the symbols that represent it: academic diplomas, clothes, uniforms and ornaments associated to status.

[5] Robert Cialdini, Influence: The Psychology of Persuasion (Quill/William Morrow, 1984). Cialdini is the source of the six principles of influence, but Steve Kleinman was the first to codify these principles under the mnemonic RASCLS.

IV. Recommendations

In order to countermeasure the abovementioned approaches, please follow PSOPHIA recommendations:

- Given the fact that you work at a CI, you are a potential target for criminals and terrorists, you must bear this in mind at all times both in your professional and private life.

- Remember that there are specific roles that are particularly vulnerable to attacks, like those in helpdesk, customer service, or those with access to important assets, such as IT administrators, security guards or certain managers.

- Examine the potential risks of publishing information on the organisation in articles, promo material, the website… always check with managers before giving away information at interviews, in surveys or academic research.

- The members of your family, specially your spouse, children or parents, might be easier to contact and deceive than you. They could also be coerced. Extend the security culture to your family, make them aware of the risks, teach them and try to prevent exposing habits. Do not share information about your work that could compromise you or them later.

- Beware of new pleasant acquaintances and people interested in you, especially those who are very complimentary. Be dubious of flirtatious strangers. Always do the exercise of thinking first 'they might be interesting in my work'.

- Before accepting a free gift or present, help or apparently innocent confidences, consider if you are going to feel obliged to return favours and what consequences that might have.

- Do not enter or participate in projects or groups that offer 'too good to be true' deals, specially without checking all details about the functioning, the people behind, what obligations they entail, etc.

- Do not trust colleagues or people around you blindly, they might be under the influence or coercion of third parties. Always check yourself the nature and security of the material or information passed on to you, even when it comes from a person you trust. Check credentials before responding to any enquiry.

- Do not rely on the safety of technology and technical devices.

- Respect the golden rules of information security (check INFOSECURE's website), like the clear desk policy and rules related to e-mails, printing, disposing documents, passwords…

- Remember that, before an elicitation attempt or a more complex attack, these aspects are against us:

    a. Comfort and relaxation
    b. Haste and rush
    c. The general feeling that 'things like that will never happen to me'. In your kind or organisation, certain attacks are very unlikely but possible, and when they occur, they have devastating effects.

- Be very selective and discreet when posting information about yourself and your job on social networking sites.

- Avoid talking about sensitive work issues in social situations. Remain discreet at all times.

- Remember that bars and restaurants are places where a lot of information circulates, but other risky places could be your local shops or businesses, sport clubs… Do not lower your guards specially at hotels, cocktail parties, receptions, seminars and congresses.

- Beware of alcohol and talking about work under its effects.

- Practice the anti-elicitation techniques and socialise or network without disclosing sensitive information.

- Do report unusual and suspicious behaviours.

REMEMBER THE PSOPHIA THREE-STEP METHOD FOR COUNTERING SECURITY THREATS RELATED TO THE HUMAN FACTOR

These steps will lead you to a more sensitised and sensible behaviour that could prevent and reduce potential attacks.

. Step 1: Know your vulnerabilities

Go through the list of risk factors provided (see WP2.2 Annex 1) and get conscious of your own personal situation and vulnerabilities. Check which techniques and tricks (right column) are more commonly used to exploit those factors. Also assess which people around you could give information about you, your habits, etc.

. Step 2: Know the value of information (sensitive and non-sensitive) and **be aware of the information you have** at your disposal

Check with your managers in case of doubt.

. Step 3: Be ready

Evaluate any personal approach in your professional or social life, always considering the possibility of hidden intentions, and the consequences of your responses, before acting.

Increasing Security Awareness of Critical Infrastructure OPerators introducing Intelligence Techniques and focusing on Psycho-social and Human factors