Embedding security messages in existing processes: a pragmatic and effective approach to information security culture change

Sebastian Lopienski, CERN

Geneva, September 2010

MBA in Information Security Governance

Haute Ecole de Gestion (HEG) de Genève/Haute Ecole Spécialisée de Suisse occidentale; and

Institut d'Administration d'Entreprise (IAE) Aix-en-Provence/Université Paul Cézanne Aix-Marseille III

heg
Haute école de gestion de Genève
Geneva School of Business Administration

iae
aix-en-provence
GRADUATE SCHOOL OF MANAGEMENT

Abstract

Companies and organizations world-wide depend more and more on IT infrastructure and operations. Computer systems store vital information and sensitive data; computing services are essential for main business processes. This high dependency comes with a number of security risks, which have to be managed correctly on technological, organizational and human levels. Addressing the human aspects of information security often boils down just to procedures, training and awareness raising. On the other hand, employees and collaborators do not adopt security attitude and habits simply when told to do so – a real change in behaviour requires an established security culture. But how to introduce a security culture?

This thesis outlines the need of developing or improving security culture, and discusses how this can be done. The proposed approach is to gradually build security knowledge and awareness, and influence behaviours. The way to achieve this is to make security communication pervasive by embedding security messages, warnings and advice in human and technological processes, and situations that already exist within an organization.

Keywords

Human Aspect of Information Security, Organizational Culture, Security Culture, Culture Change

Acknowledgements

First and foremost, I wish to thank my wife Ewa for her understanding and her encouragement, especially during the final months of my MBA studies and working on this thesis. I would not be able to start and complete the studies, and write the thesis without her support. For these and other reasons, I would like to dedicate this thesis to her.

I am also very grateful that CERN and IT department management, as well as the former Computer Security Officer, David Myers, have supported my studies, and have been favourable to my diploma project – which, I am certain, will be beneficial for CERN.

This thesis would not be as it is now without the dedicated guidance offered by my professor and tutor, Rolf Hauri. I also wish to thank Jean-Yves Oberlé, director of this MBA programme, for his initial comments and ideas for my diploma project, and in general for running successfully this very interesting educational programme.

The ideas, help and feedback that I received from my colleagues from CERN Computer Security Team members (and especially from Stefan Lueders, the Computer Security Officer; and Lawrence Gray) and the very stimulating work environment they all create was also very much appreciated.

Finally, several of my friends and colleagues in HR and IT departments (and in particular Maria Dimou, IT Department Training Officer) have also been very supportive and helpful, when I was working on the diploma project and writing the thesis.

Thank you all!

Sebastian

Table of Contents

Chapter 1. Introduction

1.1. Motivation

Computer security incidents of different type and gravity continue to plague organizations, despite growing investments into security solutions, services, products and personnel. On one hand, both attack vectors and defense measures are becoming increasingly sophisticated. And the need for advanced technological security solutions should not be neglected. On the other hand, many of the incidents – caused either by malicious activity or by simple carelessness – could just have easily been avoided.

It simply happens way too often that incidents with major consequences are simply triggered by user mistakes; lack of understanding and wrong use of security measures; or bypassing them altogether. Data leakage, often listed among the biggest information security risks these days [1], is in most cases "inadvertent or accidental" [2]. One of the most infamous cases is HMRC[1] data loss in 2007: two discs containing confidential personal details on 25 million people in the UK were lost [3]. These weakly-encrypted discs were sent via a courier to another government agency, but failed to arrive to destination. Of course, the junior official who did it (twice!) has breached security procedures when choosing weak encryption password and using unregistered post. However, he did it because he believed and assumed that this was the way to do the work and have things done. This fact is actually even more worrying and alarming. The official inquiry led to the same conclusion – the final report blamed "a culture of insecurity rather than mistakes by any single official" for this "entirely avoidable" incident [2].

> *Culture of insecurity was blamed for HMRC data loss in 2007 (confidential personal details of 25 million UK citizens lost).*

This phrasing suggests that the opposite – a culture of security – would have made this and similar incidents much less likely to happen. But actually, is this true? This is a very interesting question – and I believe that it merits looking deeper into the concept of information security culture, and seeking ways to establish it. That is exactly what I attempt to do in this thesis – and also to implement at CERN.

[1] Her Majesty's Revenue and Customs – UK's tax authority.

1.2. CERN

CERN, the European Organization for Nuclear Research, located near Geneva, Switzerland, is the world's largest particle physics laboratory. It was founded in 1954 as one of Europe's first joint ventures, and now has 20 Member States[2] and 8 Observers[3]. CERN's main purpose is to enable fundamental research in particle physics by designing, building and operating particle accelerators and detectors, as well as providing infrastructure for analysing experiment results [4].

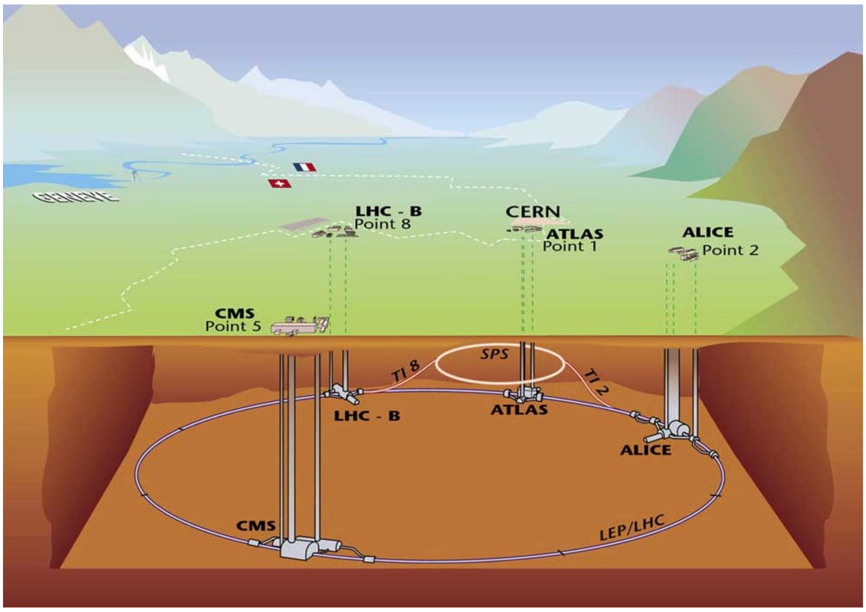


Figure 1. LHC accelerator and its experiments

The main scientific instrument currently used at CERN is the Large Hadron Collider (LHC) – the biggest and highest-energy particle accelerator in the world. The LHC lies in a circular, 27 km long tunnel about 100 meters underground (Figure 1). Beams of particles are boosted to high energies – and speeds nearing the speed of light – before they are collided with each other. Physicists analyze new particles created in these collision using special detectors in order to understand better what the universe is made of and how it works [5]. CERN is also known as the place where the Web was born [6].

Information technology (IT) plays a crucial part in CERN "business", as accelerators and detectors depend on IT solutions, and all physics data is stored and processed in distributed and often remote IT systems. The LHC and experiments operations, physics analyses, but also most engineering and administrative activities – they all require a robust and reliable (and, consequently, secure) computing infrastructure, from networking, desktop computing, various computing services to data processing and storage, Grid computing[4] and control systems.

[2] As of 2010, CERN Member States are: Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Italy, the Netherlands, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland and the United Kingdom.

[3] Observer States and Organizations currently involved in CERN programmes are: the European Commission, India, Israel, Japan, the Russian Federation, Turkey, UNESCO and the USA.

[4] Grid computing is a service for sharing computer power and data storage capacity over the Internet [102].

CERN has around 2500 employees, and its facilities are used by more than 10,000 visiting scientists representing 580 universities and 85 nationalities [7]. This means that many people who work at the laboratory are actually not employed by CERN. Staff members, fellows, associates, students, CERN users[5], project associates, apprentices, employees of CERN contractors – they all have CERN computing accounts and have access to most of CERN computing resources and services. In other words, computer user community at CERN is large and complex.

This diversity and a fairly high turnover of visitors and short-term employees, combined with CERN's openness and academic freedom, makes it more challenging to guarantee a desired level of information security awareness, knowledge and behaviour. Simply speaking, it is hard to reach all these different groups of people, raise their security awareness, educate then, and convince them to act securely. This is why I believe it is worth attempting to establish security culture at CERN – in parallel to having other existing security measures, programmes and initiatives already put in place by CERN Computer Security Team.

1.3. Outline of the thesis

This thesis starts with an examination of the human factor of information security. Security systems or solutions may be very well designed and implemented – and still they rely on people who design, use and manage them. The human factor plays a crucial role in the majority of information security incidents. **Chapter 2** ("Human aspects of information security") explains why technology alone cannot solve all security problems; discusses different aspects of the human threat; and proposes a number of measures to address that threat. The chapter finishes with a conclusion that one of the best defenses against information security threats is a culture of security.

Chapter 3 ("Security culture and culture change") looks deeper in that direction. First, it attempts to define what organizational culture is, and what it is built of – and it presents different corporate cultures, and culture models used to classify them. The chapter then focuses on security culture, trying to describe what it means, and how it can differ across different industries. An interesting question is also discussed there: whether security should be one of the corporate values. Finally, we look into the culture change process, in order to consider what it usually takes to establish or change organizational culture.

Security culture can be established by embedding relevant security messages and advice in existing human and technological processes.

As we will see, a major culture change needs to be justified with an urgent need, and requires strong leadership and significant investments to be effective. Does it mean that security culture cannot be established without these three prerequisites? In **Chapter 4** ("A different approach for security culture change") I propose another way to achieving that goal. The proposed approach is to build security knowledge and awareness, and to influence behaviours gradually, by surrounding people

[5] CERN user is a special category of scientists visiting CERN – not to be confused with computer users.

with relevant security messages and advice. It should be done by embedding security content in various processes that already exist – that people go through anyway – such as recruitment, periodic evaluation or existing training.

Chapter 5 ("Security messages in human processes") and **Chapter 6** ("Security messages in other processes and situations") contain specific ideas on which processes can be used for security communication, and what kind of security messages should be passed. The content of these chapters is based on processes that are in place at CERN – but should be easily applicable, or at least adaptable, to other organizations.

Some of the ideas and solutions proposed are already implemented at CERN, others are being currently introduced, and yet others are still in the planning phase. When possible, samples of actual security communications and their context will be included, either within Chapter 5 and Chapter 6, or in **Appendices**.

Finally, **Chapter 7** ("Inspiration, conclusions and open questions") reports some initial feedback received for the proposed approach to develop a security culture, and first results achieved. The chapter ends with a conclusion and an outlook of possible future work in the area.

1.4. Conventions

This thesis is about information security, rather than safety or physical security – although obviously all these domains have common areas. For clarity reasons, the term "information security" is often shortened to "security" – which encompasses a wide range of activities such as asset protection, managing access rights and preventing incidents from happening, among many others. Whenever it is important to distinguish between specific domains of security, full terms such as "network security" or "software security" are used.

Similarly, for the sake of simplicity, the masculine form ("he", "his", "him") is used throughout this document when referring to persons (employees, leaders, users, contractors etc.) of any gender – women or men.

While the term "organization" is widely used in this thesis, it is sometimes replaced with other words such as "corporation" or "company". However, unless stated otherwise, the content applies to any type of organization: commercial or non-commercial.

Chapter 2. Human aspects of information security

2.1. Technology, organization and human aspects

It starts with technology...

Since several decades modern information systems are based on technological solutions: computers and networks, software, databases etc. It is therefore natural that most security measures and products, designed and implemented to protect assets and detect intrusions, are also technical. Over the years, we have seen the rise of whole industry branches that are delivering sophisticated products such as firewalls or antivirus software. Other technical security solutions include network packet sniffers, intrusion detection and protection systems, vulnerability assessment tools, Web traffic monitoring and filtering systems, encryption algorithms and cryptographic protocols, multi-factor authentication solutions, or biometric systems. All these technologies are very useful, and should be considered and used where relevant, needed, and cost-justified. For example, it would simply be negligent not to encrypt sensitive data before transferring it over an untrusted network.

Yet despite using advanced security technologies, computer and information security incidents and breaches happen every day. Some of those incidents, experienced by organizations and individuals alike, become very serious. Such cases are plenty – and they are often covered even in mainstream media, as consequences regularly affect well-known companies, or large numbers of individuals. Let’s take, as an example, one of the biggest security breaches in the recent years. An SQL injection vulnerability at Heartland Payment Systems, a card payment processing company, was exploited by attackers in early 2009. It resulted in over 130 million credit and debit card numbers stolen, tens of millions of customers affected, and $60M expenses so far to cover losses [8].

The obvious question is: could that have been prevented? And how?

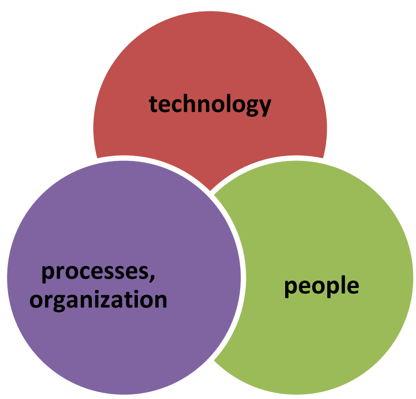


Figure 2. Information security is about technology, organization and people

… but is it enough?

The reality is that most if not all technical security solutions have their weaknesses and drawbacks, or can be simply bypassed altogether. Encrypting sensitive data in network communication is surely a must, and the encryption algorithm used may be very strong cryptographically – but confidentiality of the encrypted data depends also on a number of other factors. How well was the algorithm implemented? How reliable is external software and libraries (e.g. the pseudo-random number generator) used in that implementation? How secret are the private or shared keys used for that encryption? Aren't they simply protected with a 4 digit PIN code that would be trivial to brute-force offline? What happens to that data before and after it is being transmitted encrypted over the network? Is the recipient of the data really who the sender thinks he is? Are people who handle that data immune to social engineering attacks? Actually, are they trustworthy? etc.

> *Information security – both problems and solutions – is as much about processes and people as it is about technology.*

An answer to any of these questions could reveal a weakness that would completely undermine the confidentiality of the encrypted data – without breaking the technology (encryption algorithm) itself. This illustrates why IT or information security is not only a technology problem. It is widely understood among professionals that information security – both problems and solutions – is also about processes and organization, as well as about people (e.g. [9]).

In fact, this is true even for seemingly technical issues. Of course, SQL injection – root cause of the Heartland Payment Systems security breach discussed above – is a technical vulnerability. It could have been avoided, or prevented from being exploited, with technical measures such as vulnerability scanning or Web application firewalling[6]. On the other hand, this vulnerability was introduced by a developer, a human who followed a particular (implicit or explicit) software development process. Was he trained to write secure code, and motivated to pay attention to security issues? Were there suitable code review and security testing processes in place? Was the whole software lifecycle organized in a way to prevent or detect such vulnerabilities? We can already see that most of these questions evolve around people, and around the way things are organized.

In security, best results are achieved with so-called "layered" approach: where multiple protection and detection layers guarantee defense in depth. It is important to lock the door of a house when leaving, but living in a safe district, having watchful neighbours, and installing an anti-theft alarm give additional protection and assurance. Similarly, in IT systems, information should be protected at various levels at the same time: on the data storage level, application level, operating system / host level, internal network level, at the external network perimeter level, as well as on the physical access level, and procedural level (e.g. [10], [11], [12], Figure 3). But again, most of the defense levels listed before are technical concepts. And while it does pay off to assure security with technical

[6] Application firewalls operate on the application level, filtering and validating input to an application or a service [103].

solutions, having additional layers of defense on the process or organization level and on the human level brings much more security. Simply, assets must be protected with technical means, but also with relevant procedures and processes in place, and taking into account the human factor. As we will see, any global security effort that focuses only on the technical problems and solutions risks being highly ineffective.

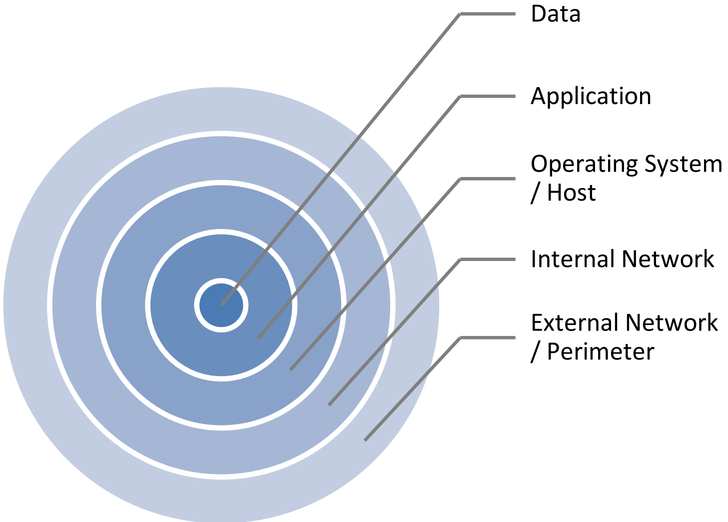


Figure 3. Multiple layers of defense in depth

Process and organization

"Security is a process, not a product", as Bruce Schneier, a renowned security technologist repeatedly affirms [13]. It is hard not to support this position (even if there are several ways of interpreting it). In most cases, just deploying a security measure does not by itself fulfil the security need. Antivirus software won't be effective without virus signature[7] updates. Monitoring systems will be useless (at least for detection) if no one regularly looks at the alarms they generate. Protecting sensitive data at its main storage is ineffective, if other copies of the same data (e.g. its backups, copies in mobile devices) are exposed. Computers that are not regularly patched, and software not updated becomes vulnerable very quickly. Security policies won't be respected unless they are kept up-to-date, and enforced. Doing just a single code review or penetration testing cannot guarantee system or software security, especially as software systems tend to evolve with time. There need to be a process behind every effective, long-lasting security solution.

This is also true on a higher level. For example, risk management[8] by its very definition is a permanent activity, not a one-off effort. The same applies to vulnerability management[9], business

---

[7] Virus signature is a pattern of bytes that can be used to detect and identify a specific virus – it is like its fingerprint.

[8] Risk management is an ongoing process of identifying, analyzing and assessing risks, and then handling and managing them with techniques such as risk avoidance, mitigation, transfer or acceptance.

[9] Vulnerability management is a process of identifying, assessing, prioritizing and fixing computer, software and network security vulnerabilities, in order to make IT environments more secure.

continuity planning[10] or security development lifecycle[11] – they are all ongoing processes. They need to be initiated, started, and then integrated in the business practices of the organization. This means, among other actions, assigning relevant resources and giving enough priorities to maintain and foster security processes.

There are also other ways how an organization can (and should) support its security efforts. They include, for example, motivating people and establishing pro-security incentives. Some possible approaches are described later in this chapter.

Last but not least, people

Computer and information systems are designed, implemented, maintained, used and attacked by humans. And, as it very often turns out, it is people who are the weakest link in the security chain. One study reports that up to 80% of major security failures could be the result of "poor security behaviour by staff", rather that of poor security solutions [14]. Design flaws, bugs in implementations, weak passwords, lax access restrictions, insecure work practices, careless handling of sensitive information, becoming a "phishing" or social engineering victim, intentional abuses etc. are all direct results of human actions. Some can be attributed to simple mistakes or errors, others to negligence or incompetence, and yet others to malicious intentions. Some are easy to avoid or to detect; others are much more subtle or specific. In any case, it's always humans that are behind incidents.

80% of major security failures result from poor security behaviour.

It is time to see in more detail the landscape of the human threat, and various existing ways of addressing that threat.

2.2. Human threats

In risk management people are primarily considered as organization's assets. For example, EBIOS[12] [15] considers people as "support assets" (as they support main business processes). In EBIOS' terminology, people may be affected by so-called "human impacts" that have negative consequences on people's physical security (their health or lives), or on the social environment (collaboration and team work, motivation and commitment etc.).

At the same time, it is commonly understood that humans are not only assets. In particular in the IT world, they are not only creators or users of information and systems, but also potential threats to

[10] Business continuity planning (BCP) means planning and implementing preventive and recovery measures to avoid business disruptions in case of unforeseen events (which are in this context often referred to as disasters).
[11] Security development lifecycle is a process aiming at ensuring software quality and security throughout software development process.
[12] EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*) – a risk management methodology related to information systems security, developed by ANSSI (French *Agence nationale de la sécurité des systèmes d'information*). Version 2010 is available at [110].

their security and correct functioning. Any serious risk assessment must take into account the human threat. For example, Landoll [16] proposes the following human threat agents[13]: insider, executive, management, sensitive position, employee, security force, outsider, terrorist, hacker, ex-employee, competitor, building crew, associate, business associates, customer, vendor, and visitor. In fact, all these people may cause or trigger a threat to happen, either with or without an intention of actually doing something malicious. This important distinction is also recognized by EBIOS, which splits human threat sources into two categories: those acting deliberately and purposefully, and those acting accidentally.

Figure 4. A "certificate problem" security alert from a Web browser

This applies also to information security, with different people being involved at various phases of the information systems lifecycle. In an attempt to categorize how and why humans become the weak link in information security, Schneier [13] discusses "six aspects of the human problem":

- People don't know how to analyze risks, and their perception of risks is flawed;
- People are bad in dealing with exceptions and very rare situations (which may actually indicate an attack or a breach);
- People don't understand security warnings (e.g. such as shown in Figure 4), and can't take correct security decisions;
- People trust that their computers do what they are told to do (which may not be the case for infected computers);
- People easily fall for social engineering tricks;
- And finally, in some cases, trusted people turn out to be malicious and misbehave.

Additionally, people don't want to be hindered by inconveniences of security measures, and will go to great lengths to bypass them.

I will now look at these (and some others) aspects of the human threat in more detail.

[13] Threat agent is "an entity that may cause a threat to happen" [16], for example a malicious person or a natural disaster.

User mistakes and errors

Smith [17] argues that "the majority of well-known major incidents, such as Three Mile Island, Bhopal, Chernobyl [...] are related to the interactions of complex systems with human beings". It is no less true for information systems. The interface between computers and their users is the principal place where mistakes happen. The main reason is that systems are complex and hard to understand, and hence they seem unpredictable. Moreover, people generally do not want to spend time reading documentation, learning how computer systems work and double-checking every action taken. They just want to have their job done, and quickly. Inevitably, some of the mistakes resulting from human-computer interactions do affect security. Examples include wrongly configured access rights, accidentally exposed confidential documents, and important data being unintentionally overwritten or altered. Such mistakes occasionally happen to even most security-conscious people.

Actually, people do mistakes even when performing simple or routine tasks. Human error rates tables (for example in [17]) contain interesting entries. For example the probability of wrongly reading a 10-digit number is 0.6% – but already when calling a 10-digit phone number, this number is wrongly dialled 6% of the time. While of course these probabilities are just very rough estimates, they clearly show that mistakes simply cannot be avoided. In addition, the likelihood of making an error may become much higher in certain unfavourable conditions. Human Error Assessment and Reduction Technique (HEART, [17]) contains estimates that the probability of an error raises when the person is "unfamiliar with infrequent and important situation" (maximum probability multiplier MM=17 – i.e. in this case the probability of error increases by a factor of up to 17) or when there are "no obvious means of reversing an unintended action" (MM=8) – but also with stress (MM=1.3), low morale (MM=1.2) or inconsistent displays and procedures (MM=1.2)[14].

Let's imagine a person who mistypes the URL of an e-banking Web site, ends up on a "typo-squatted"[15] Web site set up by criminals, ignores a Web browser warning about a wrong certificate, and types in his e-banking credentials, thus exposing them to those criminals. This is a typical scenario where a series of user mistakes and errors lead to potentially severe consequences. Surely, everyone makes typos. However, a habit of double-checking the Web site address and protocol (https) before entering passwords on it would help to avoid such traps. So would reading security warnings and correctly acting upon them. (There are also possible technical solutions that can help preventing such a scenario, but we don't discuss them since they are less relevant here.) Unfortunately, most people are not aware of the typo-squatting threat, don't want to be annoyed with security, and tend to ignore security warnings. As a consequence, many do such mistakes, and some become victims of such (or different) attacks.

Understanding security and risks

As we already saw, people notoriously ignore or underestimate risks (*"Identity theft? It has never happened to me"*). They often take wrong security decisions (*"My browser complains about some certificate problems, but I just want to see that Web page, so I click the 'OK' button!"*). And many

[14] Of course, a probability cannot be higher than 100%. If the result of error rate calculations is above 100%, it is assumed that this error will almost certainly occur.

[15] Typo-squatting means creating Web sites with addresses very similar to those of legitimate sites, in hope that some users will mistype the address and accidently end up on a typo-squatted Web site [93].

tend to bypass security measures or to break rules, especially for a seemingly legitimate reason (*"Yes, I know it is forbidden to copy that data on a CD, but I just need to work on it at home tonight"* or *"Of course, passwords should not be shared, but I give you mine, so that you can do what I ask you to do"*).

In fact, researches realize that the perception of security is very often biased ([18], [19]). For instance, people naturally downplay common risks (e.g. driving a car), and exaggerate and fear spectacular but rare risks (like air travel). Same applies to situations that we control (again, driving a car) versus those which we don't control – the former are perceived much less risky that the latter, regardless of the reality. Furthermore, our understanding of risks is strongly influenced by the media, which is not always transmitting a representative and balanced view of (in)security.

Social engineering

Additionally, even if systems are user-friendly and easy to operate, and users are trained and experienced enough to avoid mistakes, they can still become victims of social engineering attacks. It has been repeatedly proven and described in various publications (e.g. [20], [21]) that manipulating legitimate users and tricking them into taking actions they should not take is surprisingly easy. In fact, a talented social engineer will be able to enter guarded premises, learn passwords, get access to sensitive systems, and obtain confidential information without having to attack the technology protecting it. He will use influence, persuasion or threat, abuse people's compassion and tendency to trust and to help etc. – all that in order to deceive them and achieve his malicious goals.

> *A social engineer may get access to a restricted system*
> *without attacking the technology protecting it –*
> *but rather by tricking its legitimate users.*

One of the main reasons why social engineering works so well is simply that people are helpful. They want to be team players rather than "blockers", and will often break procedures and rules just to be able to help someone else who for example sounds stressed and in a hurry. This attitude may actually be useful and productive for the organization, especially if the existing policies and procedures are too rigid or restrictive. But it also makes social engineering attacker's life much easier.

In some cases, attackers will try to persuade victims into directly violating security rules or measures. A most common example is a phishing e-mail that asks the recipient to provide his password "for verification", or else "his account will be blocked". Quite often though, attacks are more subtle. For example, an attacker targets people that have privileged access to a specific system, and attempts to trick them so that they make mistakes when working with that system. Attacker's plan (and hope) is that such mistakes will be beneficial for him, or in line with his attack objectives.

Criminals and malicious insiders

It is also obvious that "computers do not commit crimes – people do", as the saying goes. Indeed, it is important not to forget that attacks and especially targeted attacks (aiming at a particular organization) do not come “out of the blue”. There are always people behind attacks. Their criminal actions are a result of their agendas and motivations. As we will see later in this chapter, understanding attackers’ motives and goals helps establishing a more effective protection and response measures.

Hopefully most attackers are external people, with limited access to, and knowledge of internal systems and processes. Organizations must, however, protect themselves also from the malicious insider threat – the possibility that a disgruntled internal person (an employee, a contractor, a recently fired collaborator) turns rogue and starts abusing the knowledge and access privileges he was trusted with. The main reasons for this happening are “revenge, fear or greed” – and malicious insider attacks are inevitably on the rise during economic hardships, when more people fear or experience dismissals [22].

One of the most spectacular cases of a malicious insider breach that happened recently is the data theft at HSBC Switzerland private bank, confirmed in early 2010. A former employee managed to steal details of as many as 24,000 accounts of the bank’s wealthiest clients, and passed them to the French tax authorities [23]. This data can be used by governments to identify their citizens who evade taxation by keeping fortunes on their private Swiss bank accounts. Very similar data theft has happened lately to at least one other Swiss bank. Of course, such incidents are disastrous for the reputation of the whole Swiss private banking sector – traditionally known for the confidentiality of their services.

2.3. Addressing the human factor

As we have seen, humans are in fact behind all security incidents, both as users or victims and as attackers. And many types of incidents cannot be prevented with technical measures or solutions only. It is therefore clear that no information security management programme or activity can afford to ignore the human aspect of security.

This presumption is now commonly accepted. It became the theme of events such as “Human Factors in Information Security” conference [24] (held for the first time in February 2010), “Human Aspects of Information Security and Assurance” symposium [25] (organized since 2007) or “Security and Human Behaviour” workshop [26] (since 2008). It is also the subject of a few books, including David Lacey’s “Managing the Human Factor in Information Security” [19].

There are a big number of possible security practices or measures that address the human threat. We will discuss some of them in the rest of this chapter. The goal is not to make a comprehensive compendium of all possible measures, but to present a variety of practices and solutions – the general landscape – and briefly describe their advantages and drawbacks. As always, the choice of measures to be implemented in a given organization will depend on the needs, costs and perceived risk levels. For instance, a financial institution that handles money will have to care more – and spend more – than an industrial factory or a university.

It is worth adding that while humans pose threats to information systems, they are also naturally placed to protect them. People can, and should act as a defense line, as well as be engaged in detecting security problems and responding to them. In many areas, if properly encouraged, motivated and trained, they will do better than technological security measures. Why? Because unlike computers, people can adapt and improvise, learn on the spot and have good intuitions or feelings. This means that security programmes should consider people not only as a threat, but also as part of the solution. As Schneier puts it, "a good security system leverages the benefits of trusted people, while building counter-measures to prevent them from abusing that trust" [18].

Policies and procedures

The obvious first step in dealing with the human element of security is defining what people are actually allowed to do, what they are expected to do, and what they must not do. This may take form of acceptable use policies (AUP), organization's information security policies, or computing rules. Such documents usually specify security needs of a system or an organization, define the scope (only employees? or maybe contractors and users as well?), describe the rules, clarify responsibilities, and mention possible consequences.

There are many sources that propose guidelines for developing effective security policies (e.g. [27]). Policies must be short enough to be readable and written in a clear, understandable and engaging language. They should be implementable and enforceable (and actually enforced). They'd better be kept up-to-date. And they need to be communicated effectively to those expected to read and follow them.

Similarly, employees should be equipped with documentation and procedures that help them carrying on their tasks (especially those repetitive or sensitive) and responding correctly in emergency or exceptional situations. As with policies, procedures should be clear and easy to follow, also under stress conditions.

Establishing policies and relevant procedures is essential, but the problem is that many people simply don't read nor follow them. There are several reasons for that – one being that policies are often too generic (e.g. *"information must be protected"*), and not directly applicable to everyday's work. Or, on the contrary, they are too technical and therefore out of date as soon as the technology changes. Moreover, rules tend to be imposed without explanation of why they are established. Finally, if a given rule is unreasonable, not justified, hard to implement and/or not enforced, it will inevitably be ignored.

The problem with procedures, on the other hand, is that people usually prefer taking shortcuts rather than following them step by step. In addition, in emergency situations, when some advice on how to react would be very handy, it often turns out that documentation is not really up-to-date or misses some crucial piece of information.

Work organization

The next step in addressing the human factor of information security is to organize security management. This should not be limited to those working full time on security. The goal is to define clearly security roles and responsibilities across the organization – including the executive board, business management, IT people, internal users and even external customers when relevant [19]. People on all levels should understand what they are expected to do, what they must not do, and what cases to escalate – and be given sufficient authority to do so (e.g. [28]). In other words, information security should not be just left to individual initiative.

Another way how work processes can be organized to support security is to enable consistent reporting of incidents, near misses and exceptional situations. Each of these could indicate an attack, abuse or breach attempt. “There is no such thing as an isolated incident” – behind each major incident there are usually dozens of minor incidents, hundreds of near misses and thousands of bad practices [19]. Being able to monitor and correlate such events allows for detecting problems and investigating their root causes[16] – possibly before a major related incident happens.

Awareness raising

Establishing security policies and defining roles must be complemented by actually enabling people to act and behave securely. That means making them aware of the threats, attacks and risks that a given organization faces; and educating them how to avoid or mitigate those. Otherwise many employees will keep assuming that information security is taken care of by a “security department”, and that they don’t need to care about it themselves.

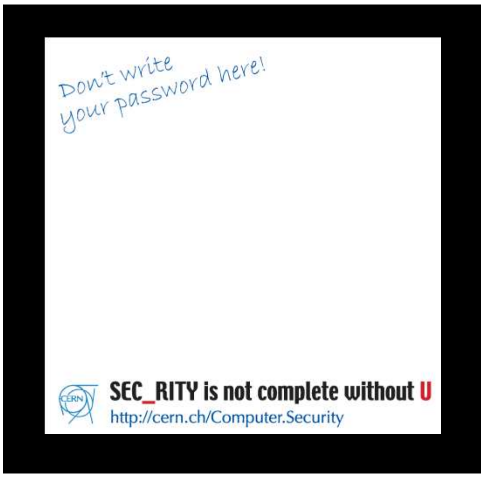


Figure 5. Computer security post-it notes at CERN (idea adopted from Fermilab)

Raising security awareness is usually the first thing that comes to security managers’ minds, when they talk about the human factor. Indeed, it is important not to neglect it. It is, however, not that trivial to do it right.

First, the content of the awareness programme must be based on the analysis of key problem areas, and main root causes of incidents. It must correspond to risk assessment results. At the same time, a single awareness campaign cannot possibly address all security issues that an organization faces. A prioritization is necessary – it is better to pass well just some of the messages than to flood audience with too much content. Main messages or slogans should be short and catchy enough so that people retain them. In general, security awareness raising should be considered a continuous and sustained effort, since the technology is constantly evolving, and consequently threat landscape changes rapidly as well.

The communication needs to be attractive and has to stand out. Awareness campaigns too often boil down to hanging a couple of posters and giving one or two presentations. But more can be done. Using different means such as videos, games, quizzes, and giveaways makes it more likely that the message will be appealing to each of the different people it is targeted at. Making security

[16] This approach is actually similar to concepts behind ITIL’s Problem Management process. This process “aims to resolve the root causes of incidents and thus minimize the adverse impact of incidents [...] and to prevent recurrence of incidents” [111].

communication visual and vivid, positive and entertaining, and associated to what people already know (e.g. places, situations, objects or feelings) helps them notice and remember it [19]. As an example, some of the security awareness materials used at CERN are shown in Figure 5 and Figure 6.

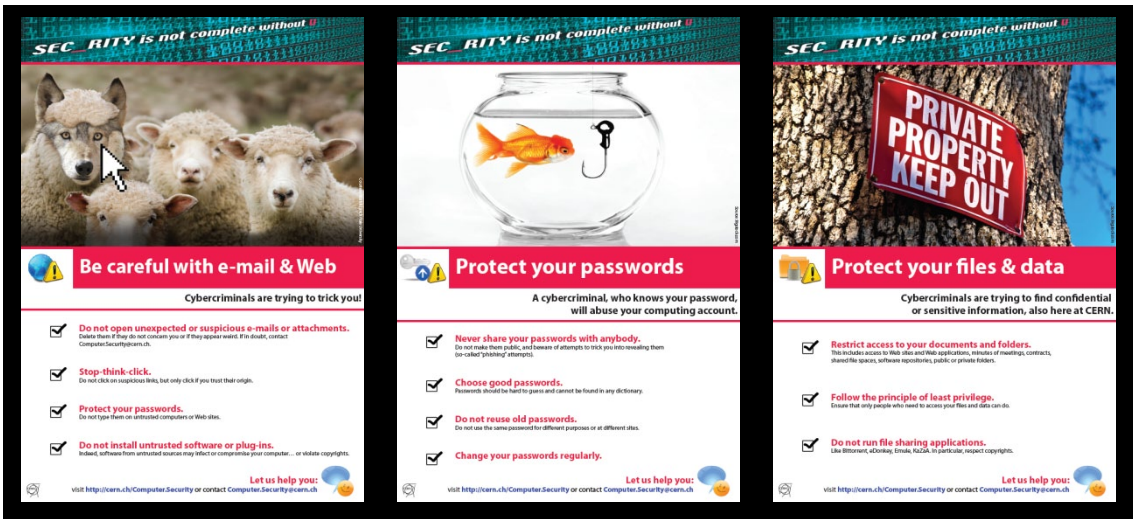


Figure 6. Computer security posters at CERN

Big organizations may go as far as investing in producing dedicated awareness films. On the other hand, many smaller organizations will not have enough resources to develop their own security awareness content, nor to outsource those efforts. The solution is to use publicly available materials, developed thanks to initiatives such as Information Security Awareness Forum [29] or OnGuard Online [30] – or offered by other national cyber awareness programmes[17]. The risk, though, is that external messages will not be tailored to the needs of the organization, and thus will be only partially effective. Any external content should be adjusted, and adapted to the internal audience.

Some authors (e.g. [31]) believe that staff awareness is actually *the* answer for the human threat. Although I think this view is probably too narrow, I agree that raising security awareness among employees, collaborators and users is absolutely essential.

Education and training

Awareness raising efforts should be addressed at the whole population of computer users. On top of this, people dealing with sensitive information systems need to be specifically trained to do that securely – in order to limit the number of security-related mistakes, understand security consequences of their actions and avoid falling for social engineering tricks. This is still true for users, but also those who create and operate computer systems (i.e. architects, designers, developers, testers, system administrators etc.). In particular software developers should imperatively follow courses of software security, relevant to their programming language, platform and application type. Otherwise operating systems, software and especially Web applications will continue to be the vulnerable and commonly exploited, as they are now. Training developers isn't the only remedy to software insecurity – it is, however, an indispensable one.

[17] Many such programmes are listed for example in Information Security Awareness catalogue published by ENISA [112].

Training and awareness activities should be organized together with education departments of the organization – "to target training programs in the most effective possible manner" [32]. A security course should contain more than a list of "do not do this" points. The best is if training is creative, related to work – and if it manages to engage participants. As always when conveying ideas, it is useful to build up on real-life examples – in this case on examples of security incidents that actually happened in the past. Analogies also help understanding abstract concepts – and most popular analogies are those to driving, cars and road traffic.[18]

The problem with training and awareness messages (as well as with policies) is that many people just either ignore them, or easily forget them. Among various reasons for that, the main one is that people are generally flooded with information – e-mails, media messages, advertisement, the Web etc. – and learned to filter out everything that is not immediately and directly applicable for them. We all have to do so; otherwise we couldn't survive in this "information-rich world" [19]. Furthermore, many computer users see inconveniences but no benefits of following security advice (that is, until they suffer from a security incident that could have been avoided). One security researcher even suggested that "users' rejection of the security advice they receive is entirely rational from an economic perspective" [33], because the inconvenience and burden of following security recommendations far overweighs the direct costs of potential incidents. This is where awareness raising helps – once users understand the threat and risk landscape, they can make better decisions.

Technology

This chapter started with a claim that technology cannot solve all security problems – because of the human factor. At the same time, technology can in fact help addressing the human threat. As we saw, one of the major causes of security incidents is user mistakes (accidental, caused by negligence, or triggered by attackers). The obvious – and correct – mitigation technique is to design and implement systems so that they are easy to use and hard to make mistakes with, don't require users to take difficult security decisions, and possibly detect their mistakes and propose corrections. Simply speaking, software usability matters for security.

Technology should be designed
to help users avoid mistakes,
and to correct their errors.

Technology may also help to reduce other human-related risks. For instance simple phishing attacks, aiming at stealing user passwords, are no longer a threat if hardware tokens or biometry solutions (e.g. fingerprint readers) rather than passwords are used for authentication and access control.

Another example how technology can help is employee on-line activity monitoring. Such monitoring may be limited just recording anonymous activity patterns – thus keeping privacy, and still allowing incidents to be investigated if needed. There are also more intrusive or sophisticated techniques,

[18] For example "security is locking your car, while safety is having air bags" or "software industry is now where car industry was in 1920s – it will take you where you want, but it fails often and in dangerous ways".

such as detecting and reporting – or even blocking – network activity that constitute policy violations (e.g. accessing on-line gaming Web sites during working hours). Of course such practices must be in line with local legislation, which in particular often requires that employees are informed. Network monitoring works well as a deterrent: if computer users know that their on-line connectivity is surveyed, they are much less likely to engage in illegal or not tolerated activities.

Preventing fraud and abuse

Most of the security measures addressing the human factor that we discussed above do not protect organizations from a malicious insider activity. This threat requires a different set of counter-measures. On the technical level, effective audit and fraud detection is certainly one of them – and it is often advocated to achieve it by monitoring user activities at various points and correlating results [34]. On the human level, insider threat counter-measures include, among others, doing pre-employment background checks (screening), monitoring employee motivation and stopping incentives for fraudulent actions or behaviours. On the work organization level, abuse and fraud can be prevented by establishing segregation of duties, "two-person" control[19], job rotation or mandatory vacations (so that everyone is sometimes replaced by someone else) and "watching the watchers"[20] practice.

Even if "every security system needs trusted people to function" [18], that trust should be diffused "to limit the amount of damage one person can do" [13]. Organizations try to minimize the number of trusted people, and to limit how much the organization needs to trust them (following the "need-to-know"/least privilege principle). Rewards and sanctions should be balanced so that there is more to lose than to gain from abusing trust. Being consistent in investigating and publicly prosecuting fraud is also a very powerful deterrent [19].

At the end of the day, the goal is to employ honest and trustworthy people, eliminate incentives and opportunities for abuse or fraud, and minimize likelihood that they stay undetected.

Additionally, it is useful for security managers to know why attackers would target their organization. Understanding criminals' motives and emotions – and incentives that drive them – helps better prioritizing organization's response to criminal threats, both internal and external.

Promoting secure attitude and behaviours

We discussed a big variety of different approaches to address the human threat. Some are more effective (and cost-efficient), and some are less. Some are rather technical; others are more "soft". There is, however, an interesting common characteristic among them. Except for measures that address the malicious insider threat, most aim at ensuring that humans *do not* make security mistakes, and *do* care about security. In other words, organizations that employ these measures want their employees to adopt pro-security attitude, and behave securely. But wouldn't that be much simpler to achieve if people were actually motivated to do so?

[19] Two-person control means that (at least) two people are needed to complete an action, e.g. opening a safe, launching a nuclear weapon – or controlling cinema access (one person sells tickets, another controls them).
[20] "People watching people watching people" approach can be best observed in casinos, where "dealers watch the players, floormen watch the dealers, pit bosses watch the floormen, and surveillance watches the pit bosses" [13].

Of course, the answer is yes. People's motivation is a very important driving force. It is no surprise that successful managers put considerable efforts into motivating their subordinates – one way or another[21]. Motivation directly affects our work performance. It shapes the way we think and feel about our jobs. It nourishes our commitment to employers. And probably most importantly for security: it makes a difference between doing things well – and "just" doing them. This is exactly where secure attitudes and behaviours are either embraced – or rejected.

Employee attitude and behaviour are really the key concepts here. Unfortunately, they are equally hard to influence [19]. An organization cannot simply transform people's attitudes to their wish – but it may try to influence and fuel a desired behaviour change. One of the ways is to create incentives for people to act securely and to use correctly security features or solutions. Likewise, employees' work should be organized in a way to encourage and motivate them to take active part in protecting organization's assets. Rewards and punishments also work, although to a limited extent (and punishment may be demotivating). When eventually employees' behaviours and attitudes develop as desired, we can call it a culture change. And this is actually the *real* objective: establishing and sustaining an organizational culture that accommodates security values.

Organization's best defense
is a culture of security.

In fact, everybody now seems to be talking about security culture. Half of delegates to the first "Human Factors in Information Security" conference [24] see cultural change within organizations as a must, and *the* way to address the human element of security. Consulting and audit companies also believe that "organization's best defense against internal and external breaches [...] is a culture of security – a mindset on the part of every individual so that actions in support of information security become automatic and intuitive" [35]. It appears that security culture change is the Holy Grail of information security, its elusive goal, the key to success.

It is the right time to see how this can be achieved.

[21] Fear (e.g. of losing, being ridiculed, penalized, fired etc.) is a "negative motivation" factor [113].

Chapter 3. Security culture and culture change

3.1. Organizational culture

Definition

Let's start by actually trying to see what "organizational culture" or "corporate culture"[22] really is. This concept is not trivial to define – and, not surprisingly, there are many definitions of it. Schein [36] defines the culture of a group as "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems". For other authors, corporate culture is "the social and political environment in which people work" that "is reflected in everything that occurs in the organization—from the way people greet each other in the morning to the way they behave in meetings to the way decisions are made—and it affects every aspect of the business" [37]. A common definition mentioned by various authors considers organizational culture as patterns of shared values and beliefs that over time produce behavioural norms adapted to solving problems.

The notion of culture being formed as a result of a group of people having to solve problems together is prevailing. One source explains that "as groups evolve over time, they face two basic challenges: integrating individuals into an effective whole, and adapting effectively to the external environment in order to survive. As groups find solutions to these problems over time, they engage in a kind of collective learning that creates the set of shared assumptions and beliefs we call culture" [38].

> *"Organization culture is what people do when you're not watching them."*

But, perhaps, a more simple way of defining organizational culture is seeing how people would describe it in ordinary words. Some would say that the corporate culture is "how we do things around here". Lacey [19] proposes using a comparison: "If the organization was an animal, which one might it be?", and quotes a very simple but surprisingly accurate definition: "organization culture is what people do when you're not watching them".

---

[22] Some sources – e.g. [95] – make a distinction between organizational culture and corporate culture. Since the distinction is not relevant here, I will use these terms interchangeably.

Building blocks

It is interesting to look inside the concept of organizational culture, and see what its building blocks are. Culture is certainly made up of shared values, attitudes and assumptions. Likewise, beliefs, perceptions, behaviours and norms are very often mentioned in this context. Elements of culture of a group of people may also include expectations for group member behaviour, customs and rituals, stories and myths about the history of the group, "shop talk" (typical language used), climate (the feelings within and around the group), as well as metaphors and symbols [38].

Schein [36] proposes to consider different levels of culture (Figure 7). The most visible is the level of artifacts: symbols, physical environment, language, clothing, observable rituals etc. The next level is that of espoused beliefs and values. Finally, the innermost is the level of underlying tacit assumptions that are non-negotiable and taken for granted.

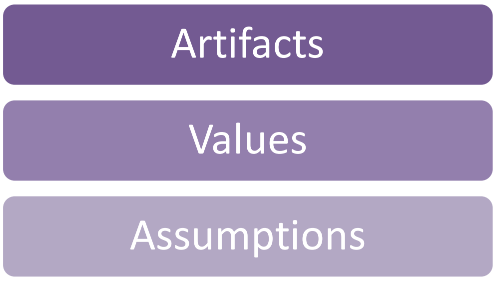


Figure 7. Schein's layers of culture (from visible to underlying)

Knowing these building elements makes it easier to analyze the culture of an organization. This can be done by observing common behaviour patterns, values and beliefs, and personal attitudes and assumptions (e.g. what people find acceptable or unacceptable) [37]. On the other hand, deducing values or assumptions based on observations may be flawed – also because interpretation is often affected with observer's own assumptions. For example, relaxed clothing habits could indicate that employees don't feel attached and "don't care". Or it could indicate that the company is young, "cool" and innovative, and employees consider it fun to work there. Or maybe yet something else. For this and other reasons, deciphering and assessing culture of a given organization is harder than it may seem.

Interestingly, behaviours are actually not mentioned in some of the definitions that we saw. Their authors argue that behaviours are determined by values, attitudes and other elements that constitute a given organizational culture. "Underlying the observable behaviours of people are the beliefs, values, and assumptions that dictate their actions" [39]. In other words, behaviour is seen by some as a manifestation of a culture, but not really a part of it. This could explain why employee behaviour may be influenced – especially over a short period – without having to alter the corporate culture. Any long-lasting behaviour change, however, needs to be sustained by a change in people's values, attitudes and assumptions – in short, by a change of culture.

Values

As we saw, organization values constitute a very important component of the culture. They can be divided into two basic types: core values and espoused values [40]. Core values "define the ways a business is conducted" – they are "reflected in the way individuals actually behave". Espoused values, on the other hand, are the explicitly stated values that an organization believes in and claims to hold. In short, they can be translated to ‘‘what we are’’ and ‘‘what we want to be’’, respectively.

Espoused values are typically stated in writing and widely communicated (both internally and externally), along with organization’s mission, vision and strategy. They are also often a starting point for documents such as a code of conduct. It is important, however, that they do not contradict with the core values of staff members. Moreover, they have to be reflected in management’s actions and behaviours – including during crisis times [37]. A gap between stated and observed values is highly demotivating. Not adhering to publicly advertised values is counter effective – it would be better not to express them in the first place. Let’s imagine managers in an organization who promote a “no blame” attitude, and at the same time look for a scapegoat as soon as a major incident occurs. It should not come as a surprise that individuals in that organization will simply ignore the “no blame” value and will consider it dead, however strongly it is advertised.

Different corporate cultures

Culture of an organization is at the very core of its identity. Its impact on employees is significant – it dictates to a large extent how they behave, interact, and work. Corporate cultures often reflect organizations’ *raison d’être* [41] – that can be implicit or explicit (stated in the vision, mission or strategy). Having those points clearly defined can have a direct effect on employee motivation and commitment, as people are naturally motivated if they know where they are heading and why.

Each organization is different, and consequently their cultures vary a lot as well. A large multinational corporation, a non-for-profit research institution, a private bank and a hospital will all have different cultures.[23] Apple, for example, is known for highly innovative culture, but also for its “notorious secrecy” [42] – and it seems that this culture contributed to Apple’s remarkable market position. Similarly, Toyota has reached no. 1 car maker position by following its famous “Toyota Way” – which is in fact a both a declaration and a description of company’s culture based on two basic principles: “continuous improvement” and “respect for people”[43].

Organizational cultures can be not only the base for rapid growth, but also a reason for decline. Many believe it is General Motors’ staid and “corroded” corporate culture that caused great inefficiencies resulting in its near bankruptcy in 2009 [44].

An interesting question is whether an organization can have just one, or several cultures. It can be observed that inside large organizations there are often variations – sometimes substantial – in assumptions, behaviours etc. Subgroups manifesting them have in fact their own subcultures [36]. This is especially true if the overall culture of the organization is weak [45].

Culture models

There are several models that try to categorize different culture types. For example, in his famous study carried on in 1970s in multiple countries worldwide, Hofstede analyzed five cultural dimensions (illustrated in Figure 8): power distance; individualism; masculinity; uncertainty

[23] We can also see a clear difference between these different organizations when it comes to risk perception and risk management. For example, an occasional loss of human life is absolutely intolerable in a private bank, while it is to some extent inevitable (and therefore accepted) in hospitals.

avoidance and (later) long-term orientation. He observed significant (and stable) differences in these cultural dimensions between different nationalities [46].

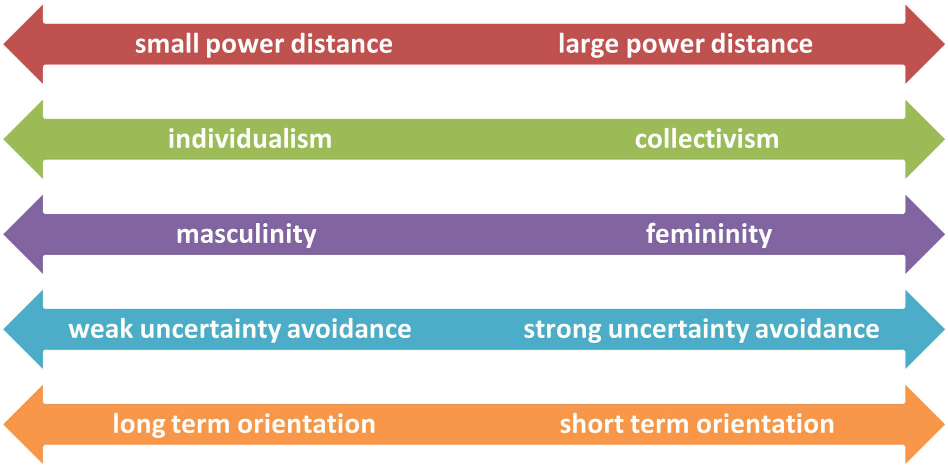


Figure 8. Hofstede's five cultural dimensions

Another categorization was proposed by Sonnenfeld in 1988 [47], when he defined four corporate culture types: the academy (exposing members to different jobs so they can move within the organization); the club (which is concerned with people fitting in); the baseball team (with its well-rewarded stars who leave for better opportunities); and the fortress (concerned primarily with survival) [48].

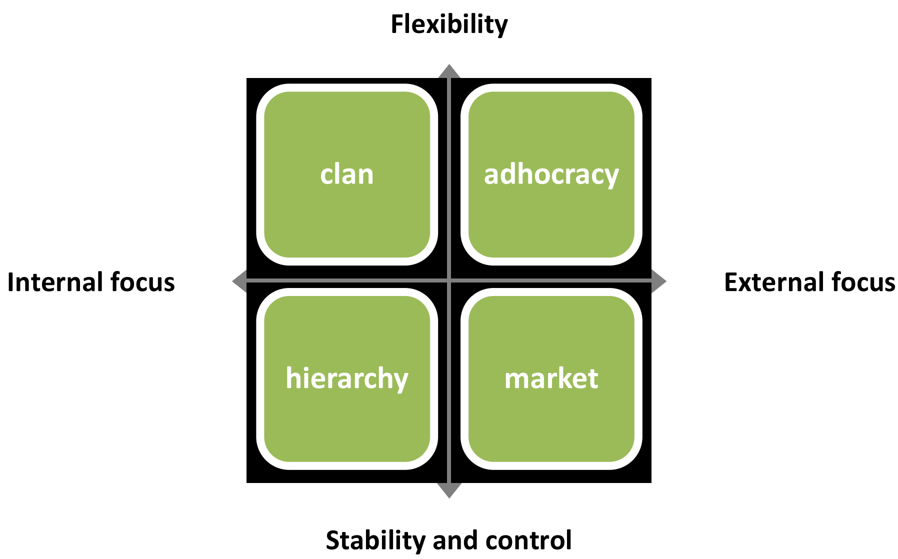


Figure 9. Types of organizational cultures according to Cameron and Quinn

This model was followed by an organization culture framework developed in 1999 by Cameron and Quinn [49]. This framework, based on Competing Values Framework, proposes evaluating[24] organization's position on two independent axes: internal or external focus; and flexibility vs.

[24] Organizational Culture Assessment Instrument (OCAI, available for example at [96] is a useful tool for classifying organizational cultures according to Cameron and Quinn's model.

stability and control (Figure 9). Depending on where a given organization is situated on these two axes, it falls into one of four main types: a clan (internal focus and flexibility); a hierarchy (internal focus, and stability and control); an adhocracy (external focus and flexibility) or a market (external focus, and stability and control).

These and other[25] corporate culture models mention several culture characteristics that are actually quite relevant for security. A direct communication between subordinates and superiors, for instance, makes it much easier for lower-level employees to point out security inefficiencies or weaknesses they observe. Another good example is that a flexible organization will react better to innovative or bottom-up security initiatives, while imposed policies and procedures will be more effective in a hierarchical organization. Information security managers that are aware of such characteristics of their organizations may indentify more precisely sources of human-related problems, and better adapt their security procedures, processes and communication.

3.2. Security culture

What is security culture?

We concluded from Chapter 2 ("Human aspects of information security") that the way to address most of the human-related threats is to have a sound information security culture. The goal is to develop and maintain an organizational culture where people integrate security practices into their everyday working habits, and each person contributes to security of information assets by his or her actions. Proactively protecting information and computing resources, and being vigilant and aware of threats and risks should be considered an essential part of professionalism. Opposite behaviours (e.g. negligence or carelessness) should simply be shameful.

Information security should be "the second nature to all employees" [50] – so that it unconsciously becomes a natural aspect of their daily activities [51]. This must not be limited to end-users only – but should also include management on all levels [52]. In this ideal world, employees understand value of information and assume personal responsibility it; decisions taken by management (e.g. for launching a new project) take into account risks and security issues; everyone knows how to react when observing or suspecting a security breach; and desired security behaviour (such as reporting policy violations) is recognized and rewarded.

Information security should be
the second nature to all employees.

A strong and mature security culture "will emphasize the fact that each employee is a valued participant in preventing data breaches", and not a potential abuser that needs to be monitored [53]. Preferably, employee adherence to information security policies and procedures is intuitive rather than enforced [54].

[25] There are many other models or categorizations for corporate cultures. For example, [97] lists as many as 10 main types of organization structures, among them "work hard/play hard" and "bet your company" cultures.

It would be unreasonable to expect that employees will massively adopt what Schneier calls a "security mindset" [55] – thinking about security "outside the box", as an attacker. Similarly, it is probably unrealistic to hope that each employee becomes "a Security Deputy", as some researchers advocate [56]. However, having most of organization's staff and management vigilant, risk conscious, and naturally following good security practices is certainly something desired, and at least partially achievable.

OECD[26] highlighted "the need to develop a culture of security" already in 2002. "Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks"[27] [57]. However, still very few companies or organizations can claim to have satisfactorily embedded information security into their organizational cultures. This is a journey, and a long one.

Towards a security culture

It takes parents quite some time, but most of them finally manage to teach and convince their children to look left and right before crossing a road – even if children would naturally rather just run across. Likewise, using seatbelts gives car passengers additional safety, but is also inconvenient – and so people didn't use them widely at first. However, road safety campaigns repeatedly explained and demonstrated how seatbelts can save lives; governments made using seatbelts obligatory and enforce it with fines; and car makers install alarms that sound when passengers don't fasten their seatbelts. As a result, it becomes more and more natural for people to fasten seatbelts – even if this wasn't at all the case a decade or two ago. Sure, it is a behaviour change, but also a change in beliefs and risk perception – so in fact, it's a culture change.

Similarly, developing an information security culture on an organization is a long process that has to be pushed with policies, awareness raising, motivation and encouragement, and technical solutions. It can be considered that information security culture is well established when senior management supports and is involved in security management; security responsibilities are assigned; information security policies are enforced; ongoing security awareness measures are in place; security training is regularly conducted; and security budget is adequately allocated [58]. We already discussed most of these points in section 2.3 ("Addressing the human factor") – and indeed, they all need to become reality. But as we saw earlier, establishing security culture requires a deeper change: in people's assumptions, beliefs and values. If employees aren't aware of, or underestimate threats and their consequences, they will never fully adopt secure work practices.

In fact, the biggest difficulty when attempting to establish a security culture that organizations don't believe that security is important [59]. As numerous researchers have pointed out, significant security initiatives are usually started in the aftermath of major incidents. Unfortunately, only when something wrong happens, security starts to be taken more seriously.

---

[26] Organisation for Economic Co-operation and Development.
[27] See also OECD's nine principles of security culture [57].

Security needs across industries

Industries have different security risk profiles – and consequently they differ in terms of their information security needs [60]. For example, financial institutions are a natural target for profit-driven cyber criminals. Because money is directly at stake, they tend to invest more than other industries in information security activities, programmes and measures. On the other hand, manufacturing companies simply have less information and computing assets to protect, and therefore require less investment into information security [61].

At the same time, financial organizations were at risk since their conception, well before they started using information systems. As a result, the notion of security is well integrated in such organizations, its people and its processes; and caring about security is already part of their culture. In a bank, for example, measures such as guards, bars, or "two-person" control are hardly a surprise for managers, employees or clients. This means that promoting information security awareness and fostering information security culture may in fact be much easier there, than in organizations where security is an entirely alien concept.

Security as a corporate value

Accountability, collaboration, excellence, innovation, integrity, respect, and many others are typical corporate values [62]. Should security be one of them? In other words, is it worth to establish and promote security as a corporate value, and build the corporate culture on it?

That, of course, depends on the type of the organization, on its industry, and on its business model. It may be desired in organizations that are particularly exposed to security risks; or in companies that operate in safety or security industry. Quite naturally, security is the first of four corporate values for Microsoft's Trustworthy Computing initiative [63]. Similarly, safety is listed among the core values of the New York City Fire Department [64].

> *While security is rarely one of the corporate values, it should be mentioned in documents such of the Code of Conduct*

On the other hand, most companies do not list security among their core values – even if they take security very seriously. Probably the main reason is that adherence to security doesn't directly generate income – at least not in the same way as innovation, excellence or client orientation does. I believe that this approach is justified – security, although often correctly considered as very important, is hardly ever crucial to the point of making it one of the few organization's values. Additionally, security is more a concept than a quality. That is perhaps why it is not mentioned among corporate values of companies operating even at the core of security industry, e.g. Securitas [65] or Xe Services[28] [66].

Probably the reasonable solution in most cases is to emphasise the importance of security in a different way. For instance, UBS' Code of Conduct highlights company's commitment to "adhering to the highest standards of information security" in order to protect "client confidentiality" [67] –

[28] Formerly known as Blackwater.

both to direct employees and to reassure clients. Similarly, Cisco states that “information security policies are integral to [its] Code of Business Conduct” [68].

3.3. Culture change

Culture is more that behaviours

We already mentioned that changing staff behaviours is possible. Even if employees are not happy with what is imposed, and wouldn’t naturally behave that way, they can be commanded. And they will usually obey, especially if consequences – both positive such as rewards and negative such as punishment – are personal, immediate and certain [19].

Their values, assumptions and beliefs, however, are much more difficult to influence. Assumptions are on the most personal level of Schein’s culture levels model discussed before. They are, as axioms in mathematics, very often taken-for-granted and non disputable, and therefore extremely hard to alter. People get anxious and feel unsafe when their assumptions, beliefs or attitudes are challenged or questioned – and will naturally oppose. In fact, only when people discover something themselves, they change their assumptions and attitudes accordingly.

This means that organizational culture is very difficult to change. Culture cannot be directly modelled. It *may* react to certain change initiatives and efforts, although not necessarily precisely in the way it was hoped. Additionally, changing corporate culture is “like turning an oil tanker” – it takes a lot of time; and past experience certainly helps. A culture change cannot be simply planned and executed - it requires major time and resource investments.

Change management

Three different orders of cultural change can be distinguished [69]. In first order change, the existing culture changes incrementally – making the transition slow but gentle. In second order change, change agents (those who plan and pilot the change) attempt to replace the existing culture with a new one. Third order change happens then group members see the need for a change and implement it themselves.

Any major change in an organization – like a second order change – inevitably triggers concerns and even opposition from many of the employees. At the same time, there will always be others who actually do support the change and want to be part of it. When managing a change, and guiding an organization through the transition process, a successful approach means including as much as possible the supporters, while trying to convince the doubtful, and neutralising or separating those who still oppose.

In his famous book on change management [70], Kotter discusses eight change process phases that are all a natural part of any successful change initiative. They need to be correctly planned and implemented. Skipping any of the steps, although may seem tempting, “creates only the illusion of speed and never produces satisfactory results”. These phases are:

- Creating a sense of need and urgency;
- Grouping a team of enthusiastic supporters and early adopters;
- Developing a compelling vision;
- Communicating effectively that vision and the corresponding strategy;

- Empowering people on all levels to act;
- Celebrating quick-wins;
- Consolidating efforts and keeping the momentum (rather than declaring victory too soon);
- Making changes sustainable and permanent by institutionalizing them.

These eight steps can be mapped to six guidelines for cultural change proposed by [71]: formulate a clear strategic vision; display top-management commitment; model culture change at the highest level; modify the organization to support organizational change; select and socialize newcomers and terminate deviants; and develop ethical and legal sensitivity [72].

Leading a culture change

It is believed that a culture change requires strong leadership, rather than just management skills and techniques. Some even say that "the unique function of leadership that distinguishes it from management and administration is [the] concern for culture. Leaders begin the culture creation process and [...] must also manage and sometimes change culture" [36].

A successful culture change requires strong leadership.

Not only leaders and top management need to initiate the change process, but also they have show their support and commitment throughout the transition period (and also afterwards). Since cultures don't change overnight, a certain level of patience is needed. If those who pilot the change start to get frustrated with its slow progress, and express their disappointment ("Why haven't you yet..."), they may actually trigger additional resistance from people in the organization, that will slow down the process even more [73]. Simply, people need time to change.

And people need time for a neutral phase in the transition period. This is when they have already accepted that the previous culture will be gone, but haven't yet embraced the new one. In a security culture transition, the neutral phase is a good moment for engaging employees in redefining security requirements, and in reviewing policies and procedures [74].

Additionally, it is crucial that good example comes right from senior managers. When trying to introduce security culture, they should follow security procedures and practices as any other employee. They should lend their names and rank to support security initiatives. If, on the contrary, they actually tend to bypass security controls to get their job done (or just because it is more convenient), not surprisingly other employees will not hesitate to do the same.

At the same time it should not be forgotten that because culture is a sum of common assumptions, values and behaviours, and because it results from social interactions, it "cannot unilaterally be created and manipulated by management" [75]. In a way, the culture change has to come from the concerned people themselves. They are likely to accept or even trigger the change only when the inconvenience related to the current culture, and the desire for having the new culture combined together are bigger than the perceived cost of the change [37].

Chapter 4. A different approach for security culture change

4.1. A non-urgent need

As we saw in the previous chapter, a major culture change needs to be justified with real urgency, and requires strong, top-level leadership. In particular, an organization may hope to be successful in introducing a security culture, if there is a widely understood and urgent need (e.g. major recent incidents, new regulatory requirements), and top leaders are personally and directly engaged in piloting the change throughout the whole transition period.

Quite often though, a culture change is desired or even necessary, but the need for it is not widely recognized and not urgent. This is typically the case for organizations lacking security culture. Let's imagine an organization where information security staff observes many security incidents. For instance, confidential information is accidently published on public Web pages; computers and data are missing basic protection (e.g. patches) and recovery (e.g. backup) measures; software developed in-house is too often vulnerable; and some users still respond to "phishing" attacks and divulge their passwords. Such incidents could have been prevented if computer users better understood threats and risks, and behaved more securely. Or, in other words: if security was part of the organizational culture. Unfortunately, as long as impact of such incidents stays relatively minor, organization's leaders do not feel too worried or concerned. Only when a seemingly similar incident happens to have major consequences, it raises awareness among decision-makers, and triggers additional security initiatives. But, of course, the good practice is to prevent major incidents – for example by establishing security culture – rather than to react to them afterwards.

Can culture be effectively influenced by some other means, by people other than top management? In particular, can we embed security – its needs and its solutions – into an existing culture before the need becomes really urgent? How to do it without starting a heavy, full-blown change process and without engaging top-level leaders?

In fact, establishing security culture doesn't necessarily require remodelling completely the existing culture – but rather adding the notion of security to it. Moreover, I believe that this can be achieved without using heavy, intrusive, top-down or costly measures. The proposal below describes how.

4.2. The proposal: gradually building security knowledge, awareness and behaviours

The proposed approach is to build security knowledge and awareness, and to influence behaviours gradually and increasingly, by surrounding people with relevant security messages and advice. These messages should not be too intrusive (and therefore annoying). They should, on the other hand, be pervasive. The way to achieve this is to embed security messages in processes that already exist (e.g. cover security in existing training courses), rather than creating new processes (e.g. introducing dedicated security courses).

One of the trends observed in modern organizations is that their personnel boundaries become less and less sharp. There are, of course, those directly employed. At the same time most organizations will also face a constant flow of temporary staff, contractors, visitors, external but trusted users, outsourced staff, consultants etc. Standard top-down measures – such as obligatory courses, contract amendments, or awareness raising campaigns – are likely to miss many of these groups. Embedding security messages into existing processes, however, makes it more likely that different people will see or hear them.

The proposed approach is to build security knowledge and awareness,
and to influence behaviours gradually and increasingly,
by surrounding people with relevant security messages and advice.

Additionally, these security messages and advice should be directly applicable whenever possible. This can be achieved by automatically suggesting secure actions and behaviours related to person's current work activity. For example, when someone requests creation of a new Web site, the confirmation e-mail he receives should contain relevant security advice such as how to manage access rights and how to develop secure Web applications.

Planting pervasive security messages in work environment has two positive effects: it promotes secure practices and behaviours, and – even more importantly – it builds security knowledge[29] within the organization. The ultimate goal, and hope, is that this acquired knowledge will influence people's assumptions, beliefs and values concerning risks and security – and will therefore contribute to security culture change.

From the three change orders mentioned in section 3.3 ("Culture change"), this approach combines first order change (incremental and gradual) and third order change (coming from members of the group themselves), avoiding second order change (an imposed change, which is expensive and hard to implement successfully). Nonetheless, as in any change process, factors already discussed such leadership, patience, management support and good example from the top will certainly help.

Advantages

There are several big advantages of this proposed approach. First, embedding security messages into existing processes improves chances that the messages reach different people in and around the organization – without them having to participate explicitly in any specific security activities like awareness raising or training courses. Second, relevant security advice can provided at the very moment when users need it; and therefore it is more likely to be followed. Third, pervasiveness of security communication creates a desired (and true) impression that security is actually important – and hopefully will engage more people to take risks and security seriously. And finally, this approach

[29] Actually, some researchers [98] propose to add knowledge as a forth level of culture, extending Schein's three levels model (artifacts, espoused values and shares tacit assumptions; [36]).

is very inexpensive to implement, even on a large scale – especially if compared to a major culture change campaign (with potentially dozens of people to pilot it, materials that need to be used, loss of productivity during the transition period etc.).

An additional advantage of this approach is that employees and users are less likely to get antagonized. Even if they strongly disagree with certain messages, they will just silently ignore them. Such reaction is not possible in case of a widely advertised and all-encompassing culture change pushed from the top management – which, in turn, doesn't leave much choice to employees: they can either embrace and follow it, or reject and oppose it. Facing such choice, inevitably some people will not only refuse to cooperate, but also will more or less openly undermine change efforts.

Similarly, a heavily imposed culture change could potentially result in an organizational culture that is "too secure". Such culture can also lead to inefficiencies (e.g. staff too focused on following procedures, rather than on the work itself). There is no such risk with the proposed "soft" (gentle and gradual) approach.

Finally, it is important to note that any culture change, regardless of the method, is a long-term process. It is a matter of years rather than weeks or months. On the other hand, the fact that significant results cannot be expected immediately should not serve as an argument not to start that culture change process in the first place.

Security messages

What should be the security messages to pass? Naturally, some can, and should be adapted to the particular situation in which they are presented. For instance, when a user is granted privileged access to a system, he should be reminded about the related security risks and measures, and pointed to relevant documentation. When a person follows a training course on Web application development, he should be taught at the same time about typical Web vulnerabilities, their consequences, and ways of avoiding them.

In some other cases, though, it may not be possible to have a specific message to pass – so security communication will need to be generic. There are many possible security messages that an organization may wish to pass. The following list contains some proposals for slogans and ideas behind them[30]:

- "Security is not complete without you"[31] – information security depends on actions and behaviours of everyone;
- "Security is as strong as the weakest link" – all weaknesses and vulnerabilities need to be identified and fixed;
- "Security is a hierarchical responsibility" – everyone is responsible for his actions; managers are also responsible for what their subordinates do;
- "Follow the least privilege principle" – use, and give only the privileges that are needed, and revoke them when they are not needed anymore;
- "Password is like a toothbrush – use it every day, change it regularly, and don't share it even with your friends", "your password should be as unique as you are";

[30] For more slogans and messages, refer to [99]
[31] This slogan could also be written in the following way: "SEC_RITY is not complete without U".

- "Be vigilant", "stay alert", "think before you click", "stop – think – click", "don't trust blindly", "double-check if in doubt", "expect the unexpected" etc.;
- "Contact your Computer Security Team / CERT / CSIRT[32] at [*e-mail address or phone number*] in case of incidents, suspicions or security-related questions";
- "Reminder: You have committed to comply with the Computing Rules";
- "Respect copyrights";
- "We are under attack, even right now" – organizations (as well as home users) are permanently under attack; and some attacks are actually targeted at specific organizations.

It is also useful to bring up a well-known security incident with major consequences, and then to show how it could have been avoided. Another idea is to remind people about their obligations as defined e.g. in security policies. Or to bring their attention to the fact that privileged access to systems is monitored and logged.

It is important, though, that messages aren't too generic (e.g. "security is important") – otherwise they become meaningless. And obviously, the choice of messages will greatly depend on security threats and risks, on existing awareness level, on technologies used etc. They should always be adapted to the needs of an organization, and not just blindly copied from elsewhere.

Processes within an organization

In every organization, and especially larger ones, people go through a large variety of processes. Obviously, employees are subject to a number of human resources (HR) processes: they are recruited, employed, trained, evaluated, promoted, reassigned etc. – and finally they retire, quit, or get dismissed. Some of these processes apply as well to contractors, visitors etc. – but these groups also have their specific "paths" into and inside the organization. In order to reach people other than regular employees, all processes affecting these people should be identified, and considered for passing security messages. The idea is to select key moments in employees' professional life, and used them for building security culture.

> *Key moments in employees' professional life*
> *should be identified and used for building security culture.*

Similarly to human processes, there are different organizational and technical processes or situations, which people follow or experience during their work in an organization. Employees request and get computing accounts and are granted access to information systems; users change their passwords; people attend meetings and read reports; managers discuss and decide on IT-related topics etc.

Many if not most of these processes and situations may be used as a platform for passing security messages and advice. Some of them even allow for adapting content of messages, making them

[32] Terms CERT (Computer Emergency Response Team) and CSIRT (Computer Security Incident Response Team) are generally considered to have the same meaning [100].

relevant to that situation and directly applicable. In the next chapters, using CERN as an example, we will see how different processes may be extended to accommodate security communication.

Chapter 5. Security messages in human processes

In this chapter we will discuss various phases of employee's lifetime in an organization, from his recruitment to contract termination (Figure 10). We will also try to include similar processes that apply to people other than employees – so to contractors, visitors, users etc. Different ways of passing security messages and advice will be proposed for each of these processes, phases or situations.

Figure 10. HR processes in employee's lifetime in an organization

As already explained in section 1.3 ("Outline of the thesis"), the content of this chapter is based on HR processes that are in place at CERN. Consequently, CERN terminology will be used throughout the chapter. When needed, it will be explained for non-CERN readers.

5.1. Recruitment and employment

The period when future employees are recruited and get employed creates very good opportunities for cultivating security culture among them. This is when organizations can ensure that newly employed people are risk conscious and "security literate". Organizations can achieve it by both selecting the ones who already take security more seriously, and positively influencing those who are less security aware.

By the time new employees actually start working, their impression should be that the organization cares about security, and privileges those who also care about it. As in human relations, the first impression is very important and lasts long. If the organization send clear signals about its commitment to security already during the recruitment phase, new employees are much more likely to take security seriously as well, throughout the whole employment period.

It may seem that new employees are just a fraction of the personnel, and so don't justify special investment in establishing a security culture already at the recruitment phase. I believe it is a wrong conclusion. Culture change is inevitably a long process that takes a couple of years. With that time perspective, even in organizations with low personnel rotation, a non-negligible portion of the staff is replaced or newly recruited – and therefore it is worth to make them security allies already during recruitment.

The goal is to have security messages and questions included in various recruitment steps, as proposed below. People working for the HR department are well placed to ensure that it happens consistently and routinely for all job openings, since they are involved in handling them anyway. If adding security-related points is left to individual initiative of future supervisors, it will be done inconsistently, and only for a small part of all job vacancies.

Job description

When job openings are announced, they usually come with a more or less detailed description of that job. At CERN, vacancies are published on the "Careers at CERN" Web portal [76]. A sample job description is presented in Appendix A.

Whenever relevant, job descriptions should include security-related points. Such points should certainly appear in the descriptions of future functions or tasks. They can also be added to the list of requirements, if justified. This should not be limited only to security vacancies. On the contrary, it applies to most IT posts (any jobs related to software, networking, system administration, databases, computing services etc.), and even to other posts, for instance those that require working with sensitive (e.g. financial, personal, confidential) information.

Here are some proposals of security-related function description of job openings:

- *"When developing software, follow Security Development Lifecycle principles", "Ensure software security using techniques such as reviews, security testing and vulnerability assessment"* (for software developers or maintainers);
- *"Propose and implement protection and intrusion detection measures", "Establish and enforce procedures to guarantee data integrity and availability"* (for service managers or system administrators)
- *"Ensure confidentiality of personal, financial, or otherwise sensitive information", "Manage correct access rights in order to protect documents and systems from unauthorized access"* (for people handling sensitive documents)

Some possible additions are also marked in the sample job description in Appendix A.

> *Candidates should see security aspects covered in job description; and hear questions on security during their job interviews.*

Job interviews

Job interviews are the obvious and natural place for questioning potential future employees – including questioning for security. This opportunity must not be missed. Candidates should be probed both for their current level of knowledge, and for their attitudes to security. The latter is actually equally important as the former – because it is easier to acquire missing security knowledge, than to replace a lax attitude with a more serious one.

The questions concerning security don't have to technical, even for a technical job. The following and similar questions will still do their job, and can be asked (and answers analyzed) even by a non-technical person such as the HR representative:

- *“Which risks would you consider as the biggest for system X?”*
- *“How would you protect service Y, its users and their data?”*
- *“What is the correct security level for system Z, from your point of view?”*
- *“How did you contribute to computer/information security in your previous job?”*

Asking security questions at job interviews has a double benefit of allowing comparing candidates’ answers and thus assessing their security knowledge and attitude, and also raising awareness of the successful candidate even before he is employed. As a positive side effect, other members of the interviewing panel will also get exposed to security issues related to that specific job.

Tests and case studies

For the same reasons why candidates should hear security-related questions during their interviews, they should see relevant security points in any tests or case studies they do. This certainly applies to questionnaires assessing their technical competences – but also to aptitude tests or business case studies. Most of them can accommodate security content in one aspect or another.

Security questions in technical tests should allow verifying if the applicant knows the terminology and main concepts; understands details of vulnerabilities and attack, protocols and cryptographic solutions etc.; and has experience with security tools and technologies – all in relevance to the particular job. For instance, a network expert should understand how SYN flood attacks work, even if his is not specialized in security. Similarly, developers should be able to correctly validate input and sanitize output; and system administrators should know at least several different security measures that contribute to defense in depth of their servers. More generally, IT staff can be expected to have a certain reasonable level of security knowledge, for example to understand the difference between symmetric and asymmetric cryptography or to know properties of hashing (digest) functions. The same logic applies also to non-IT post – for instance candidates to positions in HR or finance should know how to protect confidential information and data.

Contract and agreements

Once the successful candidate is chosen (and terms and conditions details are agreed), he is offered a work contract to sign. For employees – or contractors – who will deal with sensitive information or get privileged access to computing resources, the papers to sign could include one or more of the following documents:

- an agreement on security roles and responsibilities;
- a code of conduct or a code of ethics;
- a confidentiality or non-disclosure agreement (NDA); and/or
- an acceptable use of assets agreement [77].

In particular, ISO 27002 standard states in section 8.1.1 that “security roles and responsibilities should include the requirement to:

a) implement and act in accordance with the organization’s information security policies;
b) protect assets from unauthorized access, disclosure, modification, destruction or interference;
c) execute particular security processes or activities;
d) ensure responsibility is assigned to the individual for actions taken;

e) report security events or potential events or other security risks to the organization" [78].

Some of these documents may be generic enough to fit most job positions within an organization (e.g. an organization-wide code of conduct). At the same time, other documents may as well be specific for a particular activity (for example running the e-mail service or handling financial documents).

I actually believe that it is worth preparing a separate, dedicated code of conduct for each professional activity that involves privileged access. A code of conduct should contain "principles, values, standards and/or rules of behaviour" [79] – both security-related and other, e.g. concerning ethics, acceptable behaviours etc. – that guide employees in their professional activities. Even if such document is composed of just a couple of short points, and agreed to by the new employee over e-mail rather than on paper, it still sends a clear signal to the employee and hopefully reinforces his commitment. Here are a few samples of possible security-related statements for code of conduct documents:

- *"I have read, understood and accepted the Computer Security Rules."*
- *"I will respect confidentiality of any information I may need to access for my professional duties."*
- *"I will protect users' privacy (e.g. by masking usernames when manipulating activity logs; only disclosing user-related information to those who need to know; strictly avoiding accessing personal data, files or information unless there is a direct, justified professional need; etc.)."*

5.2. Induction

When people enter an organization, they are usually invited to participate in some induction activities. Again, this is a great opportunity for building security culture among newcomers – especially that some of them (e.g. contractors) may have not gone through the usual recruitment process, and therefore missed some of measures proposed in section 5.1.

It is important to give due attention to the future members of the organization. First, since they will be new in their jobs, they are more prone to make involuntary mistakes. Highlighting risks related to handling information, using Internet, developing software etc. will stimulate them to be attentive and exercise care. New employees are also naturally motivated to perform well in their new assignments [80] – and so they are more likely to follow strictly security rules and advice. This is why it is so useful to surround newcomers with security messages and advice as soon as they join an organization.

> *Newcomers should be surrounded with security messages as soon as they join an organization.*

Here is a list of different induction activities as offered at CERN, together with ideas how security can be made part of them:

- **General induction programme** (two parts, the second part is organized every 3 months and takes a full day – the agenda is presented in Appendix B): provide a short presentation to present security policies and to raise security awareness.
- **IT services induction presentation** (every month, 15 minutes): highlight the importance of computer and information security.
- **IT services induction course** (every 1-2 months, 2-3 hours): mention security threats and risks that users of IT services face; discuss common security errors or misconfigurations; and propose ways of avoiding them. A sample slide is shown in Figure 11, and more are presented in Appendix C.

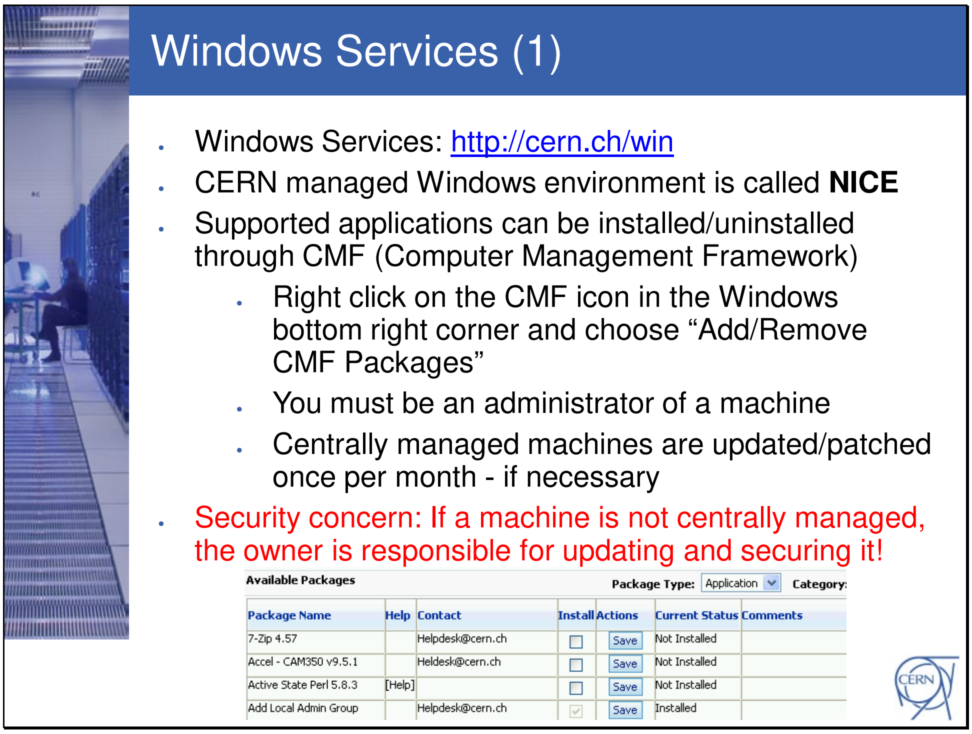


Figure 11. An induction slide on CERN Windows desktop computing

- **Meeting between a new member of the organization and the HR representative** (a one-to-one meeting, few weeks after the contract start): profit from this opportunity to propose attending relevant security courses ("Secure e-mail and Web browsing" to non-technical people, "Developing secure software" to future developers or system administrators), and to remind the employee his responsibilities (e.g. *"Do you have any questions concerning your security responsibilities?"*).

5.3. Annual reviews

Most organizations have formal processes in place to ensure that employees have regular (usually annual) reviews. At CERN, this process is called MARS (Merit Appraisal and Recognition Scheme). An important element of it is the interview between an employee and his supervisor. The goal is to evaluate past performance of the employee and to set his future work objectives, goal and priorities.

MARS interviews are scheduled following organizational hierarchy[33]. First, department leaders will meet with each of group leaders in their departments. Next, group leaders will meet with section leaders, who will later see their employees. Each interview results in a MARS appraisal report that has, among others, the following sections: Summary of functions; Evaluation of results over the reference period; Work objectives to be achieved over the next reference period; and Training objectives.

Functions

The summary of employee's functions is a very short, high-level overview of that person's job. Except for people working at least part time on security, it will not contain security-related points. At the same time, this section of the appraisal report can – and should – be used for highlighting key principles or requirements, including those concerning security.

For example, some people at CERN (and in particular managers of computing services) have the following confidentiality clauses in their summary of functions: *"This function, allowing access to confidential and/or sensitive information, implies strict conformance to the rules laid down in OC5[34] and in particular those governing confidentiality"*. I believe that adding such clauses serves as a reminder of mentioned principles, but also emphasizes their importance – and as such is very useful (and also cost-efficient).

Evaluations and work objectives

Clearly, the annual review process is ideal for setting security-related objectives, and for promoting and rewarding secure attitudes and behaviours. Preferably, supervisors should specify their expectations concerning security when setting work objectives. These expectations can be formulated to say what the employee is supposed to do (e.g. *"Design and propose additional measures to protect confidentiality of information and prevent data leakage"*) – or how he is supposed to work (e.g. *"When handling confidential documents, conform to the Computing Rules and security recommendations"*). Security objectives will usually evolve around principal security concerns – ensuring confidentiality, integrity and/or availability of information and systems; strengthening protection, detection and recovery mechanisms etc. – as relevant to each particular job.

> *Ensuring protection of sensitive information and systems*
> *should be part of work objectives.*
> *Secure behaviours and attitudes should be noticed and praised.*

Security expectations stated as individual work objectives have a stronger effect that those listed in general documents such as policies or procedures. The top-down nature of MARS process (objectives initially come from department leaders via group and section leaders to individual

[33] At CERN, top-level organizational units are departments, which are composed of groups, which in turn consist of sections.

[34] Operational Circular N°5 (OC5; [114]) governs the use of CERN computing facilities.

employees) additionally reinforces this effect – especially if it is clear for an employee that security-related points were explicitly stated by top level management and come from them.

Additionally, when evaluating past work performance of their people, supervisors should welcome and praise pro-security behaviours and attitudes. Even if there is no direct reward, employees should see that such behaviours are well appreciated. Consequently, negligence or carelessness when it comes to security should be pointed out and discussed.

It is unfortunately not easy for security or HR personnel to ensure that security is taken into account in performance assessments and work objectives across an organization. No single person or group can directly influence the content and outcome of MARS interviews. Security-related objectives have to come from the hierarchy itself. HR and security experts can only suggest that managers include such objectives in annual reviews of their subordinates – and remind about it in relevant support documents such as guidelines or FAQ.

Training objectives

In addition to work objectives, an employee and his supervisor discuss and agree also on training objectives. This is a perfect moment to propose attending dedicated security courses – especially those which are offered for free.

At CERN there are two security courses available for free – and I believe that either one or the other should be attended by most employees working with computers:

- "Secure e-mail and Web browsing" (1.5 hours) for non-technical people; and
- "Developing secure software" (3.5 hours) for developers or system administrators.

Additionally, the following dedicated security courses are also available, and should be considered by anyone using these programming languages or technologies:

- "Secure coding for Java" (1 day)
- "Secure coding for PHP" (1 day)
- "Secure coding for Perl" (4 hours)
- "Secure coding for Python" (4 hours)
- "Secure coding for Web Applications and Web Services" (1 day)
- "Secure coding in C/C++" (2 days)

5.4. Training

As discussed in section 2.3 ("Addressing the human factor"), organizations should provide security training to their personnel. A natural approach is to design security courses for different type of employees: general users, developers, system administrators, users of sensitive systems etc. Such courses should indeed be offered to educate personnel on security issues.

Nevertheless, I would argue that establishing a security culture requires more. In addition to providing dedicated security courses, other courses should include relevant security content. For example, a course on Web application development in PHP must contain a fair share of warnings and advice concerning typical vulnerabilities and attacks. Otherwise it would be simply incomplete.

Arranging that security is included as needed in different courses needs to be a mutual effort of HR or training departments (who organize courses, negotiate with trainers etc.) and security experts (who can provide suggestions for the course content). This should not be a one-off action – adding security to existing courses – but rather an established cooperation, to ensure that any new course added to the training catalogue is checked and covered as well.

> *Even non-security training activities need to cover relevant security issues.*

The training programme at CERN is divided into three categories: language courses, management and communication courses, and technical courses. I believe that the proposal (having some security content in different courses) is valid certainly for many of the technical courses, and possibly for some of the management courses. I will look into these categories in more detail.

Additionally, any other educational activities that are already in place in an organization (e.g. lecture programmes) or in its industry or community (e.g. conferences) should also be considered as good opportunities for delivering security content in the form of lectures, talks or presentations. I will examine these possibilities as well.

Technical training courses

CERN technical training catalogue contains 166 courses[35] grouped in five categories: "electronics design", "mechanical design", "office software", "software and system technologies", and "special". Because of the focus on computer and information security, we will skip electronics and mechanical design courses, and will look into the last three categories.

One of the biggest threats in modern organizations is potentially insecure or badly protected Web applications and Web sites. Consequently, relevant courses should include material that helps future Web masters and Web developers to mitigate that threat. For instance, one of the "office software" courses is about SharePoint Designer[36]. This course teaches how to use the tool to design Web pages. At the same time, I strongly believe that it should also include relevant security points, for example:

- a warning that any non-public Web content must be protected with authentication and authorization mechanisms;
- advice on how to establish such protection (preferably: how to do it on the CERN Web hosting service); and
- an explanation why hiding confidential documents by not linking them and keeping their URLs "secret" without doing proper authentication and authorization is a bad idea.

---

[35] The number of courses is as of September 2010.

[36] Microsoft SharePoint Designer, successor of FrontPage, is an HTML editor and Web design tool, formerly part of Microsoft Office suite.

Similarly, the “software and system technologies” category includes several courses about different Web application development technologies (J2EE / JSP[37], JavaScript, Oracle JavaDB, Oracle Forms and PL/SQL, AJAX[38], Oracle APEX[39]). Future Web developers attending these courses must also be trained to understand typical Web application attacks, vulnerabilities, and ways of avoiding them.

Table 1. CERN technical trainig courses for which security is particularly relevant

Course name
Intermediate Linux System Administration
JAVA 2 Enterprise Edition - Part 1: Web Applications
Linux LPI 101 - Introduction à Linux et LPI 102 Administration systèmes sur Linux
Oracle JavaDB
PERL 5 - Advanced Aspects
Web 2.0 development with AJAX

Appendix D presents the full list of “office software”, “software and system technologies”, and “special” courses, together with my estimates on how much of security content needs to be included in each of them. Table 1 lists courses for which security is particularly relevant, and should therefore receive due attention (at least 10% of the course time). Not surprisingly, courses on Linux administration are also on the list, along with Web development courses – because insecurely configured or maintained Linux servers are as easy target as vulnerable Web applications.

As a side note, it is worth reporting that one of the trainers objected when asked to include some security content in his courses. He mentioned several arguments: that software security is not more important than, say, internationalization[40] or accessibility[41]; that security advice must only be given by security experts; and that because security is orthogonal to the subject of particular courses, it should be covered in separate courses. Needless to say, I disagree with all these statements. In particular, concerning the last argument, I believe quite the opposite: security should be covered in different courses (rather than only in dedicated security courses) precisely because it is orthogonal to other courses’ subjects.

Management training courses

While benefits of having security aspects covered in technical course are (hopefully) obvious, it may be less clear so for management courses. Security is, however, not only about the technical aspects of attacks, vulnerabilities and protection measures. More generally, information security is about risk management. This includes managing processes such as threat modelling, risk analysis, business continuity planning (BCP) and disaster recovery planning (DRP).

I believe that briefly describing these processes – when relevant – during management courses is beneficial for future project or service managers, and section or group leaders. First, because many managers will anyway need to implement most of these processes, even if implicitly or very

[37] Java 2 Enterprise Edition / Java Server Pages.
[38] Asynchronous JavaScript and XML [101].
[39] Oracle Application Express rapid application development tool.
[40] Internationalization is a mean to adapt software to different languages and regional differences [115].
[41] Accessibility is a property of software that is accessible to all people regardless of disability or severity of impairment [116].

informally – so they better do it right. And second, because just mentioning these processes sends a desirable signal: the organization cares about security.

Educational programmes

In addition to individual courses that can be taken independently, organizations often offer educational or academic programmes composed of a series of lectures or courses. Again, it is certainly worth including some lectures about related security topics.

Here is a list of different academic programmes at CERN, together with descriptions and considerations on how security lectures already are, or can be included:

- **CERN School of Computing** (CSC) [81] is a summer school for young computer engineers and physicists from CERN and collaborating laboratories, institutes or universities. It is organized every year in a different European country, takes two weeks, and is usually attended by 60-80 students.

  CSC 2010 programme consists of lectures and exercises grouped in three themes: Data Technologies, Base Technologies and Physics Computing. The second theme includes lectures and hands-on exercises on software security – they take a non-negligible 10% of the total tuition time. The full programme of CSC 2010 is presented in Appendix E.

  In fact, various lectures on security ("An Introduction to Cryptography", "Public Key Infrastructure", "An Introduction to Kerberos", "Computer Security", and "Creating Secure Software") were delivered at the School since at least 2004.

- **Summer Student Lecture Programme** [82] proposes a very big choice of lectures, over a course of 7 weeks every summer, on a large variety of topics related to particle physics and CERN, from theoretical physics to accelerators and detectors. The lectures, depending on the topic, are followed by up to 300 students.

  On a positive note, the very first welcome presentation contains a 15 minute introduction to computer security. On the other hand, given the big number of lectures in this programme, I believe it would be both feasible and desirable to have a short series of lectures on topics such as safety or information security also added to the programme and proposed to CERN summer students.

- **openlab[42] summer students lectures** programme [83] complements the Summer student lecture programme by offering several talks on applied computer science. Usually some 30 to 50 students attend each lecture.

  In 2010, three lectures out of nine were dedicated to security:

  - "Control System Cyber-Security" by S. Lüders/ CERN;
  - "Software Security" by S. Lopienski/ CERN;
  - "Web Application Security" by S. Lopienski/ CERN.

[42] CERN openlab is "a collaboration between CERN and industrial partners to study and develop data-intensive solutions to be used by the worldwide community of scientists working at the Large Hadron Collider" [105].

Interestingly, these three lectures where scheduled as the first of the series – which highlights the importance that CERN (or at least the programme coordinator) attaches to security – and so, by itself, sends a desirable message. The full programme of this lecture series is presented in Appendix F.

- Other educational programmes at CERN include **Computing Colloquia** [84], **Computing Seminars** [85] and **Academic Training** [86]. They are described in more detail in Appendix G.

Conferences and workshops

People working in scientific laboratories or research organizations attend and sometimes organize various conferences and workshops. Although probably less often, employees of commercial companies also attend conferences, and have workshops or meetings with their colleagues from other offices, with their contractors etc. Whenever possible and relevant, such meetings should have tracks related to security, and participants should be encouraged to submit papers and present their work in the area. As a result, the whole community will benefit from additional security awareness and knowledge.

For example, the High Energy Physics[43] (HEP) community – which CERN is part of – has two conferences related to computing: CHEP (Computing in High Energy Physics; taking place every 18 months) [87] and HEPIX (two workshops a year) [88]. While the latter has a track half-dedicated to security ("Security and networking"), regrettably the former doesn't ("Grid /Cloud security" topic is just listed in the "Grid and Cloud Middleware" track).

5.5. Termination or change of employment

There are several security actions that must be taken when a person changes his assignment or completely leaves an organization. In particular, a supervisor of an employee that quits (for whatever reason) should arrange that:

- all access rights, privileges and authorizations of that person are revoked;
- membership of sensitive groups and mailing lists (e.g. those that are granted group access to information resources) is removed;
- all shared secrets known to that person (e.g. passwords to databases or service accounts; private keys of service or host certificates; private SSH server keys etc.) are changed;
- ownership of all non-personal computing resources (e.g. projects' Web sites, network devices, service accounts, software repositories etc.) is passed;
- security knowledge of that person (e.g. concerning protection, detection or recovery mechanisms) is properly documented; and
- security roles and responsibilities of that person are reassigned, and this change is adequately announced.

[43] High energy physics (particle physics) is a branch of physics that studies subatomic particles. Its name comes from the fact that many elementary particles can only be created and observed during high energy collisions, for example in particle accelerators [104].

These steps should preferably be part of exit procedures, in order to ensure that they are taken consistently and in a timely manner for each person who leaves. Following them, besides simply being good security practice, has an additional benefit of raising security awareness among those who leave or change jobs, and (more importantly for the organization) those who stay: their supervisors and colleagues.

Steps such removing access rights of a person who quits should be part of exit procedures – also in order to raise awareness of those who stay.

Additionally, upon termination, the employee should be reminded of any non-disclosure agreements that have been signed previously [16].

Chapter 6. Security messages in other processes and situations

In the previous chapter I have discussed how security communication can be effectively embedded into a range of different HR processes – or, in other words, processes that individuals go through during their career in an organization. Many of these processes can be easily adapted to include security content that is meaningful and relevant but not too intrusive – and that consequently contributes to establishing information security culture.

At the same time, employees are also involved in many other activities and situations that are not related to their career, but rather to what technologies they use and how they communicate. For simplicity, I will still use the term "process" to describe all these activities and situations – even if some may not match the precise definition of that term[44]. In this chapter we will discuss several such processes (and see examples from CERN) to examine how they may be used for reinforcing security awareness, knowledge and behaviours – so, in short, security culture.

6.1. Technological processes

Various situations when users interact with computer systems or services represent good opportunities for passing security messages and advice. This approach allows tuning and adapting messages to the context, and thus making them relevant and directly applicable to the particular activity performed by a user.

Figure 12. A slide from the obligatory computer security on-line course at CERN

[44] A process is usually defined as a series of steps that are done in order to achieve a particular goal.

Getting a computer account

In order to be able to access most computer systems, users need to get an account first. The process of account creation is an ideal opportunity to get users' attention and commitment to security.

For example, an owner of a newly created CERN account must follow a short on-line presentation on computer security (a sample slide is shown in Figure 12), pass a multiple-choice test and digitally sign the CERN Computing Rules [89]. If a user fails to do that within five days from account creation, his account will automatically get blocked.

Log-in interfaces

Authentication interfaces to Web applications and other computer systems are another good place for adding security messages. By design people visit them often in order to log in when they want to use any system or resources with restricted access. Such interfaces are usually quite simple and just contain forms for providing user credentials – so any security messages added will be easy to spot. Moreover, users are hopefully at least slightly more attentive than on average when they are asked to type in their passwords. As a result, they are more likely to notice security messages posted there.

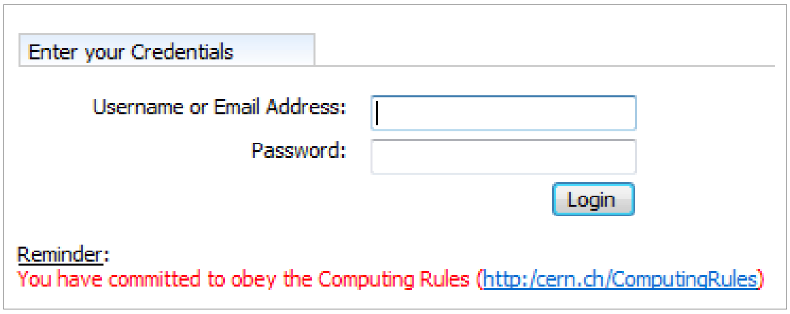


Figure 13. Part of the CERN Single Sign-On (SSO) Web page

When users are about to log in to a computer system, it is useful to remind them security policies that govern the usage of that system, and give them warnings or advice concerning the system. At CERN, computer users are reminded that they are subject to the Computing Rules – a screenshot of CERN Single Sign-On (SSO) Web page is shown in Figure 13, and more examples can be found in Appendix H. Additionally, CERN SSO Web page is also used occasionally for posting special security warnings – for example concerning current phishing attacks, as shown in Figure 14.

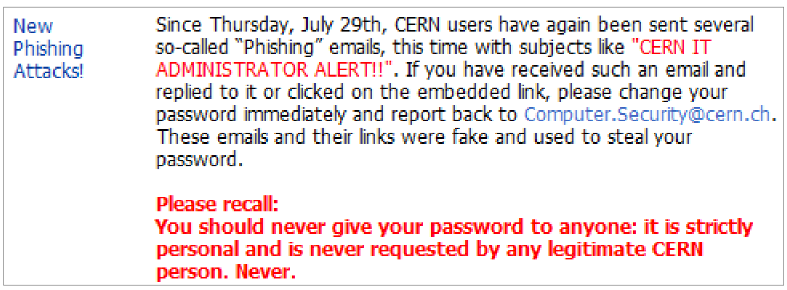


Figure 14. A special security warning posted on CERN SSO Web page

Password change

Clearly, some of the security advice that users get concerns protecting their online identities, their credentials, their passwords. It is therefore logical to assist them when they change their passwords and need to come up with a new one. A good password needs to be long, composed also of non-alphanumerical characters, not based on dictionary words, not already used by that user in other places – and at the same time easy to remember. These requirements are contradicting, and no wonder that many users miss at least one of them. It is therefore very handy, for a user who changes his password, to get some help and good security advice. This may take form of a real-time password quality and conformance checker; of some specific tips; of a unique list of suggested passwords[45]; or even of an embedded video that discusses password security. All these possibilities are shown in Figure 15.

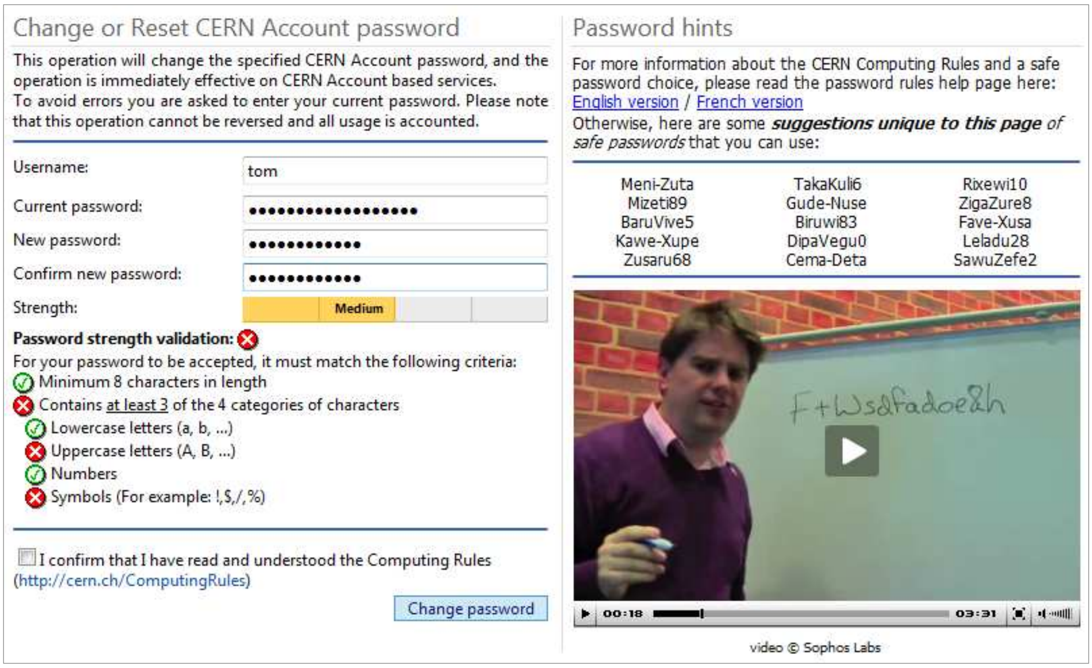


Figure 15. A possible layout of a password change page

Requesting and managing resources or privileges

Similarly, when users request new resources, access or privileges – especially for the first time – it is crucial to make them aware of any related threats and risks, and to remind them their obligations. Both the interface to make requests, and the confirmation message must contain relevant security content: warnings, advice and references. The same applies also for sensitive actions that may be taken by users when they handle or manage their resources.

For example, a CERN user requesting a new Web site (that will be hosted at CERN Web hosting service) and managing it afterwards should see security messages in various moments of that process. This is especially important since Web sites may be made public (although by default they are visible to CERN users only), and dynamic (scriptable; by default they are static). Possible security communication for requesting and managing Web sites include:

[45] Such a list of good quality passwords is regenerated randomly for each visit of the page, and is therefore different each time the page is visited.

- a mandatory confirmation of the Computing Rules (in the request form, as shown in Figure 16);
- a reminder that by default the Web site is not public and not scriptable (in the confirmation message once the Web site is created);
- a warning about the risks related to non-encrypted Web traffic (when the owner disables "require encrypted HTTPS connection" option);
- references to training courses on secure Web application development (in the confirmation message, and when the Web site is reconfigured to be scriptable);
- an explanation of how a vulnerability scan can be requested.

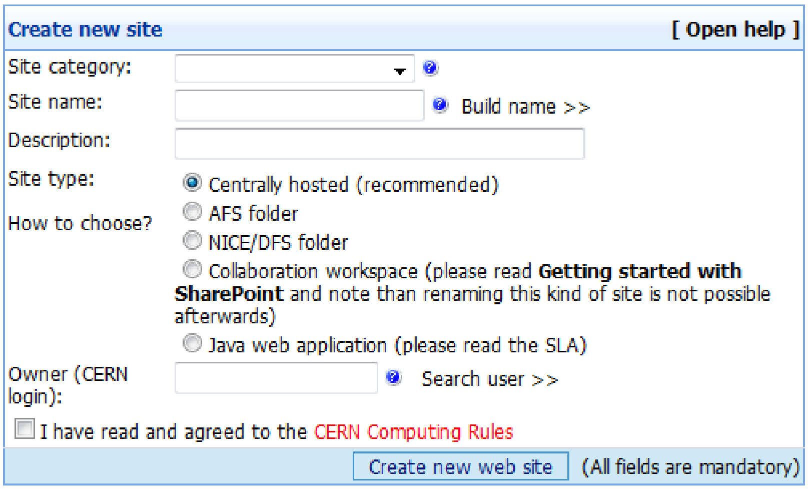


Figure 16. Requesting a new Web site at CERN

Adding security communication should also be considered for other similar processes. For instance, the creation of a new e-group (mailing list) is a good moment to warn its creator about the risks of keeping subscription policy open, and to suggest secure settings. When a new Subversion source code repository is requested, it is relevant to remind developers about software security training courses and about static source code analysis tools[46]. Other security messages can be (and, at CERN, some already are) passed at similar situations: for example at the creation of new database accounts and schemas, J2EE containers, TWiki webs, Savannah or Indico[47] categories etc.; and also when access to Terminal Services is requested, a new network device is registered, a firewall opening is requested, a server is added to Quattor[48], a Lemon[49] sensor is being registered etc.

---

[46] Static code analysis tools examine the source code of software and look for potential bugs or vulnerabilities (both security- and non security-related). Several such tools were evaluated by CERN Computer Security Team, and are recommended to CERN developers [109].
[47] Indico (Integrated Digital Conference) is a Web-based system for managing and organizing events (meetings, workshops, conferences etc.), developed at CERN and released under GPL free software licence [106].
[48] Quattor is a system administration toolkit for managing large clusters (>1000 nodes), developed initially at CERN and released under Apache free software licence [107].
[49] Lemon is a client-server monitoring system developed at CERN and released under GPL free software licence [108].

User documentation

Finally, any user documentation of computer systems or computing services should contain relevant security points. In reality, the initiative often needs to come from the security team. Moreover, some documentation authors will have the necessary security awareness and knowledge – but other will not. It is therefore quite likely that security experts' help or guidance is needed to cover sufficiently all relevant security issues.

6.2. Other processes

There are other organizational processes, situations and communication channels that are not directly related to individuals or their use of technology. Examples include decision-making meetings; different management and production processes; internal bulletin boards, paper publications or electronic newsletters etc. As with processes discussed before, it is important to identify those which can be effectively used for passing security messages. Two of these points are discussed in the rest of this chapter: how security-related information can be spread around an organization, and how to ensure that security is taken into account when decisions are taken.

Reporting and dissemination

Security teams must ensure regular reporting on different security-related issues. Security reporting is crucial, as it contributes to raising awareness and building knowledge (and, in the long term, to reinforcing security culture); and it makes security efforts more visible and transparent, and – consequently – security spending more justified. Topics that should be covered in such reports include:

- new vulnerability and attack trends (both expected and already observed);
- incidents that happened – and near-misses – together with lessons learned;
- changes to security rules or procedures; and
- updates on security tools, services and operations.

Security reports should reach both the management and the general user community. Naturally, the choice of topics and the level of detail may differ between these two groups. At CERN, the Computer Security Team reports regularly to several management and technical boards, such as the IT Group Leaders Meeting (GLM) and C5[50] meeting (both have weekly meetings) as well as at the IT Departmental Communication Meetings (DCM; monthly). On top of that, monthly computer security reports are published and made available to anyone at CERN.

Additionally, any communication channels that exist in an organization should be used for security communication when relevant and reasonable. At CERN, this includes the bi-weekly Bulletin [90] and the quarterly CERN Computer News Letter (CNL) [91][51]. Articles on various computer security topics are often published in the CNL (one of the recent headlines is shown in Figure 17) and occasionally also in the Bulletin – the list of recent security-related articles in presented in Appendix I.

On a side note, although it is certainly a good idea to profit from any established publications, it is far from granted that everyone in an organization reads them and will notice entries on security.

[50] C5 stands for CERN Computer Centre Coordination Committee – that discusses technical aspects of running the Computer Centre and offering computing services.
[51] Both the Bulletin and the CNL are available on-line and on paper.

Technical brief

Attackers are on the prowl for your security weaknesses

The academic freedom at CERN demands a rather open computing environment, which is reflected in the liberal nature of the CERN Computing Rules (http://cern.ch/security/ComputingRules). Depending on your project(s), you have the liberty to use whatever programming language you wish to use, be it to program your physics analyses, your controls software or your web application. For the CERN Computer Security Team, however, such a liberal environment poses an interesting challenge, because this freedom of choice is hard to control and even more difficult to secure. Even more interesting, this challenge has to maintain a justifiable balance between CERN's academic freedom and its security.

You are responsible for securing your systems

A screenshot of Findbugs, a Static Source Code Analyser available for Java.

In addition, the Security Team provides a tool to check (and if desired to correct) the access control lists on a user's home directory. The tool is aware of the

out what they consider to be potential weaknesses. A typical example of what such tools can find is calls to the "gets" C function. This function is inherently insecure and can lead to buffer overflows. Specially crafted user input values can for instance allow an attacker to access or modify confidential data or even take control of any computer executing that piece of vulnerable software.

Of course, such automated source-code analysis tools are only able to find a fraction of bugs present in a piece of code. Still, you are strongly recommended to use them to find at least some of the existing weaknesses (of any type, not only security related) – especially given how easy it is to install and run these tools.Because these tools need to understand the code, they are language specific.

Figure 17. Headline of an article on computer security published in CERN Computer News Letter

Advisory panels and decision boards

It is desirable that security experts are members of any advisory panels and decision boards that discuss computing projects or services. When needed, they will be able to voice comments concerning risks and propose security counter-measures. Generally speaking, they will attempt to influence the process so that relevant security issues are given a thought. As a result, each time recommendations are made or decisions are taken, security will be considered and hopefully taken into account. Moreover, other involved people will regularly be exposed to security considerations. This is even more important as far as a long-term security culture change is hoped for.

To be effective in this role, the security person clearly needs to be a skilled communicator and diplomat – and needs to maintain a balanced view on security versus other needs. Otherwise he risks having his security input always rejected, even when it is actually reasonable and justified (the "cry wolf" effect).

At CERN, there are four periodic meetings during which IT projects and services are discussed – either internally (the GLM, and the annual IT Programme of Work meeting) or with the management or representatives of user communities (IT Service Review Meeting and IT Technical Users Meeting). They are all attended by a member of the Computer Security Team.

Chapter 7. Inspiration, conclusions and open questions

7.1. Inspiration and feedback

This thesis described a proposal for a pragmatic, efficient and cost-effective way of establishing a security culture in an organization. It started by examining the human aspect of information security, and discussing ways of addressing it – and went on to investigate what organizational culture is, and what it usually takes to develop a security culture. While normally a culture change requires significant efforts, I proposed to cultivate security culture in a less imposed way: by increasingly building security knowledge and awareness, and influencing behaviours. The rest of the thesis presented how this can be attempted by adding relevant security communication to existing human processes (such as recruitment or training), as well as to other situations and activities that take place in any organization.

> *Security initiatives that are optional and depend on employees' will to cooperate, attend or participate, will only have limited impact.*

This order of chapters actually reflects the way how I gradually came to the idea itself. It started with an observation that human errors, carelessness, and lack of security understanding is behind a big percentage of both weaknesses and incidents. In order to address this problem, I initiated and led, or participated in a number of efforts that aimed at raising security awareness (e.g. CERN Computer Security Day [92]) and providing training (e.g. software security courses). It soon became apparent, though, that any such initiative that is optional and depends on someone's will to cooperate, attend or participate will have only limited impact. This is simply because most people will not participate, for one reason or another (they will not have time; will think that security needs don't justify investments; will not believe that risks are considerable; will forget to come and participate when the day comes etc.). Consequently, many efforts (e.g. some of the awareness raising activities) result just in "convincing the convinced": attracting only those who are already security-aware and want to learn more, but missing those who aren't. Clearly, another method was needed to achieve the goal: making people understand security, and take it seriously.

I decided to try the "opt-out" rather than "opt-in" approach – or, in other words, to ensure that people receive security messages and advice embedded in the context of their usual work activities. This approach guarantees that security content reaches people, unless they *explicitly* decide to reject or ignore it. Actually, some measures don't even allow users to opt out – for example the security presentation and test at the CERN account creation are mandatory.

Naturally, this approach was first discussed within the Computer Security Team, and it got validated and is supported by CERN Computer Security Officer. The proposal was consequently submitted to, and accepted by the IT department leader. Since a number of the proposed measures involve different HR processes (and training in particular), this approach was then presented to the HR representative in the IT department, and to the IT Departmental Training Officer. They were both very positive about it – and contributed with several additional ideas.

> *The "opt-out" rather than "opt-in" approach was validated by the Computer Security Officer and by the IT department leader.*

The comments received were encouraging – the proposed approach was considered "feasible" and "certainly worth implementing". This feedback came with a couple of suggestions for similar measures that can be put in place at CERN – most of them were adopted and are also listed in this thesis.

A number of ideas described in the thesis were already implemented at CERN since some time, independently of this proposal (although in line with it) – thanks to individual initiative of different people in the IT department, thanks to efforts of HR people, and thanks to the work done by the Computer Security Team. Several other ideas from this thesis have been put in place recently, in order to try this approach, and to serve as a proof of concept. The remaining ideas are in the planning or early implementation phases.

7.2. Observations, results and conclusions

The implementation work already done at CERN led to some interesting observations and conclusions that are worth mentioning.

All the proposed measures meant adding security content to existing processes of different kinds. This can only be done in cooperation with the corresponding process owners, e.g. the recruitment service, or the manager of the Web hosting service. The first step is therefore to convince them that the idea is good, and worth their time. This can be potentially a challenge – people may, for example, consider the proposed solutions ineffective; they may simply want to avoid introducing any changes; they may think that security needs don't justify the proposed measures; they may believe that it is not their role to work for security etc. As it was presented in section 5.4 ("Training"), one of the course trainers did in fact openly oppose to the idea. At the same time, I observed that many of the contacted people were actually positive about the idea (or even contributed to it) from the very beginning – even if time or resource constraint didn't allow a quick implementation

There are additional advantages of these interactions with process owners. Not surprisingly, discussing security issues with different people across the organization is beneficial for both sides: they learn more about security, and security people learn more about their security needs and worries.

Another conclusion is that effective security measures need to be centralized and coordinated either by HR people (for human processes) or by security experts. For example, job descriptions are written by the corresponding groups – but later they are all edited and published by the recruitment people, who can easily influence them in a consistent and thorough way. On the other hand, measures that need to be put in many places by different people will never get fully implemented. As already explained in section 5.3 ("Annual reviews"), it is much harder to ensure that security is covered during MARS interviews. The one-to-one nature of these interviews (an employee meets with his supervisor) means that security will be included only if the supervisor remembers about it, is convinced himself etc.

In other words, any security measures implementing this proposal should be designed, whenever feasible, so that they can be easily introduced and managed by a single organization unit, or even a single person. Luckily, such design is also likely to make them relatively inexpensive. It requires less efforts and resources, for example, to complement existing training courses (that are already advertised and well established) with security content, than to prepare dedicated security courses and attract people to attend them.

Moreover, I am more and more convinced that when security communication becomes pervasive, people will start paying more attention to it. Even if they don't really absorb the content of all these security messages, still they will eventually have no choice but to conclude that the organization cares about security – and that consequently they should, too.

> *Pervasive security communication is a clear signal that the organization cares about security – and that people should, too.*

Finally, it is clearly too early to have meaningful results, and measure how effective is the proposed approach. As explained in Chapter 3 ("Security culture and culture change"), a successful culture change is a long-term goal. At the same time it can be observed that the global level of security knowledge and awareness at CERN is noticeably higher than just a few years ago. For instance, more people report phishing attempts to the Computer Security Team than fall for them; and having major vulnerabilities is now also considered embarrassing, and not just wrong. Naturally, there may be different factors (both internal to the organization, and external) contributing to this gradual change. Nevertheless, I think that various security initiatives that are already in place at CERN – some for weeks or months, other for years – have certainly contributed to it.

7.3. Open questions

As this proposal is being implemented at CERN, it will be interesting to see its outcome in a couple of years – and to draw conclusions and see what lessons can be learned from that experience. There are two open questions that will naturally be asked. First, was it really feasible and realistic to implement all these measures, especially with investing only limited resources? And second, did they indeed lead to a sustainable security culture change?

I believe that – as explained throughout this thesis – the answer to both questions is "yes". But to know for sure, we will just have to try it, wait, and see.

Appendix A A sample job description

This appendix presents a sample description of a job vacancy as announced on "Careers at CERN" Web portal [76] in July 2010. For clarity reasons, some parts and details such as qualification requirements, eligibility and employment conditions were stripped away.

Actually, this job description does include points relevant to security – they are <u>underlined</u>. Other possible security-related additions are <u>*in italic and underlined*</u> (they were not part of the original job description).

Financial IT systems support

- Providing IT support to the Finance and Procurement teams across a range of projects
- Working on reporting statistics, key performance indicators, and data analysis <u>*as well as on data security*</u>
- The team's expert on IT systems, liaising with experts in the IT department

[...]

Introduction

The Finance and Procurement Department (FP) is responsible for the financial administration of the Organization in compliance with the Financial and Procurement Rules and the Financial Guidelines for LHC Collaborations.

Functions

As an administrative assistant or computing technician in the Reporting and Computer Support Section of the Finance and Procurement Department, the successful candidate will gradually take on the following responsibilities:

- Reviewing existing universes in Business Object and redesign where necessary to facilitate use by end users.
- Generating various ad hoc reports and statistics, including the purchasing report for the FP Department, <u>*while ensuring confidentiality of financial data*</u>.
- Maintaining the FP website.
- Taking part in the implementation of <u>control mechanisms and procedures to guarantee the integrity and quality of financial data</u>.
- Providing technical assistance and training for users of the various software packages in use and maintain contacts with experts in the Information Technology Department.
- Managing local administrative computing (management of computer equipment, <u>management of access rights</u> for the applications and for the different servers, etc.) <u>*and ensuring its security (protecting it, detecting security incidents etc.)*</u>.
- Maintaining the database of suppliers and entry of new suppliers.
- Providing technical support for the FP Treasury system.

[...]

Appendix B Induction programme

This is the agenda of the second part of CERN induction programme as held in September 2010. It is also available at http://indico.cern.ch/conferenceDisplay.py?confId=100920. Among presentations on various aspects of working at CERN, there is one discussing CERN Computing Security and Rules.

Filter More | Europe/Zurich | English | Login

INDUCTION PROGRAMME - 2nd Part

chaired by Cécile GRANIER, Margarita SGOURAKI

Tuesday 07 September 2010 from **08:30** to **18:00** (Europe/Zurich)
at CERN (13-2-005)

Description Les présentations sont faites alternativement en français et en anglais.
Presentations alternate between French and English.

Tuesday 07 September 2010

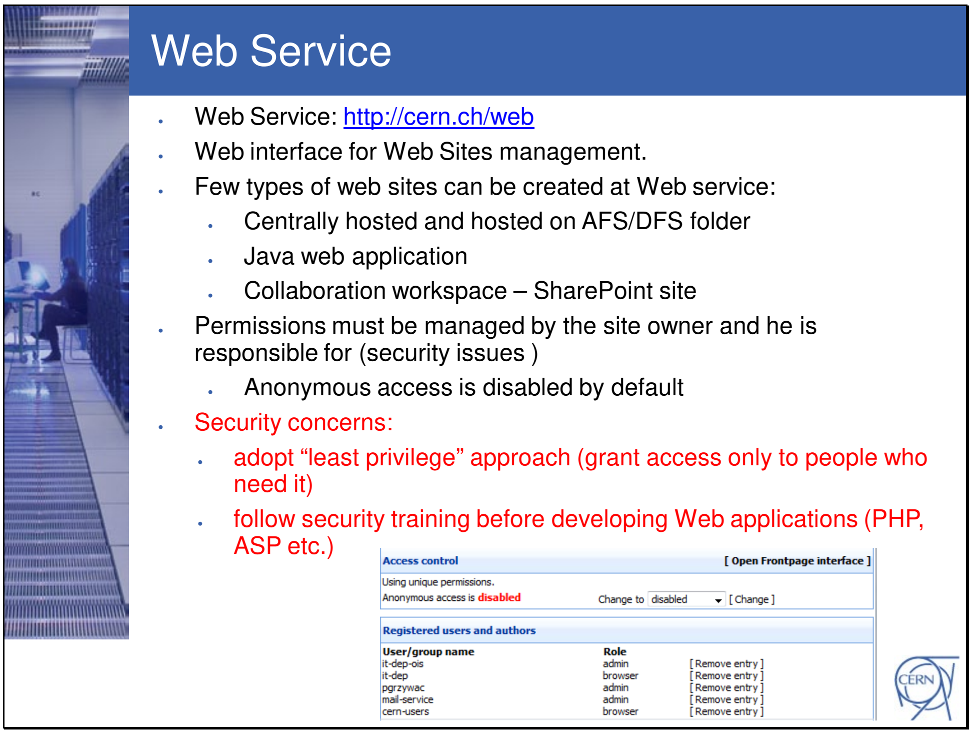
08:30 - 09:00	Welcome *30'*
09:00 - 09:15	Introduction *15'* Speaker: Cecile Granier (CERN)
09:15 - 09:35	CERN activities (Head of PH Department) *20'* Speaker: Philippe Bloch (CERN)
09:35 - 10:05	CERN people and CERN organization (Deputy Head of HR Department) *30'* Speaker: Jean-Marc Saint-Viteux (CERN)
10:05 - 10:20	Group photo
10:20 - 10:35	Fellows *15'* Speaker: Katharine Thomas-Chevreux (CERN)
10:35 - 11:00	Coffee break
11:00 - 11:15	Staff members *15'* Speaker: Clementine Lehtinen (CERN)
11:15 - 11:45	Merit Recognition *30'* Speaker: Ariana Morris (CERN)
11:45 - 12:00	CERN's Computing Rules *15'* Speaker: Sebastian Lopienski (CERN)
12:00 - 13:20	Lunch - table reserved (Restaurant 1 - NOVAE (self service))
13:20 - 13:30	Quizz - Games *10'*
13:30 - 14:15	Question and Answer session with Ph. Bloch, Head of PH Department *45'* Speaker: Cecile Granier (CERN)
14:15 - 14:35	Communication, Education and Outreach *20'* Speaker: Rolf Landua (CERN)
14:35 - 14:40	Film *05'*
14:40 - 14:55	Pension Fund *15'* Speaker: Emilie Colette Clerc
14:55 - 15:10	Staff Association *15'* Speaker: Catherine Regelbrugge
15:10 - 15:15	Presentation of a CERN Club *05'*
15:15 - 15:45	Coffee Break
15:45 - 16:00	Library *15'* Speaker: Tullio Basaglia (CERN)
16:00 - 16:15	Equal Opportunities *15'* Speaker: Tim Smith (CERN)
16:15 - 16:45	Learning & Development *30'* Speaker: Sudeshna Datta Cockerill (CERN)
16:45 - 17:00	Closing speech with the Director General *15'* Speaker: Rolf Heuer (CERN)
17:00 - 18:00	Closing drink *Department Heads / Speakers/ Human Resources Advisors/ DAO*

http://indico.cern.ch/event/100920
Last modified: 03 September 2010 13:54

Powered by CDS Indico

Appendix C Induction presentation of IT services

This appendix contains a selection of presentation slides from CERN IT services induction course. This course is given every 1-2 months, and lasts 2-3 hours. The selected slides contain computer security warnings or advice, marked in red as in the original slides.



Linux Service

- Linux at CERN: http://cern.ch/linux
- CERN runs a customized version of Linux called Scientific Linux CERN (SLC)
  - Based on Red Hat Enterprise Linux
  - Providing long term stability and support
- Same version is used on individual systems and central services in Computer Center
- Integrated with other CERN IT services
- Providing access to AFS distributed file system
- Centrally managed lxplus.cern.ch provides users with home directory which have backup
- Used also outside CERN by many Grid sites and collaborating High Energy Physics institutes.
- Security concern: AFS access rights (ACLs) are different than Linux file system access rights!

Windows Services (1)

- Windows Services: http://cern.ch/win
- CERN managed Windows environment is called **NICE**
- Supported applications can be installed/uninstalled through CMF (Computer Management Framework)
  - Right click on the CMF icon in the Windows bottom right corner and choose "Add/Remove CMF Packages"
  - You must be an administrator of a machine
  - Centrally managed machines are updated/patched once per month - if necessary
- Security concern: If a machine is not centrally managed, the owner is responsible for updating and securing it!

Available Packages **Package Type:** Application **Category:**

Package Name	Help	Contact	Install	Actions	Current Status	Comments
7-Zip 4.57		Helpdesk@cern.ch	☐	Save	Not Installed	
Accel - CAM350 v9.5.1		Heldesk@cern.ch	☐	Save	Not Installed	
Active State Perl 5.8.3	[Help]		☐	Save	Not Installed	
Add Local Admin Group		Helpdesk@cern.ch	☑	Save	Installed	

Macintosh

- Information available from http://cern.ch/mac
- Not centrally managed
  - User accounts local
  - Users responsible for installing security updates
- Applications available from central server (details on the info page)
- Security concern: Mac computers can also be infected by viruses, trojans, malware, keyloggers etc.

E-Groups

- Group members can be CERN people, external e-mail addresses, other groups or computing accounts ("static groups")
- Optionally, people can be allowed to subscribe themselves to the group (subscription policy setting)

egroups-training	Static	Training about egroups	Active	Pawel.Grzywaczewski@cern.ch	Unsubscribe
egroups-training-admin	Static	Administrator group for e-group: egroups-training	Active	Pawel.Grzywaczewski@cern.ch	Subscribe

- Groups members can also be defined by using a selection criteria on CERN people ("dynamic groups"), for instance "all people in department X"
- A group's owner can designate additional administrators for the group
- Security concern: "Open self subscription policy" means that everybody can join the group!

Appendix D Technical training courses

This appendix lists CERN technical training courses from categories “office software”, “software and system technologies” and “special”, as of September 2010. For clarity reasons, categories “electronics design” and “mechanical design” are not presented, as they are less relevant in the context of information security.

The first column of the table contains my estimates on how relevant security is for the subject of each particular course, and consequently what fraction of the course time should it take. Symbols used in this column have the following meaning:

*	*the trainer should briefly mention basic security considerations for the given technology (<5% of the course time)*
**	*several security-related points should be discussed during the course (5-10% of the course time)*
***	*security aspects are very important for the subject and should be well covered (>10% of the course time)*
(sec)	*a dedicated security course (100% of the course time)*

No symbol in the first column means that no particular security-related points need to be raised during that course.

	Office software	**Duration**
*	A hands-on overview of EVO	4 hours
	ACCESS 2007 - Level 1 : ECDL	2 days
	ACCESS 2007 - Level 2 : ECDL	2 days
*	CERN EDMS - Introduction	8 hours
*	CERN EDMS MTF in practice	4 hours
*	CERN EDMS for Engineers	1 day
**	CERN EDMS for Local Administrators	2 days
	Dreamweaver CS3 - Level 2	2 days
	Dreamweaver CS3 - Niveau 1	2 days
	EXCEL 2007 (Short Course I) - HowTo... Work with formulae, Link cells, ...	3 hours
	EXCEL 2007 (Short Course II) - HowTo... Format your worksheet for printing	3 hours
	EXCEL 2007 (Short Course III) - HowTo... Pivot tables	3 hours
	EXCEL 2007 - Level 2: ECDL	2 days
	EXCEL 2007 - level 1 : ECDL	2 days
	Get the most of Office 2007!	1 hour
**	HRT(Human resource toolkit) & EDH (Electronic document handling) / INDICO&CDS	3 hours
*	Indico - Conference Organization	3 hours
*	Indico - Meeting Organization	2 hours
*	Individual Coaching	1 hour
	LaTeX par la pratique	12 hours
	OUTLOOK 2007 (Short Course I) - E-mail	3 hours

	OUTLOOK 2007 (Short Course II) - Calendar, Tasks and Notes	3 hours
	OUTLOOK 2007 (Short Course III) - Meetings and Delegation	3 hours
	PowerPoint 2007 - Level 1: ECDL	2 days
	Powerpoint 2007 - Level 2	1 day
	Project Planning with MS-Project	2 days
(sec)	Secure e-mail and Web browsing	1.5 hours
*	Sharepoint Collaboration Workspace	2 days
*	Sharepoint Collaboration Workspace Advanced	4 hours
	Sharepoint Designer (Frontpage) - Level 1	2 days
*	Sharepoint Designer (Frontpage) - Level 2	2 days
*	Videoconferencing and collaborative tools	2 hours
	WORD 2007 (Short Course I) - HowTo... Mail merge (with Outlook)	3 hours
	WORD 2007 (Short Course II) - Working with long document	3 hours
	WORD 2007 - level 1 : ECDL	2 days
	WORD 2007 - level 2 : ECDL	2 days
*	Windows Vista Advanced	8 hours
*	Windows 7	3 hours

	Software and system technologies	
	Core Spring	32 hours
*	Agile Project Management with Scrum	16 hours
	Business Objects Basic	2 days
	Business Objects advanced	1 day
*	C++ Part 1 - Hands-On Introduction	4 days
*	C++ Part 2: Object-Oriented and Generic Programming	4 days
	C++ Programming Part 3 - Templates and the STL (Standard Template Library)	2 days
*	C++ Programming Part 4 - Exceptions	1 day
	CERN openlab Multi-threading and Parallelism Workshop	2 days
	CERN openlab/Intel Computer Architecture and Performance Tuning Workshop	2 days
*	Certification: Ingénieur en Sécurité Fonctionnelle	28 hours
(sec)	Developing secure software	3.5 hours
	Emacs - way beyond Text Editing	1 day
**	Fonctions Instrumentées de Sécurité	16 hours
**	ISTQB International Software Testing Qualifications Board	32 hours
*	ITIL Foundations (version 3)	3 days
	ITIL Foundations (version 3) EXAMINATION	1 hour
***	Intermediate Linux System Administration	4 days
	Introduction to Databases and Database Design	2 days
*	JAVA - Level 1	24 hours
*	JAVA - Level 2	32 hours
***	JAVA 2 Enterprise Edition - Part 1: Web Applications	2 days
*	JAVA 2 Enterprise Edition - Part 2: Enterprise JavaBeans	3 days
*	JCOP - Finite State Machines in the JCOP Framework	3 days
*	JCOP - Joint PVSS-JCOP Framework	4.5 days
**	JavaScript for web development	3 days
**	Javascript/jQuery/AJAX course	3 days
**	Le Langage C (ANSI et C99)	4 days

***	Linux LPI 101 - Introduction à Linux et LPI 102 Administration systèmes sur Linux	32 hours
*	NetApp	5 days
	Object-Oriented Analysis and Design using UML	3 days
	Object-oriented Design Patterns	3 days
	Oracle - Advanced SQL	3 days
**	Oracle - Build Internet Applications with Oracle Forms	40 hours
**	Oracle - Develop Web-based Applications with PL/SQL	2 days
	Oracle - Programming with PL/SQL	3 days
	Oracle - SQL	3 days
	Oracle BEA WebLogic Server 9/10	5 days
*	Oracle Certified Professional	5 days
	Oracle Database Performance Tuning	4 days
	Oracle Database SQL Tuning	3 days
*	Oracle Database Server Administration	5 days
*	Oracle Database: RAC Administration	5 days
*	Oracle Databases: Advanced Backup & Recovery Scenarios	3 days
	Oracle Databases: Advanced PL/SQL Programming	3 days
*	Oracle Forms Developer - Move to the Web	2 days
*	Oracle JDeveloper - Build Applications with ADF	3 days
***	Oracle JavaDB	5 days
*	Oracle iDS Designer - First Class	5 days
***	PERL 5 - Advanced Aspects	1 day
**	PERL 5 - Introduction	2 days
	Project Development using Python	4 days
*	Python - Hands-on Introduction	4 days
*	Python: Advanced Hands-On	4 days
	ROXIE User's Course - Beginners Level	3 days
	ROXIE Workshop 2009	40 hours
(sec)	Secure coding for Java	1 day
(sec)	Secure coding for PHP	1 day
(sec)	Secure coding for Perl	4 hours
(sec)	Secure coding for Python	4 hours
(sec)	Secure coding for Web Applications and Web Services	1 day
(sec)	Secure coding in C/C++	2 days
	System Development and Programming with the Analog Devices' SHARC Family	3.5 days
	Vouchers for Oracle Certification Test I	1 hour
	Vouchers for Oracle Certification Test II	1 hour
***	Web 2.0 development with AJAX	3 days
**	Web Applications with Oracle Application Express (APEX) 3.2	3 days
	XML - Introduction	16 hours

	Special	
	AXEL: Introduction to Particle Accelerators	2 days
	Demonstrating Reliability with Accelerated Testing	2 days
*	Designing effective websites	2 days
*	Egroups training	3 hours

Appendix E CERN School of Computing – programme

CERN School of Computing (CSC) is a summer school for young computer engineers and physicists (see more in section 5.4, point "Educational programmes"). The programme of CSC 2010 – available also at http://cern.ch/CSC/2010/This_year_school/Scientific_Programme/Programme_overview.htm – is presented below. It includes lectures and hands-on exercises on software security (marked in red) – they take a non-negligible 10% of the total tuition time.

Programme Overview 2010

CERN School of Computing

The CERN School of Computing 2010 is organised around 3 thematic themes, each theme comprising lectures and exercises.

Theme	DT Data Technologies			BT Base Technologies			PC Physics Computing		
Theme Coordinators	Alberto Pace Bend Panzer Steindel			Pere Mato Sebastian Lopienski			Rudi Frühwirth Ivica Puljak Are Strandlie		
			H			H			H
Lecture Series	Data Technologies	A. Pace B. Panzer-Steindel	5	Computer Architecture and Performance Tuning	S. Jarp A. Nowak	3	General Introduction to Physics Computing	R. Frühwirth	2
				Creating secure software	S. Lopienski	2	Introduction to ROOT	A. Naumann B. Bellenot	3
				Virtualisation	P. Mato	2	Data Analysis	A. Heikkinen I. Puljak	4
				Networking QoS and Performance	F. Fluckiger	2	Software Tools for Physics Computing	B. Jacobsen	2
			5			9			11
Exercises	Data Technologies exercises	A. Pace B. Panzer-Steindel A. Peters	5	Creating secure software	S. Lopienski	3	Introduction to ROOT	A. Naumann B. Bellenot	3
				Computer Architecture and Performance Tuning	S. Jarp A. Nowak	3	Data Analysis	A. Heikkinen I. Puljak	4
				Virtualisation	P. Buncic P. Mato	1	Software Tools for Physics Computing	B. Jacobsen	5
			5			7			12
Total hours			10			16			23

Appendix F openlab summer student programme

The programme of CERN openlab summer student lectures 2010 is presented below (see also section 5.4 “Training”, point “Educational programmes”). It should be noted as a very positive fact that the three security talks were scheduled first.

CERN openlab

openlab summer student program 2010

Computer Science Overview talks

All the lectures will be held in the IT Auditorium (bldg. 31-3rd Floor) at 16:00

Date	Topic	Speaker
19 Jul	Lecture 1: Control System Cyber-Security	S. Lüders/ CERN
20 Jul	Lecture 2: Software Security	S. Lopienski/ CERN
21 Jul	Lecture 3: Web Application Security	S. Lopienski/ CERN
27 Jul	Lecture 4: Physics Computing at CERN	H. Meinhard/ CERN
02 Aug	Lecture 5: Size and complexity of the CERN network	R. Jurga/ CERN
03 Aug	Lecture 6: Worldwide LHC Computing Grid overview	M. Schulz/ CERN
04 Aug	Lecture 7: Overview of the gLite middleware	M. Schulz/ CERN
06 Aug	Lecture 8: Data Reliability at CERN and ideas on how to improve it	A. Pace/ CERN
09 Aug	Lecture 9: Invenio Technology (you can also download handouts)	T. Simko/ CERN

Appendix G Other educational programmes at CERN

This appendix complements the list of CERN educational programmes mentioned in section 5.4 "Training", point "Educational programmes", and mentions past security-related lectures.

- **CERN Computing Colloquia** [84] are infrequent talks given by often distinguished personalities[52] that present future trends in computing and information technology.

  In previous years, the following colloquia related to security where given:

  - "Quantum cryptography for secure optical communication networks"
    by G. Ribordy (CEO, id Quantique);
  - "Anytime, Anywhere, Active Computing Security in the 21st century"
    by D.K. Matai (Executive Chairman, mi2g Ltd);
  - "A High-Performance Pattern Matching Engine for Intrusion Detection"
    by J. van Lunteren (IBM Zurich Research Labs).

- **CERN Computing Seminars** [85] are occasional seminars on technical topics related to computing.

  In previous years, the following seminars related to security where given:

  - "Shibboleth"
    by C. La Joie (SWITCH);
  - "Vulnerability Assessment and Secure Coding Practices for Middleware"
    by E. Heymann (UAB) and B. P. Miller (U.Wisconsin);
  - "Securing with the OSSTMM 3"
    by P. Herzog (ISECOM);
  - "Code Analysis Tools: finding your bugs before somebody else does!"
    by T. Hofer (CERN/IT);
  - "Creating Secure Software"
    by S. Lopienski (CERN/IT);
  - "Control systems in practice - Safety issues in modern railway traffic control"
    by M. Carbone et al (Ansaldo STS).

- **CERN Academic Training** lecture programme [86] consists of series of lectures on both pure and applied scientific subjects.

  Most Academic Training lectures are not related to computer or information science – nonetheless, a series of three lectures on "Internet Security Technologies" was given by R. Cowles, SLAC in March 2003.

---

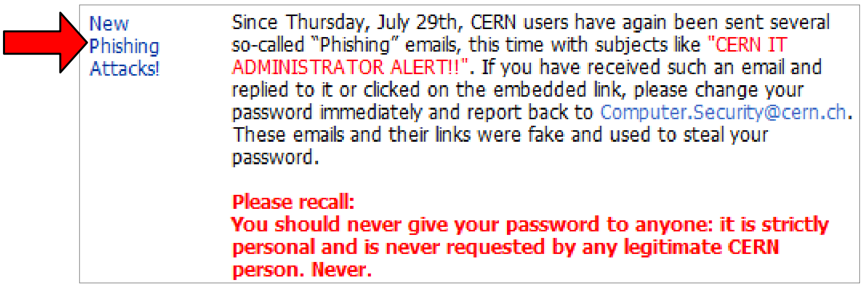
[52] CERN Computing Colloquia speakers in the past include Craig Barrett (Chairman, Intel Corporation), Vint Cerf (TCP/IP protocol designer; Vice President, Google), James Gosling (inventor of the Java programming language), Mark Shuttleworth (founder of Thawte certification authority; sponsor of Ubuntu Linux distribution), Richard Stallman (founder of the GNU Project and initiator of the free software movement) and Bjarne Stroustrup (creator of the C++ programming language).

Appendix H Log-in interfaces

This appendix contains screenshots of log-in interfaces of several CERN computer systems. For Web applications, these are simply Web pages on which users provide their credentials. Reminders of CERN Computing Rules, and other security-related points are marked with red arrows.

CERN Single Sign-On (SSO) Web page:

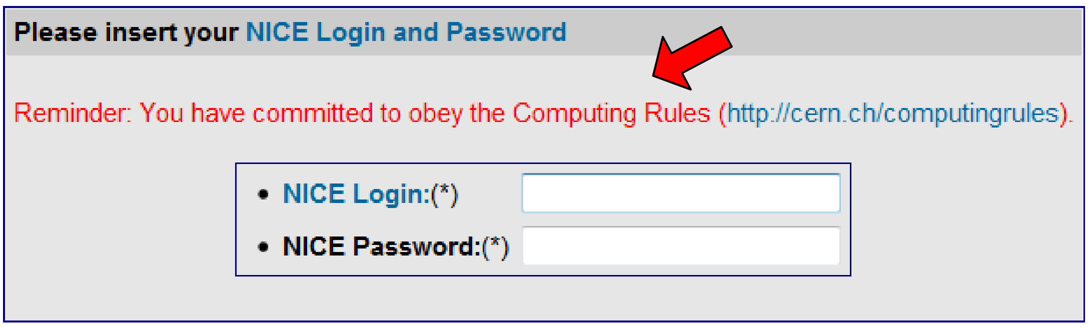
Security warnings are occasionally posted on CERN SSO Web page:



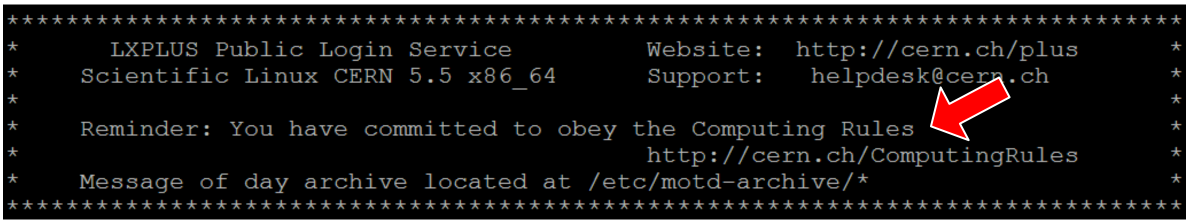
AIS (Administrative Information Services) log-in page:

EDMS (Engineering and Equipment Data Management System) log-in page:

CERN network management system log-in page:



Log-in banner at LXPLUS – CERN Public Interactive Linux Service:



Although not a log-in interface, the Service Status Board also includes occasional security alerts:

Appendix I Security articles in CERN Bulletin and Computer News Letter

This appendix lists articles on security-related topics that were published in CERN Computer News Letter (CNL) and in CERN Bulletin in previous years.

CERN Computer News Letter security articles since 2005**:**

- *"Siemens openlab team lays emphasis on cyber security analysis for industrial control systems"* by Tilaro, Filippo (CNL 2010-001)
- *"Attackers are on the prowl for your security weaknesses"* by Computer Security Team (CNL 2010-001)
- *"New training improves code quality and security"* by Computer Security Team (CNL 2009-004)
- *"Computer team advises reviewing your security now and frequently"* by CERN Computer Security Team (CNL 2009-003)
- *"Training on computer security keeps cyber attackers at bay"* by CERN Computer Security Team (CNL 2009-002)
- *"MS Forefront Client Security application starts to protect NICE PCs against virus attacks"* by Anti-virus Services (CNL 2009-002)
- *"Follow best practice for Windows file/folder security management"* by Lenski, Bruno (CNL 2009-001)
- *"Add-ons make surfing with Mozilla Firefox more secure"* by Iven, Jan (CNL 2009-001)
- *"Training on computer security keeps cyber attackers at bay"* by CERN Computer Security Team (CNL 2009-001)
- *"Phoney messages target CERN"* by CERN Computer Security Team (CNL 2008-004)
- *"Web attacks target instant messaging"* by IT Department (CNL 2008-003)
- *"IT strengthens reset password procedure"* by IT Department (CNL 2008-003)
- *"Fake mail targets CERN"* by CERN Computer Security Team (CNL 2008-002)
- *"Project gives integrated site security for Grids"* by Bradshaw, Kate (CNL 2008-002)
- *"Computer security: think before you click!"* by CERN Computer Security Team (CNL 2008-001)
- *"Computer security: think before you click!"* by CERN Computer Security team (CNL 2007-005)
- *"Twelve steps to improving control systems cyber security at CERN"* by Lüders, Stefan (CNL 2007-005)
- *"Web applications security: risks and countermeasures"* by Wartel, Romain (CNL 2007-005)
- *"Suggestions for designing and writing secure software"* by Lopienski, Sebastian (CNL 2007-004)
- *"IT strengthens firewall security"* by Heagerty, Denise (CNL 2007-003)
- *"CERN CA provides security"* by Ormancey, Emmanuel (CNL 2007-001)
- *"How to help keep you PC secure"* by Bradshaw, Kate (CNL 2007-001)
- *"CERN mail service requires secure protocols"* by The CERN Mail team (CNL 2006-005)
- *"Let Kerberos guard your password"* by Bradshaw, Kate (CNL 2006-005)

- *"Internet Services improve security"* by CNL Editors (CNL 2006-003)
- *"CERN tightens computer security"* by CNL Editors (CNL 2006-003)
- *"CERN urges mail clients to use secure protocols"* by The CERN mail team (CNL 2006-002)
- *"NonAdmin tackles Windows security"* by The NICE team (CNL 2006-001)
- *"CERN enforces Web-authoring encryption to ensure security"* by Lossent, Alexandre (CNL 2006-001)
- *"Account closure tightens security"* by Richards, Judy (CNL 2005-005)
- *"Keep your software updated and stay ahead of viruses"* by Richards, Judy (CNL 2005-005)
- "Use of VPN access puts CERN's security at risk" by Computer Security Team (CNL 2005-003)

CERN Bulletin security articles since 2005:

- *"And now, for the winners"* (Bulletin 27/2010)
- *"New computer security campaign"* (Bulletin 23/2010)
- *"Security needs you"* (Bulletin 23/2010)
- *"Computer Security Day"* (Bulletin 19/2010)
- *"Security scanning of Web sites at CERN"* (Bulletin 08/2010)
- *"Review your Computer Security Now and Frequently!"* (Bulletin 35/2009)
- *"The dangers of Twitter"* (Bulletin 32/2009)
- *"Recent "phishing" attacks"* (Bulletin 20/2009)
- *"CERN Technical Training: new courses on computer security"* (Bulletin 12/2009)
- *"Facing Two Rapidly Spreading Internet Worms"* (Bulletin 7/2009)
- *"Copyright and personal use of CERN's computing infrastructure"* (Bulletin 5/2009)
- *"Use of Tor (The Onion Router) disallowed from within CERN"* (Bulletin 41/2008)
- *"Closure of connection to off-site DNS services from within CERN"* (Bulletin 41/2008)
- *"New computer security measures"* (Bulletin 41/2008)
- *"CERN's Computing rules updated to include policy for control systems"* (Bulletin 39/2008)
- *"Change of Computer Security Officer"* (Bulletin 37/2008)
- *"Change in the CERN account password reset procedure"* (Bulletin 37/2008)
- *"CERN, AFS and PLUS credentials converge into a single credential pair"* (Bulletin 26/2008)
- *"Access to CERN from the Internet: termination of the VPN service"* (Bulletin 45/2007)
- *"End of Interactive Emailing from the Technical Network"* (Bulletin 45/2006)
- *"AIS authentication"* (Bulletin 41/2006)
- *"E-mail security: mail clients must use encrypted protocols"* (Bulletin 17/2006)
- *"New Procedures for the Management of Computer Accounts"* (Bulletin 17/2006)
- *"E-mail security: new restriction on attachments"* (Bulletin 09/2006)
- *"Improving Windows desktop security - the 'Non-Admin' Project"* (Bulletin 50/2005)
- *"Monday 9 January 2006: RESTRICTED ACCESS to the Technical Network"* (Bulletin 47/2005)
- *"Secure external access to CERN's services to replace VPN"* (Bulletin 26/2005)
- *"Restrictions on running IRC (Internet Relay Chat) at CERN"* (Bulletin 04/2005)

List of figures

List of tables

Bibliography

[1]. **Brenner, Bill.** Why Security Matters Now. *CIO Magazine.* 15 Oct 2009. http://www.cio.com/article/504837/Why_Security_Matters_Now.

[2]. **Leyden, John.** Culture of insecurity blamed for HMRC data loss. *The Register.* [Online] 25 Jun 2008. http://www.theregister.co.uk/2008/06/25/hmrc_data_loss_reports/.

[3]. HMRC Data Loss Scandal. *Safe from scams.* [Online] http://www.safefromscams.co.uk/hmrc-data-loss-scandal.html.

[4]. CERN in a nutshell. [Online] http://cern.ch/public/en/About/About-en.html.

[5]. The Large Hadron Collider. [Online] http://cern.ch/public/en/LHC/LHC-en.html.

[6]. Where the Web was born. [Online] http://cern.ch/public/en/About/Web-en.html.

[7]. A global endeavour. [Online] http://cern.ch/public/en/About/Global-en.html.

[8]. **Phifer, Lisa.** Top Ten Data Breaches and Blunders of 2009. *eSecurity Planet.* [Online] 8 Feb 2010. http://www.esecurityplanet.com/features/article.php/3863556/Top-Ten-Data-Breaches-and-Blunders-of-2009.htm.

[9]. **Werlinger, Rodrigo, Hawkey, Kirstie and Beznosov, Konstantin.** An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security.* 2009, Vol. 17, 1, pp. 4-19.

[10]. **Paloma, Jay.** Windows Server 2008 in an Organization's Defense in Depth Strategy . *Microsoft TechNet.* [Online] 12 Dec. 2007. http://technet.microsoft.com/en-us/library/cc512681.aspx.

[11]. **Anderson, Ross.** *Security Engineering.* Indianapolis, IN : Wiley, 2008.

[12]. **Chuvakin, Anton and Peikari, Cyrus.** *Security Warrior.* Sebastopol, CA : O'Reilly, 2004.

[13]. **Schneier, Bruce.** *Secrets and Lies.* Indianapolis, IN : Wiley, 2004.

[14]. **Leach, John.** Improving user security behaviour. *Computers & Security.* Dec 2003, Vol. 22, 8, pp. 685-692.

[15]. **ANSSI.** EBIOS - bases de connaissances. [Online] 25 Jan 2010. http://www.ssi.gouv.fr/IMG/pdf/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf.

[16]. **Landoll, Douglas J.** *The Security Risk Assessment Handbook.* Boca Raton, FL : Auerbach Publications, 2006.

[17]. **Smith, David J.** *Reliability, Maintainability and Risk.* Burlington, MA : Butterworth-Heinemann, 2001.

[18]. **Schneier, Bruce.** *Beyond Fear.* New York, NY : Copernicus Books, 2003.

[19]. **Lacey, David.** *Managing the Human Factor in Information Security.* Chichester, England : Wiley, 2009.

[20]. **Mitnick, Kevin D and Simon, William L.** *The Art of Deception.* Indianapolis, IN : Wiley, 2002.

[21]. **Mann, Ian.** *Hacking the human.* Hampshire, England : Gower, 2008.

[22]. **Shiels, Maggie.** Malicious insider attacks to rise. *BBC News.* [Online] 11 Feb 2009. http://news.bbc.co.uk/2/hi/technology/7875904.stm.

[23]. HSBC admits huge Swiss bank data theft. *BBC News.* [Online] 11 Mar 2010. http://news.bbc.co.uk/2/hi/business/8562381.stm.

[24]. *Human Factors in Information Security conference.* [Online] http://www.humanfactorsinsecurity.com.

[25]. *Human Aspects of Information Security and Assurance symposium.* [Online] http://www.haisa.org.

[26]. *Security and Human Behaviour workshop.* [Online] http://www.cl.cam.ac.uk/~rja14/shb10/.

[27]. **Weise, Joel.** *Developing a Security Policy.* [Online] Dec 2001. http://www.sun.com/blueprints/1201/secpolicy.pdf.

[28]. **Krutz, Ronald L.** *Securing SCADA Systems.* Indianapolis, IN : Wiley, 2006.

[29]. *Information Security Awareness Forum.* [Online] http://www.theisaf.org.

[30]. *OnGuard Online.* [Online] http://www.onguardonline.gov/.

[31]. **Hinson, Gary.** Human factors in information security. *Infosec Writers.* [Online] 2003. http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf.

[32]. **Henry, Kevin.** The Human Side of Information Security. [book auth.] ed. Harold F. Tipton and ed. Micki Krause. *Information Security Management Handbook.* Boca Raton, FL : Auerbach Publications, 2004.

[33]. **Herley, Cormac.** So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *Microsoft Research.* [Online] 2009. http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf.

[34]. **Contos, Brian.** Can we really stop malicious insiders? *NetworkWorld.* [Online] 29 Sept 2008. http://www.networkworld.com/columnists/2008/092908insider.html.

[35]. **Deloitte.** Protecting what matters. The 6th Annual Global Security Survey. [Online] 2009. http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_fsi_GlobalSecuritySurvey_0901.pdf.

[36]. **Schein, Edgar H.** *Organizational Culture and Leadership.* San Francisco, CA : Jossey-Bass, 2004.

[37]. **Johnson, Larry and Phillips, Bob.** *Absolute Honesty: Building a Corporate Culture that Values Straight Talk and Rewards Integrity.* New York, NY : Amacom, 2003.

[38]. Organizational culture. *Symphony Orchestra Institute.* [Online] http://www.soi.org/reading/change/culture.shtml.

[39]. **Khan, Asim.** Matching People with Organizational Culture. [Online] 2005. http://www.themanager.org/HR/Matching_People_with_Organizational_Culture.pdf.

[40]. *A fuzzy approach to value and culture assessment and an application.* **Soyer, Ayberk, Kabak, Ozgur and Asan, Umut.** 2, 2007, International Journal of Approximate Reasoning, Vol. 44, pp. 182-196.

[41]. **Schabracq, Marc J.** *Changing Organizational Culture.* Chichester, England : Wiley, 2007.

[42]. **Wattanajantra, Asavin.** Is Apple's corporate culture a security risk? . *IT Pro.* [Online] 17 Jul 2009. http://www.itpro.co.uk/612901/is-apples-corporate-culture-a-security-risk.

[43]. The Toyota Way. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/The_Toyota_Way.

[44]. Some say GM needs shake-up of corporate culture. *The Washington Times.* [Online] 3 Mar 2009. http://www.washingtontimes.com/news/2009/mar/3/some-say-gm-needs-shake-up-of-corporate-culture/.

[45]. **Heathfield, Susan M.** Culture: Your Environment for People at Work. *About.com.* [Online] http://humanresources.about.com/od/organizationalculture/a/culture.htm.

[46]. **Hofstede, Geert.** *Culture's Consequences; Comparing Values, Behaviors, Institutions and Organizations Across Nations.* Thousand Oaks, CA : Sage Publications, 2001.

[47]. **Sonnenfeld, Jeffrey.** *The Hero's Farewell.* New York, NY : Oxford University Press, 1988.

[48]. **Sadri, Golnaz and Lees, Brian.** Developing corporate culture as a competitive advantage. *Journal of Management Development.* 2001, Vol. 20, 10, pp. 853-859.

[49]. **Cameron, Kim S. and Quinn, Robert E.** *Diagnosing and changing organizational culture.* Reading, MA : Addison-Wesley, 1999.

[50]. **Deloitte.** Global Security Survey. [Online] 2005. http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/2005%20Global%20Security%20Survey.new.pdf.

[51]. **Thomson, Kerry-Lynn, Solms, Rossouw von and Louw, Lynette.** Cultivating an organizational information security culture. *Computer Fraud & Security.* Oct 2006, Vol. 2006, 10, pp. 7-11.

[52]. **Ruighaver, A.B., Maynard, S.B. and Chang, S.** Organisational security culture: Extending the end-user perspective. *Computers & Security.* Feb 2007, Vol. 26, 1, pp. 56-62.

[53]. **Rapkin, Gordon.** Building a security culture. *SC Magazine.* [Online] 5 Jun 2008. http://www.scmagazineus.com/building-a-security-culture/article/110970/.

[54]. **Dojkovski, Sneza, Lichtenstein, Sharman and Warren, Matthew John.** Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. 2007.

[55]. **Schneier, Bruce.** Inside the Twisted Mind of the Security Professional. *Wired.* [Online] 20 Mar 2008.
http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0320.

[56]. **Styles, Martyn and Tryfonas, Theo.** Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. *Information Management & Computer Security.* 2009, Vol. 17, 1, pp. 44-52.

[57]. **OECD.** OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. [Online] 2002. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

[58]. **Lim, Joo Soon, et al.** Embedding information security culture - emerging concerns and challenges. 2010.

[59]. **Chia, P., Maynard, S. and Ruighaver, A.B.** Understanding Organisational Security Culture. [book auth.] M. G. Hunter and K. K. (eds.) Dhanda. *Information Systems: The Challenges of Theory and Practice.* Las Vegas, NV : Information Institute, 2003, pp. 335-365.

[60]. *Exploring the Relationship between Organizational Culture and Information Security Culture.* **Lim, Joo S., et al.** Perth, Australia : s.n., 2009. Proceedings of the 7th Australian Information Security Management Conference.

[61]. **Yeh, Quey-Jen and Chang, Arthur Jung-Ting.** Threats and countermeasures for information system security: A cross-industry study. *Information & Management.* Jul 2007, Vol. 44, 5, pp. 480-491.

[62]. **Amit.** 20 Examples Of Core Values. *Mystic Madness.* [Online] 2010. http://www.mysticmadness.com/20-examples-core-values.html.

[63]. **Microsoft.** Trustworthy Computing. [Online] http://www.microsoft.com/about/twc/en/us/default.aspx.

[64]. **F.D.N.Y.** Mission Statement of the New York City Fire Department. [Online] http://nyc.gov/html/fdny/html/general/mission.shtml.

[65]. **Securitas.** Our Management Model - Values. [Online] http://www.securitas.com/en/About-Securitas/Our-Management-Model/Values/.

[66]. **Xe Services.** Business Ethics - Statement of Core Values. [Online] http://www.xeservices.com/WhyXe/BusinessEthicsandCompliance.aspx.

[67]. **UBS.** Code of Business Conduct and Ethics of UBS. [Online] http://www.ubs.com/1/ShowMedia/about/code_of_conduct?contentId=152516&name=Code%20of%20Business%20Conduct%20and%20Ethics%20of%20UBS.pdf.

[68]. **Cisco.** Code of Business Conduct. [Online] http://investor.cisco.com/documentdisplay.cfm?DocumentID=3263.

[69]. *First-Order, Second-Order, and Third-Order Change and Organization Development Interventions: A Cognitive Approach.* **Bartunek, Jean M. and Moch, Michael K.** 4, 1987, Journal of Applied Behavioral Science, Vol. 23, pp. 483-500.

[70]. **Kotter, John.** *Leading change.* Boston, MA : Harvard Business School Press, 1996.

[71]. **Cummings, Thomas and Worley, Christopher.** *Organization Development and Change.* Mason, OH : Thomson / South-Western, 2004.

[72]. Organizational culture and change. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Organizational_culture#Organizational_culture_and_change.

[73]. **Moussa, Mario.** What Every Security Executive Should Know about Corporate Culture. *SecurityInfoWatch.com.* [Online] 6 Feb 2009. http://www.securityinfowatch.com/root+level/1284252.

[74]. *Understanding Transition towards Information Security Culture Change.* **Ngo, Leanne, Zhou, Wanlei and Warren, Matthew.** Perth, Australia : Edith Cowan University, 2005. in Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference,. pp. 67-73.

[75]. *Strategy, technology, and social processes within professional cultures: A negotiated order, ethnographic perspective.* **Fischer, Michael J. and Dirsmith, Mark W.** 4, 1995, Symbolic Interaction, Vol. 18, pp. 381-412.

[76]. Careers at CERN. [Online] http://cern.ch/jobs.

[77]. Human resources security. [Online] http://it.med.miami.edu/x2229.xml.

[78]. *ISO/IEC 27002:2005(E) - Code of practice for information security management.* s.l. : ISO, 2005.

[79]. Code of conduct. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Code_of_conduct.

[80]. **Tremblay, Michel, ed.** *Mobilisation des personnes au travail.* Montréal, Canada : HEC Montréal, 2008.

[81]. CERN School of Computing. [Online] http://cern.ch/csc.

[82]. CERN Summer Students Lecture Programme 2010. [Online] http://indico.cern.ch/scripts/SSLPdisplay.py?stdate=2010-07-05&nbweeks=7.

[83]. openlab summer student program 2010. [Online] http://cern.ch/openlab-mu-internal/07_Student-Programme/2010/Student-programme_lectures_2010/07-01_Summer_student_lectures.htm.

[84]. CERN Computing Colloquia. [Online] http://cern.ch/it-dep/colloquia/.

[85]. CERN Computing Seminars. [Online] http://cern.ch/cseminar/.

[86]. CERN Academic Training. [Online] http://cern.ch/hr-training/acad/default.asp.

[87]. CHEP 2010 - 18th International Conference on Computing in High Energy and Nuclear Physics. [Online] http://event.twgrid.org/chep2010.

[88]. HEPiX. [Online] https://www.hepix.org/.

[89]. *CERN Computing Rules.* [Online] http://cern.ch/ComputingRules.

[90]. *CERN Bulletin.* [Online] http://cdsweb.cern.ch/journal/CERNBulletin/.

[91]. *CERN Computer News Letter.* [Online] http://cern.ch/cnl/.

[92]. *CERN Computer Security Day 2010.* [Online] http://cern.ch/SecDay/2010.

[93]. Typosquatting. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Typosquatting.

[94]. *Measuring organizational cultures: A qualitative and quantitative study across twenty cases.* **Hofstede, G., et al.** 2, 1990, Administrative Science Quarterly, Vol. 35, pp. 286-316.

[95]. Organizational culture. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Organizational_culture.

[96]. Organizational Culture Assessment Instrument (OCAI) online. [Online] http://www.ocai-online.com/.

[97]. **Pradnya, S.** Types of Organizational Culture. *Buzzle.com.* [Online] http://www.buzzle.com/articles/types-of-organizational-culture.html.

[98]. *Understanding Information Security Culture: A Conceptual Framework.* **Niekerk, Johan Van and Solms, Rossouw von.** 2006. Proceedings of the ISSA 2006 conference. pp. 1-10.

[99]. **Native Intelligence, Inc.** Security Awareness Slogans, Mottos, Tag lines, Catch Phrases, Maxims... [Online] http://www.nativeintelligence.com/ni-free/awareness-slogans.asp.

[100]. Computer emergency response team. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Computer_emergency_response_team.

[101]. Ajax (programming). *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Ajax_%28programming%29.

[102]. Grid Café. [Online] http://www.gridcafe.org/.

[103]. Application firewall. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Application_firewall.

[104]. Particle physics. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Particle_physics.

[105]. CERN openlab. [Online] http://cern.ch/proj-openlab-datagrid-public/.

[106]. *Indico.* [Online] http://indico-software.org/wiki/WikiStart.

[107]. *Quattor.* [Online] https://trac.lal.in2p3.fr/Quattor/wiki.

[108]. *Lemon monitoring system.* [Online] http://cern.ch/lemon.

[109]. *Static Code Analysis Tools - recommendations.* [Online] http://cern.ch/security/recommendations/en/code_tools.shtml.

[110]. *EBIOS 2010.* [Online] http://www.ssi.gouv.fr/site_article173.html.

[111]. ITIL - Problem Management. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Problem_Management.

[112]. **ENISA.** *Information Security Awareness – Insight and Guidance for Member States.* s.l. : ENISA/European Network and Information Security Agency, 2007.

[113]. **Bruce, Anne.** *How to Motivate Every Employee.* New York : McGraw-Hill, 2003.

[114]. *Operational Circular no. 5.* [Online] http://cern.ch/security/rules/en/OC5_english.pdf.

[115]. Internationalization and localization. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Internationalization_and_localization.

[116]. Computer accessibility. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Computer_accessibility.

[117]. aaa. [Online]

About the author

Sebastian Lopienski is the deputy Computer Security Officer at CERN (European Laboratory for Particle Physics, based near Geneva, Switzerland). He works on security strategy and policies; offers internal consultancy and audit services; develops and maintains security tools for vulnerability assessment and intrusion detection; provides training and awareness raising; and does incident investigation and response.

During his work at CERN since 2001, Sebastian has had various assignments, including designing and developing software to manage and support services hosted in the CERN Computer Centre; providing Central CVS Service for software projects at CERN; and development of applications for accelerator controls in Java. He also worked in a software company in Warsaw, Poland, designing and implementing Web and Internet solutions. He graduated from the Computer Science Faculty of Warsaw University (Master of Science thesis on Distributed Computing in Java).

His professional interests include software and network security, distributed systems, and human aspects of information security. In his free time, he enjoys spending time with his family, as well as sailing in regattas and cruising on the sea. He is also a keen skier, photographer and backpacker.

Contact with the author: Sebastian.Lopienski@cern.ch