The NeoSens Training Method: Computer Security Awareness for a Neophyte Audience

Tiphaine Romand-Latapie

Abstract

This document describes how to train a neophyte audience to the basic principles of computer security. This method is based on a role-playing game, created by the author. The reader will find in this document the information needed to carry out the training.

1 License

This document is published as material from the Black Hat USA 2016 conference.

2 Introduction

The concept of this methodology is born from the need to train an operational and neophyte audience to computer security stakes. According to the author's experience, standard trainings focused on technical context (what a password is, how does a computer work etc.) tends to bore or scare neophytes.

An alternative would be to concentrate on the generic principles of infosec:

- The decision whether or not to trust an entity/a person.
- The notion of in-depth defense.
- The attacker's motivations.
- The attacker stereotype versus reality: he is not necessarily a "genius hacker".
- The necessary trade-off between operational constraints and security.
- The goals of the security team: forecast the attacker's behavior, prevent or detect the attack.

The concept of the training stems from the fact that basic principles, in particular the following, are the same for physical or computer security:

- In everyday life, we have to decide who we trust.
- In physical security, we always work on the worst-case scenario and we handle the cases where the basic security measure is deactivated/ineffective
- Attackers' motivations are money, ideology etc.
- The most common attacker is a not crime genius.

Physical security brings constraints too (lock the door, carry a badge, perform security check at the airport etc.). These constraints serve the same goal: forecast the attacker's behavior, prevent it or detect it.

Yet, an audience of neophytes is more familiar with physical security than with computer security, in their everyday life or professional life: they lock the door before going out, they don't let strangers enter their homes, they have all already gone through security checks, etc.

The core idea of this training is therefore to make neophytes realize that they already know security best practices. They only have to learn how to apply them to computer security. By playing this game, they do so in a fun way.

This training has been successfully used in real conditions with roughly 70 trainees. The trainees were top managers, project leaders, marketing, call centers, customer support, developers etc. The only people so far on which the training did not work are people from InfoSec community. The habit to anticipate the "enemy"'s behavior is leads them to over specify any defense or attack, preventing the dynamic of the game to take place.

3 The role-playing game

The training is developed around a role-playing game consisting in attacking and defending a building.

3.1 Rules

The game is led by a Game Master (GM) and involves an attack team and a defense team.

3.2 General description

- The action takes place in an office building located in a dense urban area, with an underground parking lot and an helicopter landing pad. A highly valuable object, fitting in a backpack, used by employees during the day, is stored somewhere in the building.
- At the beginning of the game, the building is not secured at all.
- The attackers propose an attack, the defenders a mitigation, in an iterative way.

3.2.1 Attack team's rules and goals

- Goals: steal the object without getting caught.

- Rules: unlimited budget, limited number of human attackers in the game (no more than ten people). The laws of physics apply (gravity, etc).

3.2.2 Defense team's rules and goals

- Goals: prevent the theft or record data allowing to identify or catch the attackers.
- Rules: unlimited budget, unlimited staff. The laws of physics apply, the laws of the country must be respected, employees must be able to work in the building during office hours and some employees must be able to use the object.

3.2.3 End of a scenario

- I recommend stopping the current exchange (called "scenario" in the following) when teams get to a blocking point (everybody is dead, the object is destroyed, the police have arrived, etc.).
- It is then possible to move on to a fresh start by the attack team. In that case, the defenders keep all the security measures they have already deployed. For example, if the attempt to pass through the front door in a first attempt is too complex, the attacker should try to pass through the roof.
- If the players want to, or if the GM wants to revive the game, it is possible to switch the teams: the attackers become the defenders and vice versa.

3.2.4 End of the game

- There are neither winners nor losers!
- I recommend doing multiple scenarios during one game. The duration of the session is a choice of the GM: forty to sixty minutes is a good duration for a 6 player game.
- The session is followed by a debriefing by the trainer, allowing him or her to highlight the concepts (see the "Debriefing" section).

3.3 Behind the rules

3.3.1 The playing environment

The playing environment (building, dense urban area etc.) was chosen to maximize the playful side of the game and facilitate its application to the training:

- The fact that the building must be usable by employees during the day allows the trainer to work on security versus constraint compromises and offer a familiar environment for the players.
  - It can be a good idea to personalize the details of the game using the players' professional environment: company's building, its key product, etc. This allows a faster immersion and involvement from the players.

- The choice of a dense urban area, as well as the helicopter landing pad and the underground parking lot, reinforce the fun part (the attackers can think of helicopter landing on the roof, can jump from a building to another etc.) and guides the players. Furthermore, it helps diversifying scenarios.
- The choice not to further detail the environment has been made to let the players' imagination run wild and to simplify the rules of the game.
- The usability of the object during office hours allows us to stay clear of non constructive mitigation, like "we cast the object in concrete".
- The location of the object within the building is not defined, it can change during the game if the defenders wish to.
- Beginning with a non-secured building is important:
  - It allows the trainer to work on the security measures stacking and on the principle according to which the attacker always seeks the easier way in (path of least resistance).
  - Sometimes, the attackers consider that there is basic security in the building (locked door, CCTV, etc.). In this case, it's not essential for the GM to recenter the frame. It is, however, interesting to make the players think about it during the debriefing.
- Fast exchange allows a lively and fun game.

3.3.2 Attackers' rules and goals

- A simple goal, referring to movie hits (James Bond, Oceans 11, etc.), easy to translate in computer security goal (going in and out without leaving a trace).
- The unlimited budget simplifies the game. Furthermore, it is always possible to discuss financial aspects during the debriefing.
- The small number of human beings authorized for the attack team during the game allows us to stay clear of non realistic scenario like "laying siege with a three hundred people army".
- Respecting the laws of physics allow us, once again, to stay clear of non realistic scenario or unsporting behavior.

3.3.3 Defenders' rules and goals

- A simple goal: protecting an object.
- The unlimited budget simplifies the game. Furthermore, it is always possible to discuss financial aspects during the debriefing.
- The unlimited staff is here to compensate a little for the need to respect the law, while allowing the trainees to experience that sometimes expensive security measures can be ineffective.
- Respecting the laws of physics allow us, once again, to stay clear of non realistic scenario or unsporting behavior.
- Respecting the laws of the country reminds the trainees that IT security engineers have to do the same.

3.3.4 Losing and Winning

There are neither losers nor winners, even if the teams usually want to name one. Rules to define winners/losers would make the game unnecessarily complex. The rules aim at stimulating fun exchanges between players while bringing out the ideas needed by the GM to achieve the training.

3.4 Facilitation of the game

The trainer, also named Game Master (GM), facilitates the game. It is essential to form small teams. I recommend two to three defenders and the same for attackers (for a total of eight players). Beyond this number, it is very difficult for the trainer to follow the game.

The trainer begins the session by explaining the aim of the game, and its rules.

3.4.1 Aim of the game

Make the trainees realize that they already know security best practices. The training is here to give them the keys to apply them to computer security.

3.4.2 Explaining the game rules

It is essential to highlight the physical aspect of the game. In a few cases the trainees, aware that they are attending a computer security training, seek straightaway to "hack" information systems. The double goal (prevent or detect for the defender, theft without being caught for the attackers) must be highlighted during the rules presentation, in order to make the concepts of impersonation and traces emerge. Finally, do not hesitate to insist on legal aspects: the attackers do not respect the rules, which is not the case of the defenders.

3.4.3 Playing the game

As soon as the game begins, the GM must write down the exchange on a medium visible by all players (see the example supplied in this document). As the Game Master, the trainer is responsible for enforcing the rules and has the right to impose limits to one or the other team.

He must make the players clarify their actions when necessary:

- If something is locked, we must know what type of lock is used (biometrics - retina scanner or fingerprint scanner, entry pass, pin code, physical key, etc.) and who exactly owns the means to open the lock.
- In case the defender's team decides to set up a backup power generator, the players must list which security systems are powered by this generator. The GM can then set a limit on the generator's operating duration it is working. Typically, if the generator powers all the security features, it cannot operate more than a few hours.

- If CCTV camers are used, the players must specify if they are watched in real time, and describe the watcher's team (size, location. . .).

The GM may require players to give more details about some of their actions, depending on the teachings he wants to highlight during the debriefing. However, I strongly recommend making players precisely describe the actions listed above.

Everything that is not explicitly said by one team can be interpreted/hijacked by the other team: if the defenders do not specify that the windows are closed, the attackers can consider them to be open. If the attackers do not tell that they are masked, one must consider that their face will be caught on CCTV.

The game master can guide one or the other team if he thinks the game is not going in the right direction, or to revive it. He can, for example, bring back the rules at the approriate time, like telling a shy attack team "I remind you that you do not need to follow the law, you can blow up these doors or kill this guard". The GM's goals is to bring up in the game (or look for) the ideas allowing him to illustrate the basic principles of computer security during the debriefing.

No analogy with computer security must be done during the game. The link is brought up during the debriefing only.

3.4.4 Game over

It is recommended to close the ongoing scenario if:

- The attackers keep going in the same unsuccessful course of action.
- The ongoing scenario becomes too complex.
- The ongoing scenario becomes too unrealistic.
- The trainer wishes to swap the teams.
- The players start to lose motivation (it is then possible to either stop the game or switch teams).
- The trainer already has the material he needs for the debriefing.

3.5 Exchange/scenario example

This exchange was observed during a training. At this time, the game had been on for 10 minutes.

Table 1: Scenario example

Attackers	Defenders	Game Master
Corrupt a subcontractor's employee and make him carry out the theft.		

Table 1: Scenario example

Attackers	Defenders	Game Master
	When used, the object stays visible to the user at all time. As soon as the user has finished, the object is put in a safe locked up by a physical key. Three people have a copy of the key: the user himself, his manager and the company's head of security. The actions of the keys owner are tracked.	Who has the key of the safe?
Find the name of the company's head of security, watch his schedule. Violently steal the key, then give it to the subcontractor.		
	The safe is not easily found.	Ineffective measure: the maintenance staff can find it easily.
	CCTV on multiple surveillance screens. One guard is behind the screens 24/7, the video streams are recorded. Another guard is in the lobby.	Warning: too many cameras implies it is difficult to watch them in real time.
A cleaning lady distracts the CCTV guard while another one perpetrates the theft.		

Table 1: Scenario example

Attackers	Defenders	Game Master
	The guards were trained by Special Forces, there is a background check on all subcontractors.	There is always a way to find a weakness to exploit or to blackmail a person. Furthermore, guards need to go to the bathroom, or can be sick. But the attackers loose: the cleaning lady's face is caught on CCTV.
The cleaning lady hides in the bathroom to dress up, the person distracting the CCTV guards uses a device that can destroy the video data on hard drive (magnet).		
	There is a CCTV camera on the corridor leading to the bathroom, the server room is protected against tampering (in the center of the building, in a Faraday cage).	The CCTV camera has been put in front of the bathroom instead of inside it because of a GM remark, French laws do not allow CCTV cameras in bathrooms.
Unplug the camera in front of the bathroom.		
	Audio and visual warning in the guard lodge as soon as the camera is unplugged or malfunctioning.	The Game Master forces the end of the scenario, to make attackers move on.

4 The game's debrief

4.1 Learning the common basic good practices

As explained in the introduction, neophytes already know security good practices that can be applied to physical security as well as to computer security. I recommend pre-

Table 2: Decoding keys

Physical security	Computer security
Key / Badge	Password, smart card
Safe, reinforced door	Technical measure of protection
CCTV	Supervision/logs
CCTV records destruction	Logs destruction or tampering
Blackout / arson	Denial of Service
Guards, surveillance employees	Security Operations People/Anti-Virus
Disguise / false ID card	Impersonation of IP addresses or identity
Observation, get some top manager's name, get info, etc.	Reconaissance, social engineering
Emergency procedure, generator etc.	Failure resistance, in-depth security
ID card	Certificate
Specific technology use (jammer, explosive, drone ..)	Use of exploits, command and control center, etc.

senting these good practices just after the game, in order to link them to the scenarios which have come up during the game. You can find below a non-exhaustive list of good practices that need to be highlighted by the trainer:

- Do not trust by default.
- Check IDs.
- Don't give your home key/alarm pin/password to anybody.
- Emergency services: would you give them your home key "just in case"?
- Call the police/security team when you suspect malicious activity.
- Ask ourselves:
  - Could someone be interested in attacking my building? To what extent?
  - Could this information/badge/key be of value to someone?
  - What do I do in case of malfunction?

4.2 Scenarios decoding keys

It's easy to draw parallels between the physical elements used by the trainees during the game and computer security elements. The goal of the debriefing is to allow the trainer to highlight the key points he chooses. Table **??** presents a non-exhaustive list of decoding keys of widely appearing elements in the game.

4.3 Similarities and divergences

The similarities between physical and computer security have already been presented multiple times in this document. We now go over them one more time to highlight key examples that illustrate these principles and come up in the role-playing game.

4.3.1 The “trusting someone” problem

Very early in the game, trainees are exposed to the access control principle. You will see that defenders begin by deploying badges and ID verification in the lobby, while attackers will turn to disguise, and lies. It is important to use this key point to make the trainees think about the concepts of trust, identity and authentication. The use of a false ID card is, for instance, very interesting: what can we use to trust someone when he states his identity? This notion is at the center of every security system. The trainer can also take advantage of this discussion to talk about various authentication methods:

- Biometrics.
- PIN code or passwords.
- Key (which can be lost, stolen, copied etc.).
- ID cards, which sends back to the concept of trusting a third party (the government in physical security, the Certification Authority in infosec).

Finally, in most game sessions, attackers quickly used deception or identity impersonation. For example, in one of the sessions, the attackers were getting the name of a top manager, and were insisting on the urgent nature of a delivery at the reception. This type of scenario is very useful to illustrate the concepts of phishing, scam and social engineering. It is also the moment to make the trainee think about a great principle in security “the human is the weakest link”.

4.3.2 Defense in depth

The defense in depth idea, which consists in piling up security measures and handling the possible failure of one of them, appears easily in the game. For example the trainees consistently proposed an access control in the lobby and a different one for the room where the object is stored. Often, they even added an access control near the object itself.

The trainer must highlight this behavior, and make the trainee notice that the same applies to computer security. It is the moment to talk about multiple security measures, and to make them aware of their benefit. As security engineers, we often hear sentences such as “But it is in the LAN, there is no risk” or “but the user has already entered a password, why do we need another one?”, etc.

The multiplication of technologies (physical key, badge, biometry, etc.) is also a way to make trainees think about security best practice (not reusing passwords, etc.). Finally, the attackers’ varied attempts allow us to illustrate the fact that the security level of a system depends on the security level of its weakest element.

4.3.3 The attackers’ motivations

The different scenarios allow the trainer to illustrate the important notion of the attackers’ (or defenders’) motivations. When the attack itself costs millions and months of preparation, we can ask ourselves: is the object worth it? The same question may be asked to the defenders.

It is also an opportunity to discuss the security level versus the attackers' level, and to think about the question at the core of all security systems: what do we protect, who do we protect against?

4.4 Demystify the attacker

The fact that there are several attacker's profiles is one of the least well-understood concepts for neophytes. The collective imagination depicts attackers as genius hackers, in an underground cave. Yet, as in physical security, there is a variety of attackers: if your door is not locked, any delinquent can enter your building. When the scenario becomes complex, we face very well organized and motivated attackers.

The black market idea is also not well understood

- In physical security, the objects can be resold or ordered prior the theft. It is the same in computer security, and the trainee must be aware of this.
- A physical attacker will buy specific tools (explosives, jammers, false ID, ...). A computer attacker will do the same. It means an economy has developed around the discovery of tools (vulnerabilities, exploits, etc.) and their trade. Make the trainee aware of these different profiles: anybody can push a button on a jammer, but you need specific skills to design one.

4.4.1 Constraint versus security trade-off

To illustrate this idea, the trainer must focus on the security measures deployed by the defenders, and the constraints they imply for the company's employees or the company itself. The link is then easily made with computer security constraints.

One interesting element to work on is the presence of emergency services (police, army, firefighters, etc.), and whether they are legitimate or not. Ask the trainees: do they give the emergency teams full access to the building, just in case? Do they check whether they are legitimate? In one of the game sessions, the attackers posed as a medical team who evacuate victims via helicopter (they, in fact, were evacuating the stolen object). This is the time to discuss the privilege accesses of teams like after-sales, IT support etc. and the need to store clear text passwords "in case of the client needs it".

4.4.2 The security teams' goals (predict attacker behaviors, prevent or detect it)

In the game, the work for the defending team is easier than in the real world: the attackers announce their intention and their goal is known. The trainer can pinpoint, during the debriefing, the difficulties of the security teams' work: they have to imagine the attackers' behavior and evaluate their possible motivations. The trainer can also make the trainees think about supervision or tracing tools.

4.4.3 Divergences

Of course, the whole physical security isn't transposable into infosec (and vice versa). But the differences, as essential as they may be, are not that many:

- The time factor differs greatly:
  - For example: testing a password is a lot faster than testing a physical key on a door.
- The geographic factor nearly no longer exists:
  - The attacker does not need to be physically present to conduct the attack. The physical distance does not matter anymore.
  - There are, of course, exceptions to this rule:
    - The laws depend on the physical location of the stolen or tampered data;
    - When attacking via compromising signals, radio flux or hardware element, the physical distance can come up again as a critical issue.
- These two scale changes result in mass attacks costing less and put them within anybody's reach.
- The exact and easily collected evidences only relates to the machines, less easily to the human beings.
  - It can be very difficult to find the actual perpetrator.
  - The attackers can hide themselves behind innocent third parties.
- The theft is virtually impossible to detect (electronic copy).
  - Some evidence of the theft can be found is the system is correctly configured.
- Too often, there is no basic security deployed in IT, where, in the physical world, people would have a working lock on the door, at a minimum.

5 Game session example

This game session has been carried out with five people (three defenders and two attackers), it lasted nearly fifty minutes.

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
Open the door, collect the object, get out.			Unprotected data theft.
	The door is secured by a badge reader and is physically locked after 8 PM. If an attempted theft is detected an alarm is triggered, linked directly to the police station.		Password based protection, access control, supervision.
A woman is sent to seduce an employee, she tells him she has forgotten her badge, the male employee let her pass (theft then exit).			Social engineering.

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
	The object is locked in a safe, a PIN code is needed to open the safe. The site supervisor is the only one who knows the PIN (people must call him each time they need to use the object). Carrying a visible badge is mandatory within the building, security agent ensure the enforcement of the rule. Furthermore, employees are aware of the risks lying in letting an unknown person enter the building.	We can notice that the measure is very restrictive for the company (one and only one person has access to the object)	Password based protection. Non sharing of passwords. Supervision. Awareness training.
Dressing up as a janitor, entering with a stolen badge and a cart containing a blowtorch. Open the safe with the blowtorch, get the object, put it in the cart and exit.			Impersonation, brute force attack.

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
	There is a smoke sensor in the room. The entry of the room is protected by a retina scan.		Attack detection, biometry.
The attackers land a helicopter on the roof of the building and use the air conditioning pipes to gain access to the room. Go down ”like in ’Mission: Impossible’” and steal the safe. Exit from the building and then open the safe.			Offline attack, theft followed by protection workaround.
	The safe is sealed in the wall, furthermore, it is electrified until the retinal scan is OK.		Offline attacks banning. Ban all action before authentication check.
Blackout			Denial of Service/failure of the security system.
	Generator supplies all the security measure of the room.		Emergency back-up system.

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
The attackers take a member of an employee's family in hostage and blackmail him to commit the theft himself.			Social engineering.
	CCTV cameras are placed in front of and in the room, the camera feeds are watched in real time 24/7 by employees in the security command center which is not in the same building.		Supervision and logs on dedicated servers.
Blowing up the security command center.			Destruction, tampering of the logs.
	In case of explosion or communication loss with the security command center, teams of guards are sent to the command center and to the building. An alarm is triggered in case of communication loss.		Logs protection, in depths security, monitoring of security measures etc.

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
Hacking of the CCTV feed to cut the video stream.			Attack to destroy the logs, DoS on the supervision system.
	A motion sensor is put on the object, if triggered, the object blows up.	Refused: the object must be usable during the day, and not compliant with French law	In infosec, “emergency erase”. If an attacked is detected, all sensitive data are erased. Very constraining.
Intrusion by using the CCTV camera blind spots, theft of a badge for entering.			
	Enough CCTV cameras to have no blind spot at all, there is one guard watching per screen, one screen per camera.	Costly measure.	Increase of the supervision and security operational people.
Cover the camera with a picture of the hallway.			
	A guard is in the lobby and controls all the entry, patrols with dogs.		
Kill the guards and feed the dogs to distract them.			
	There is always the retina scan, a fingerprint scan is added.		Biometry .

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
An infiltrated employee commits the theft.			
	Systematic person search at each entry/exit of the building.	Very constraining measure (several seconds by person, in rush hour, etc.).	Real time control of everything stored on employees computers (forbidden by French law).
Drone used to get the object out of the building.			Data exfiltration.
	Person search at each entry/exit of the room.	Very constraining measure (several seconds by person, in rush hour ...).	
Murder of the guard securing the room.			
	Anti theft device on the object allows knowing when the object leaves the building, in case of detection, the site is locked down.		Data watermarking (less effective).
Trigger an arson to obtain the automatic opening of the doors.			Emergency procedure attack.
	GPS tracker on the object.		
Use of silver foil to avoid detection.			

Table 3: Example of a full game session with five players for a duration of nearly fifty minutes (without debrief)

Attackers	Defenders	Comments	IT security parallel
	Army intervention to take down the drone.		
Hundreds of drones making diversion.			
	Radio jammer to prevent piloting the drones.		
Drones autopilot pre programmed.			
	Jammer for GPS signals to prevent the autopilot working.		
Passing by the underground parking while the drone gets out with a copy of the object, exit on three motorcycles, only one has the object.			Diversion, overload of the supervision system.
	Nails were spread on the exit road as soon as the alarm was triggered. There is a reinforced door at the exit of the parking lot.		All expected ideas have been expressed, furthermore, the scenario is becoming too complex. End of the game.