LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Facoltà: Economia e Management
Cattedra: Organizzazione dei sistemi informativi aziendali

Information Security: combining prevention and response paradigms against predictable and unpredictable risks.

RELATORE
Prof. Paolo Spagnoletti

CANDIDATA
Chiara Alessandrini
146961

ANNO ACCADEMICO 2010/2011

Contents

List of figures and tables

Abstract

Among the challenges of conducting their businesses on the Internet, companies continuously deal with information security issues. The Decalogue of the e-risks is well-known. Firms have the possibility to choose a tailored IS model, according to the specific nature of their businesses, their evaluation of the risk, and their willingness to risk.

Nevertheless mass media show that cybercrime is sadly increasing. In 2009 the victims of identity theft and related fraud have been around 11, 2 million, for an estimated cost of $54 billion U.S. dollars (Crunchgear.com).

Which is the focus of the organizations during “the before and after” incident? What do organizations put in place in order to prevent the attack?

What happens after? How does an organization revive from an attack? How does it response? Does it learn the lesson?

Academics and practitioners have explored this topic just in part, because of the lack of publicly available data. In fact, the victims of cybercrime are reluctant in coming out and revealing themselves for fear of losing public confidence and other attackers may exploit the same or similar vulnerabilities.

The growing importance of the phenomenon is forcing these firms to disclose their attack data. Furthermore, a number of organizations have started to provide security advisories in order to protect business and government information systems. They mostly address IS engineers that are concerned in eliminating technical vulnerabilities and flaws.

But is technology the only aspect to stress?

The TFI model (Åhlfeldt et al., 2007) shows the importance of two other dimensions of Security: in addition to technology, it is no longer possible to overlook the formal and the informal components of the system.

The InfoSec management literature has been investigating two paradigms, mostly depending on the context: in organizations related to the military, the so-called Information Warfare (IW) paradigm dominates the thinking (Baskerville, 2005), while in commercial, government, and not-for-profit organizations (the non-military contexts), the Business Information Systems Security (BISS) paradigm has more resonance.

At the basis of these two paradigms there are substantially different assumptions about security risks that lead to adopt different safeguards and countermeasures.

Established the complementarity of IW and BISS even in non-military contexts, in this work I’m going to uncover the eventual relationships among the two paradigms and the security countermeasures suggested by the TFI model.

1. Research motivation

"*We're a somewhat known band of pirate-ninjas. Some time ago, we were traversing the Internet for signs of enemy fleets. While you aren't considered an enemy - your work is of course brilliant - we did stumble upon several of your admin passwords which are as follows*" (Neal, 2011).

How would you react if you were the head of the information systems in question? Which would it be your next move?
In the net of these pirates there are big names like Sony, Nintendo, PBS's news website, UK ATM Database, the Arizona Department of Public Safety, the FBI, the United States Senate, etc..
They have smartly crippled entire organizations making fun of them on Twitter, attracting supporters all around the world.
June 25, 2011: The Boat docks at the port:

"*50 days ago, we set sail with our humble ship on an uneasy and brutal ocean: the Internet. The hate machine, the love machine, the machine powered by many machines. We are all part of it, helping it grow, and helping it grow on us. (...) It's time to say bon voyage. Our planned 50 day cruise has expired*" (Pastebin.com).

This should be LulzSec's final *release*.
But they are not the only criminal organization that infests our cyberspace. Security breaches are sadly becoming uncountable.
Reuters (June 24, 2011) reports that Several Brazilian government sites have been attacked including the presidency, the sports ministry and the tax collection agency. The latest target was the Brazilian statistics agency (Reuters.com).

Defense News, the well-known newsweekly on politics, business and technology, published by the Defense News Media Group (part of Gannett Company), has been hacked (June 29, 2011), as reported in Databreaches.net. DefenseNews' subscribers (active and retired military personnel, defense contractors and others in both the U.S. and other countries' defense establishments) have been stolen of their first and last name, user ID, password, email address, the internal number assigned to the account, and, if provided, ZIP code, duty status, pay grade, and branch of service.
A message to its subscribers appeared on Militarytimes.com invites them to reset or strengthen their passwords on their Gannett Government Media Corporation or Military Times, Defense News or Federal Times accounts, as well as their other online accounts, particularly those that use the same email address used for

Gannett Government Media Corporation account as a user name or account identifier. The message continues ensuring that Gannett Corporation is working together with an outside computer forensics company in order to investigate the breaches and strengthen its security controls.

Moreover, Google has recently unmasked hackers from Jinan (China) that were targeting US Government Gmail accounts via phishing attempts. J. Aron (2011) reports that the attackers were attempting to monitor their victims' email accounts by changing the settings to automatically forward messages (Newscientist.com). Victims received messages appearing to be sent from someone they knew, and then their contents mimicked the familiar Gmail interface for downloading attachments.

The official Google blog itself warns its users to be alert and aware about the myriad of traps in which they may stumble:

"The Internet has been an amazing force for good in the world—opening up communications, boosting economic growth and promoting free expression. But like all technologies, it can also be used for bad things. Today, despite the efforts of Internet companies and the security community, identity theft, fraud and the hijacking of people's email accounts are common problems online. Bad actors take advantage of the fact that most people aren't that tech savvy—hijacking accounts by using malware and phishing scams that trick users into sharing their passwords, or by using passwords obtained by hacking other websites." (Googleblog.blogspot.com)

No one seems to be sheltered from attacks, no company, government, organization.

TJX, T.J. Maxx, And Marshalls, CardSystems Solutions, Bank Of New York Mellon, HM Revenue & Customs, U.S. Department Of Veterans Affairs are only few examples of *massive* security breaches enlisted by J. Widman in a recent article appeared on Informationweek.com.

A *security breach* is an act from outside an organization that bypasses or contravenes security policies, practices, or procedures. A similar *internal* act is called *security violation*.

Sometimes victims don't even know they have been breached, as M. Schwartz warns in a recent article of InformationWeek.com. 41% of victims cannot determine how frequently they are targeted by advanced attacks, and half of them take at least a month to detect such attacks.

Another recent study conducted by Eric M. Eisenstein (2007) shows that only the so-called *identity theft* costs corporations over $20 billion per year, and

consumers are forced to spend over $2 billion and 100 million hours of time to deal with the aftermath.
Already only in 2003 the costs related to identity theft for businesses and consumers were around $48 billion (Scambusters.org), and are dramatically increasing.

There is much confusion among users. If the digital identity theft and the other security breaches continue to rise up out of the control, users will quickly lose their confidence in e-Commerce and e-Business, and this is a risk that the market cannot afford to run.

In 1999 Darcy DiNucci coined the term “Web 2.0” explaining how the web was changing into a dynamic virtual world of interaction and collaboration, the Web as we know it now. It was clear that it came with great risks for both consumers and companies, and that information security issues could greatly harm a company’s brand image and consumers trust.

Today, the growing importance of this phenomenon is forcing victims to disclose their attack data. Furthermore, a number of organizations have started to provide security advisories in order to protect business and government information systems.
In this respect, the 2009 industry report of the Secure Enterprise 2.0 Forum lists the Top 8 Web 2.0 Security Threats or Vulnerabilities (Perez, 2009):

1. Insufficient Authentication Controls. For the British Standards Institution, *authentication* is the first basic requirement of an application security, identifying and proving that the identity is as claimed. In the e-Business environment, authentication may be provided by the use of a PKI (Public Key Infrastructure), key certificates, trust hierarchies, etc. (Papazoglou, Ribbers 2010).

2. Cross Site Scripting (XSS). Attackers bypass security measures of web sites putting dangerous scripts. In this way, an attacker can gain access to sensitive pages (e.g. logging into bank website) and information. “At risk are blogs, social networks, and wikis. An example of this attack from last year was the Yahoo HotJobs XSS vulnerability exploit, where hackers obfuscated JavaScript to steal session cookies of victims. Last year and in previous years, XSS worms were also to blame for attacks on Orkut, MySpace, Justin.tv, the report states.

3. Cross Site Request Forgery (CSRF). A consumer accesses a malicious Website, and while he/she is browsing it, the website's code automatically request access to sites where the consumer is authorized. In other words the website does requests to other sites (where authorization is normally necessary) on behalf of the victim. Due to heavy use of AJAX, Web 2.0 applications seem to be potentially more vulnerable to this type of attacks.

4. Phishing. A victim receives an email with a request to install a deceptive application, or is redirected to a deceptive website where he/she has to fill in a form with personal information.

5. Information Leakage. People inadvertently post something on the Internet (think at the massive- and often *hasty*- use of social networks) that is considered sensitive by their employers. Web 2.0 brought this problem as it stimulates interaction and information sharing.

6. Injection Flaws like XML injection, XPath injection, JavaScript injection, and JSON injection.

7. Information Integrity is about losing integrity due to malicious attacks, but also due to placing misinformation the web. According to Mani's definition (2002) *integrity* is one of the major requirements for supporting QoS in e-Business, referring to the conformance with its description or service-level agreements, SLAs.

8. Insufficient Anti-automation. Attacks are automated, for example through CSRF, but also automatically opening email account and phishing (Rosenberg, 2009).

The Open Web Application Security Project provides a somewhat different list for 2010. Top 10 Web Application Security Risks are, in order: Injection, Cross Site Scripting (XSS), Broken Authentication and Session Management, Insecure

Direct Object References, Cross Site Request Forgery (CSRF), Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection, Invalidated Redirects and Forwards (Owasp.org). It is interesting to see how each risk is *studied:* threat agents, attack vectors, security weakness, technical impacts, business impacts are the dimensions considered.

Injection, the first risk in the list, for example, is analyzed as follows:

Threat Agents	**Attack Vectors**	**Security Weakness**		**Technical Impact**	**Business Impact**
———	**Exploitability** **EASY**	**Prevalence** **COMMON**	**Detectability** **AVERAGE**	**Impact** **SEVERE**	———
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends simple text-based attacks that exploit the syntax of the targeted interpreter. Almost any source of data can be an injection vector, including internal sources	Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code, often found in SQL queries, LDAP queries, XPath queries, OS commands, program arguments, etc. Injection flaws are easy to discover when examining code, but more difficult via testing. Scanners and fuzzers can help attackers find them.		Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.	Consider the business value of the affected data and the platform running the interpreter. All data could be stolen, modified, or deleted. Could your reputation be harmed?

Figure 1. The Injection according to OWASP

Injection can be prevented keeping untrusted data separate from commands and queries.

Even if it’s not a complete defense, positive or "whitelist" input validation with appropriate canonicalization also helps protect against injection.

Anyway OWASP’s Enterprise Security API (ESAPI) makes its extensible library of white list input validation routines available to users.

If this is the treatment reserved for the injection, the second risk in the list -and the most prevalent web application security flaw- the Cross Site Scripting, has an average exploitability, a very widespread prevalence and an easy detectability. Anyone who can send untrusted data to the system (including external users, internal users, and administrators themselves) may become threat agents. In this regard, Content Security Protection (CSP) is a standard developed by Mozilla whose aim is to thwart XSS attacks at their point of execution, the browser. CSP is currently only supported by Firefox 4, Thunderbird 3.3 and SeaMonkey 2.1. Recently (March 22, 2011) Twitter has announced that CSP has been added to the mobile version, accessible under mobile.twitter.com. Users who use one of the aforementioned browsers are protected from XSS attacks on that website (Engineering.twitter.com).

This is an important step, as social networking sites like Twitter are particularly vulnerable.

People don’t expect to be scammed by other users and this makes them easy preys, injuring not just their own privacy, but even the IS security of the firms in which they work.

For example, Scambusters.org defines the five most common social networking scams that are: downloading malware, false identity, identity theft, profile page hacks and sending and receiving spam.

It is easy to understand that within a firm, and in particular an information security department (ISD), all the previous technical analysis of vulnerabilities and flaws, even the most accurate, becomes vain if the employees are not educated on security issues.

It has been proved that giving the possibility to share in a common platform *all* the personal information, social networks have dramatically increased the risks for employers (Sophos.com).

However academics and practitioners, dealing with the design of Information Security (InfoSec) models, have explored this topic just in part, mostly addressing IS engineers, concerned in removing *technical* vulnerabilities and flaws.

By now it should be clear that information security is a multidimensional discipline, and it’s misleading to limit the analysis at just the technical viewpoint. In fact, security has an extremely *wide range of other facets which must all be considered in creating a secure IT environment* (Basie von Solms, 2001). Talking about information security, the interdependency of its dimensions it’s quite obvious: the technical dimension alone with its countermeasures (i.e. encryption of data, firewalls, filter contents, intrusion detection systems, etc.) doesn’t make an IT environment secure. For example, without customization a firewall doesn’t have any value. It has to be based on some type of policy (policy dimension). This in turn requires some measurement system in order to be enforced (measuring and monitoring dimension) and a training course that makes end users *aware* about the above mentioned policy (awareness dimension). Within an organization, further dimensions (legal, human, ethical, and so on) can be found: it is no longer possible to overlook them.

Extending the InfoSec model, the TFI model (Åhlfeldt *et al.*, 2007) provides a holistic approach of the problem, and even a concrete guide in an eventual *post-attack* situation. It assumes that not just the technical aspects but even the formal and informal aspects of information security must be investigated. Actually, only starting from the informal aspects- that are the most context-related factors- it is possible to design policies, standards, procedures, etc., and *after* the technical solutions that are instead the most automated and standardized aspects.
Depending on the nature of the threat, the TFI model gives a series of security measures that preserve the confidentiality, integrity, availability and accountability of the information.

If technical measures could be enough against predictable risks, facing with the unpredictable ones the normal tools used, such as risk analysis, arithmetic probability, variance, and the like, fail in front of the *uniqueness* of the event.
In a context of deep uncertainty and unsettling news, where a security incident is an event in itself, an organization cannot learn from its past mistakes.
In the Business Information Systems Security (BISS) paradigm, as proposed by the accredited literature, there is a *static* relationship between risks and safeguards that is not reflected in this reality. Here, the relationship of safeguards to threats is not determinate but *consequential*, as Baskerville points out in his “Information Warfare” (2005).
According to his statements, another paradigm should guide the organization in building an adequate IS.
In those contexts where risks are *unpredictable*, *non-measurable* and *transient*, the Information Warfare (IW) paradigm can be of decisive importance, even in not-military settings.

Given the *duality* of Information Security Management (Spagnoletti, Resca, 2008) I’m going to investigate the relationships among the two paradigms (BISS and IW) as illustrated by Baskerville and the type of countermeasures/safeguards suggested by the TFI model as explained by Åhlfeldt, Spagnoletti and Sindre (2007) in their work “Improving the Information Security Model by using TFI”.

Is it true that if the organization (that is a military organization, but even a company, a government, an association) faces unpredictable threats most likely it will adopt the IW paradigm? In case of predictable threats instead, is it sufficient to prevent its IS just with technical countermeasures? Which are the safeguards related to formal and informal aspects in the TFI model? Which is the role they play within the two paradigms?

And at the end is it possible or useful to combine and mix the two paradigms within an organization?

In the third chapter I'm going to explain the method I used in my empirical research and the structure of the upcoming interview.

The fourth chapter then will show the data analysis resulting from the abovementioned case study and my conclusions.

2. Theoretical background

Currently many risk management methods and techniques, based on security risk analysis and assessment, are available for organizations. In a positivistic perspective, standards and best practises have defined ready-made models that companies and organizations in general should follow to protect their information assets.

In this regard, in 1987 the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) formed a Joint Technical Committee, known as ISO/IEC JTC1 in order to develop worldwide ICT standards for business and consumer applications and provide the standards approval environment for integrating diverse and complex ICT technologies. From its birth to the present, a lot of progress has been made. Today an organization that is going to implement (or change) its own information security management system (ISMS) usually draws inspiration from ISO/IEC 27001:2005 that establishes the fundamental requirements of an ISMS and ISO/IEC 27002:2005. These standards address all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). The former in particular is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. It helps in formulating security requirements and objectives, ensuring that security risks are cost effectively managed, defining new information security management processes, etc. (Iso.org).

Developed from BS7799 and ISO 17799, the latter instead provides for the conservation and protection of information resources of an enterprise. It is divided in twelve sections containing best practice recommendations for all those responsible for establishing, maintaining and updating the ISMS. Together with the other ISO/IEC 27000-series standards it provides guidelines about risk assessment, security policy, physical and environmental security, and so on.

The ultimate goal of the standards is to safeguard the three widely accepted attributes of information assets (Papazoglou, Ribbers, 2010):

- Confidentiality: an unauthorized person cannot view or interfere with a communication between two or more parties.

- Integrity: safeguards the accuracy and completeness of the information, ensuring that data cannot be corrupted or modified.

- Availability: all normal services should be available, even in adverse situations.

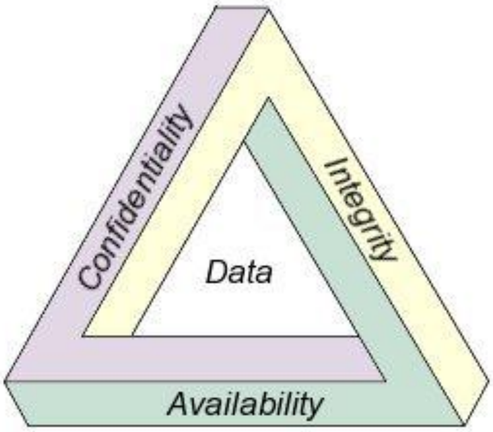


Figure 2. CIA, the widely used benchmark for evaluating information systems security (ISSWG, 2011).

Sometimes other attributes are added, such as auditability, accountability, scalability, and the like.

Auditability means that operations on content must be transparent and capable of being proven: the information must readily be audited to check if it conforms to the standards specified, even when there are interruptions.

Accountability is the capability of recognizing a single user who is responsible for the operations performed within the system.

Scalability refers to the ability to consistently serve the requests despite variations in the volume of requests.

In e-Business communication, a QoS (quality of service) plan is often used as a critical instrument for creating a reliable environment. Among the major requirements for supporting QoS in e-Business security, there is the *conformance to standards*. For instance, service provider must stick to standards outlined in the SLAs. This concept is used in cloud computing too, where service level agreements help in controlling the use and receipt of computing resources from, and by, third parties.

To be certified compliant with ISO/IEC 27001 an ISMS has to pass an audit process that could be synthesized in figure 2.

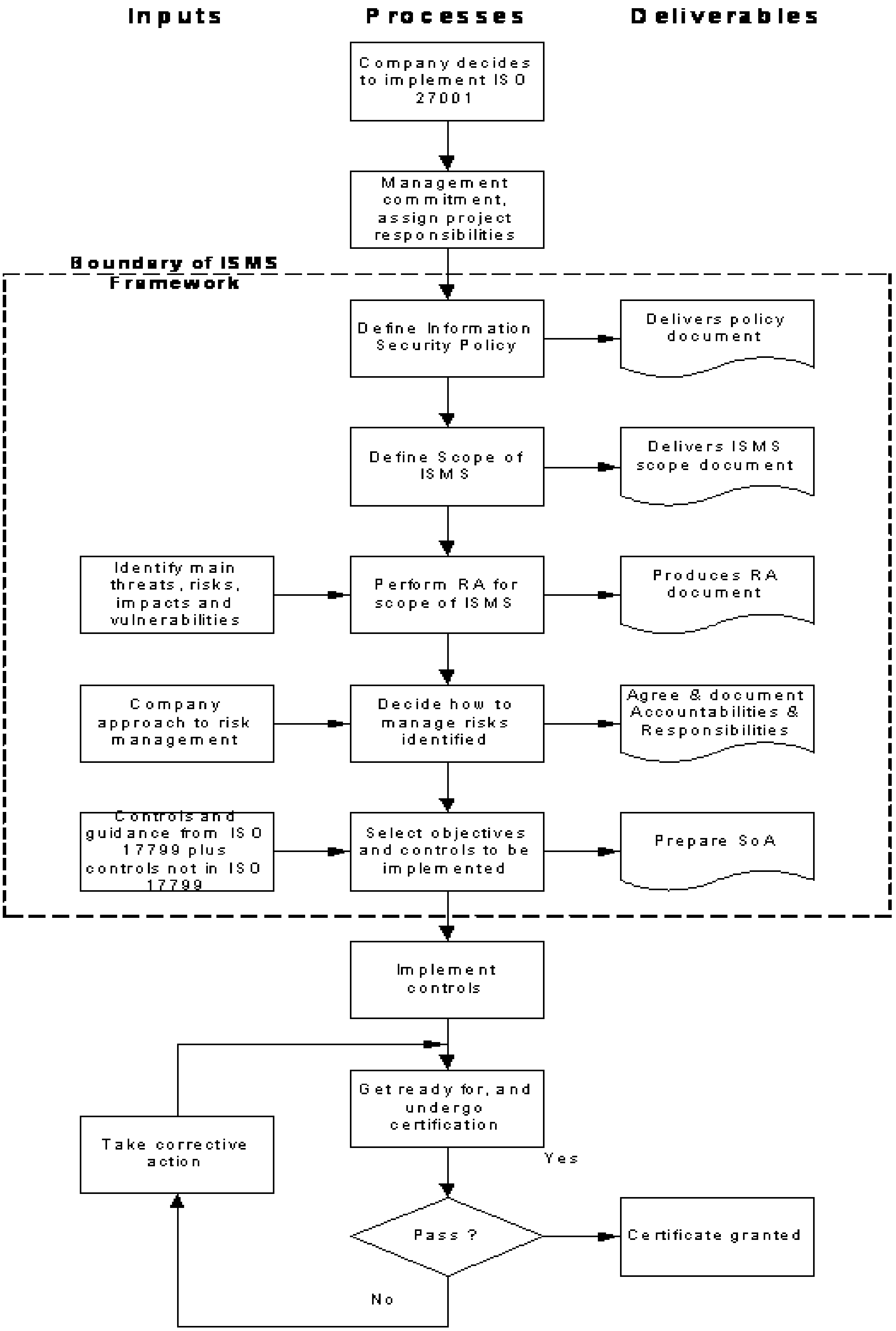

Inputs
Processes
Deliverables
Company decides to implement ISO 27001
Management commitment, assign project responsibilities
Boundary of ISMS Framework
Define Information Security Policy
Delivers policy document
Define Scope of ISMS
Delivers ISMS scope document
Identify main threats, risks, impacts and vulnerabilities
Perform RA for scope of ISMS
Produces RA document
Company approach to risk management
Decide how to manage risks identified
Agree & document Accountabilities & Responsibilities
Controls and guidance from ISO 17799 plus controls not in ISO 17799
Select objectives and controls to be implemented
Prepare SoA
Implement controls
Get ready for, and undergo certification
Take corrective action
Yes
Pass ?
Certificate granted
No

Figure 3. The logical flow of the ISO27001 Certification Process, according to 27000.org

ISO/IEC 27001 incorporates several “Plan-Do-Check-Act” (PDCA) or Deming cycles.
This testifies to the importance attributed to an ongoing process resulting in continuous *quality improvement*, as shown in figure 4:

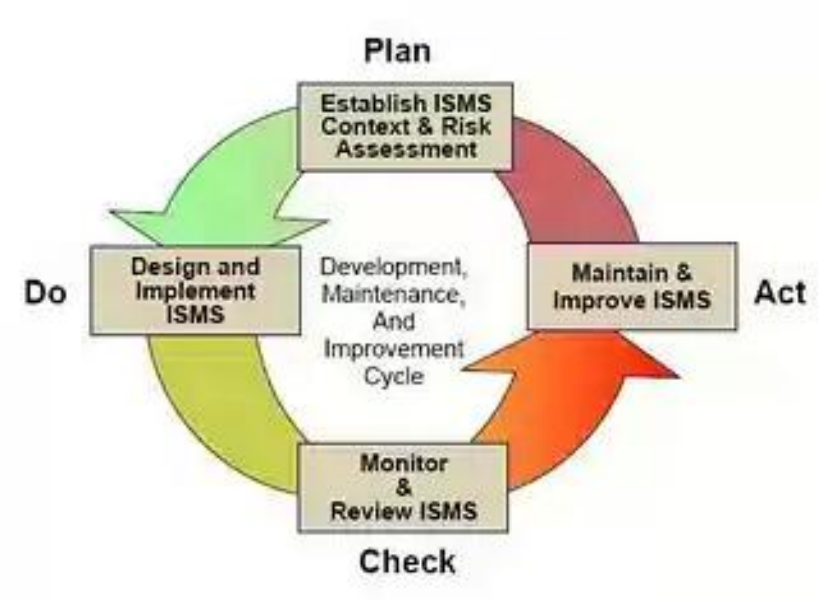

Plan
Establish ISMS Context & Risk Assessment
Do
Design and Implement ISMS
Development, Maintenance, And Improvement Cycle
Maintain & Improve ISMS
Act
Monitor & Review ISMS
Check

Figure 4. PDCA and continuous improvement process (Stefaniu, 2007)

In PDCA cycles related to information security, “Plan” refers to all the activities like the design of ISMS, risk assessment, identification of the acceptable levels of risks, selection of appropriate countermeasures, and so on.
“Do” means the implementation of the controls chosen.
“Check” signifies review, monitoring, performance reevaluation.
Lastly, “Act” implies all the changes that the organization should adopt on the basis of the results deriving from the check phase.

In which way can a correct ISMS implementation take place? How to configure here an ISO 27001 certification process?
The roadmap proposed by ISO27001security.com gives a clear picture of the actions an organization has to perform if it had decided to implement an ISMS ISO27001 compliant.
First it has to be clear that information security is not a “snapshot” and modifications of the system could be inevitable: the organization must be prepared to deal with events and changes affecting the environment, legal compliance, new policies and regulations, etc.

Risk analysis is “conditio sine qua non” for traditional risk assessment processes, as recommended by ISO27001 standard. It’s the first step, essential to ensure that controls and expenditure are fully commensurate with the risks to which the organization is exposed.

Risk analysis involves *identification* of the threats that could really occur and *analysis* of the related vulnerabilities of the organization to these threats. How much does a specific threat cost in term of loss of revenue, reputation, etc.? And the related countermeasures? Is it *convenient* to protect the firm from it? Which is the level of risk admitted by the organization?

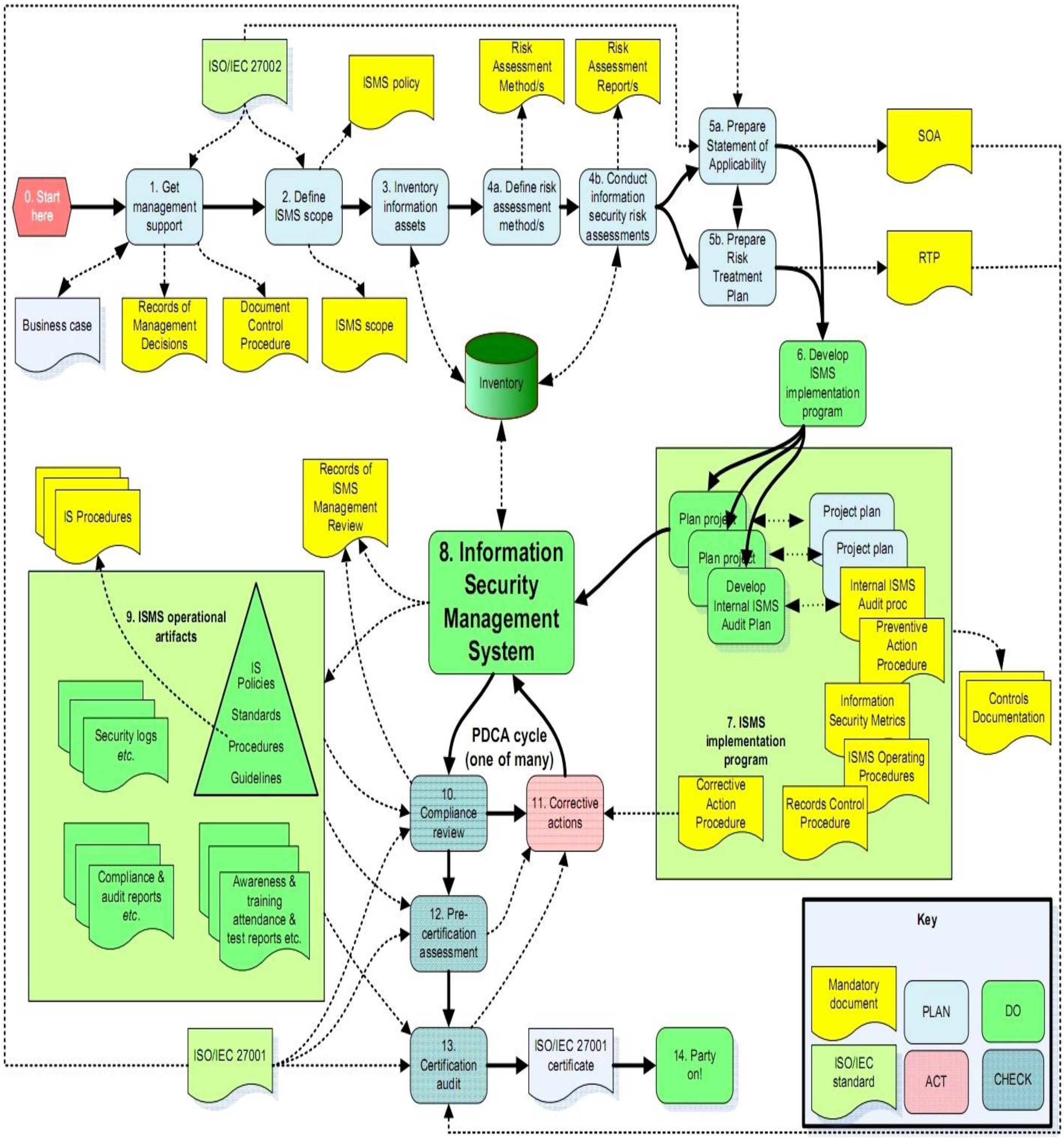
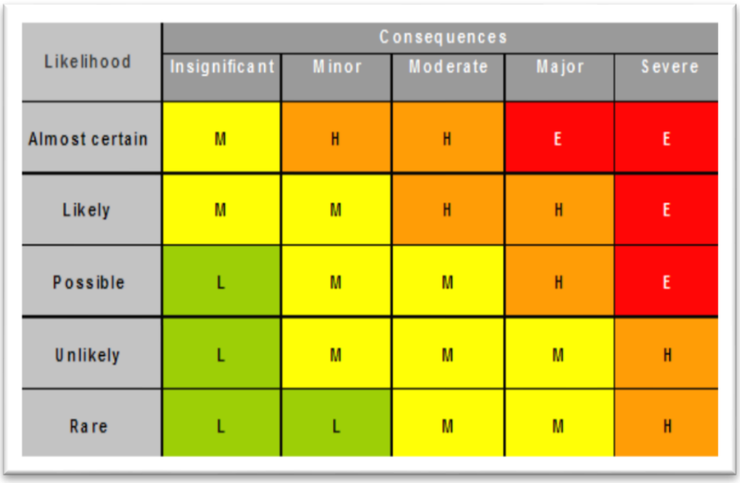

ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
5a. Prepare Statement of Applicability
SOA
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5b. Prepare Risk Treatment Plan
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
Plan project
Project plan
Plan project
Project plan
Develop Internal ISMS Audit Plan
Internal ISMS Audit proc
Preventive Action Procedure
Controls Documentation
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
PDCA cycle (one of many)
Information Security Metrics
7. ISMS implementation program
ISMS Operating Procedures
Corrective Action Procedure
Records Control Procedure
10. Compliance review
11. Corrective actions
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
12. Pre-certification assessment
Key
Mandatory document
PLAN
DO
ISO/IEC 27001
13. Certification audit
ISO/IEC 27001 certificate
14. Party on!
ISO/IEC standard
ACT
CHECK

Figure 5. Implementation and certification process by ISO27001security.com

It’s easy to understand that a reliable risk analysis can start only from the assignment of the correct probability of each threat. In fact, as the Department of Health & Human Services of USA includes among the “Basics of Risk Analysis and Risk Management” in the sixth paper of HIPAA Security series, risk is a function of:

1. The likelihood of a given threat triggering or exploiting a particular vulnerability - expressed as probability or frequency.
2. The resulting impact on the organization.

Once identified the threats, the risk rating will be based on an assessment of the likelihood of their occurrence, their potential impact (consequence), and the residual risk after risk treatments have been applied, as in the following matrix (Dpmc.gov.au):



Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Rating risk level:	**(E)**	Extreme risk - detailed action/plan required
	(H)	High risk - needs senior management attention
	(M)	Moderate risk - specify management responsibility
	(L)	Low risk - manage by routine procedures
Likelihood:	**A**	Almost certain - expected in most circumstances
	B	Likely - will probably occur in most circumstances
	C	Possible - could occur at some time
	D	Unlikely - not expected to occur
	E	Rare - exceptional circumstances only
Consequences:	**5**	Severe - would stop achievement of functional goals / objectives
	4	Major - would threaten functional goals / objectives
	3	Moderate - necessitating significant adjustment to overall function
	2	Minor - would threaten an element of the function
	1	Negligible - lower consequence

Figure 6. Risk Assessment Considerations and Questions by the Australian Department of the Prime Minister and Cabinet.

A similar way of ranking risks is used by the Finnish Government, as shown below:

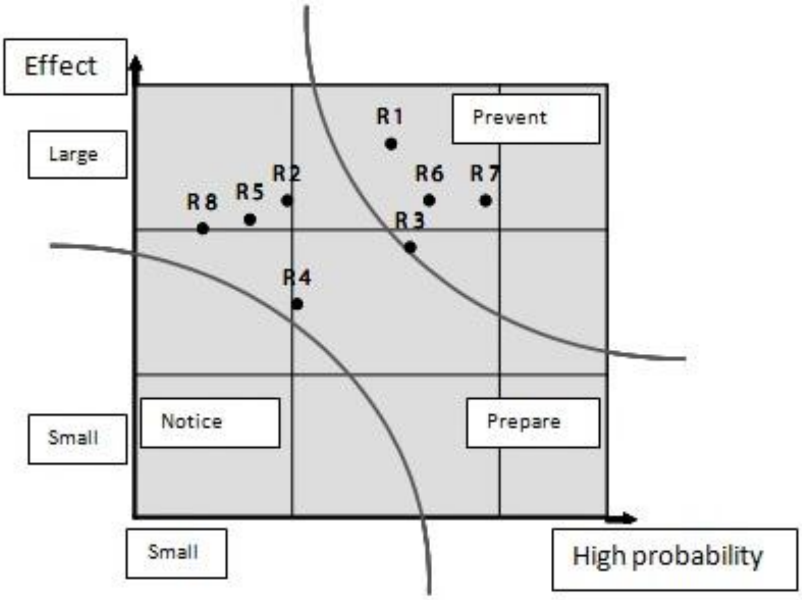


Figure 7. Prioritization of risks by Finnish Ministry of Finance (2008).

In risk analysis, the second proxy (consequences/effects) can be studied through a business impact analysis that is identifying the critical business functions within the organization and determining the impact of not performing each one of them beyond the maximum acceptable outage. A sensitivity analysis could be useful in order to rank the threats depending on the severity of their aftermath.
Nevertheless it is increasingly difficult to determine the first proxy (likelihood of the threats).

According to the Central limit theorem- justification for many procedures in applied statistics and quality control- given a sum of independent, identically distributed random variables (with mean μ and finite variance σ^2) regardless of the original distribution, that sum will tend to be Normal as the sample size increases.
Today organizations face attacks that are *targeted* and even *unique* for which it doesn't make any sense to calculate a *frequency*. "Normal distributions don't exist in these threat populations", Baskerville states in his "Information Warfare" (2005).
But then, since risk analysis is *based o*n normal probability distribution, which tool can be used in alternative? How to batten down the hatches in this context of *drift*?

It has been said that, in managing information security, organizations face a *dualism* (Spagnoletti, Resca, 2008) given by the nature of security risks that requires a *diverse epistemological approach*.

While predictable risks can be investigated and managed via positivistic approaches (and in this field various methods and techniques, as shown above, are available), unpredictable risks need to be combated with interpretative approaches that go beyond the typical risk analysis and include new elements, such as bricolage, improvisation and hacking, within the ISMS model shown above.

2.1. IW: just a military issue?

The information warfare (IW) paradigm has often been confused with an intensive form of the business information systems security (BISS) paradigm, and considered applicable only in military settings.
The two paradigms are instead characterized by opposite assumptions that should lead organizations to use one or the other depending on their reference environment, not automatically.
In fact, while the IW dominates the thinking in most organizations related to the military, the BISS prevails in all other areas, i.e. commercial, government and not-for-profit organizations.
But today, in light of the exponential growth of *unpredictable risks*, organizations should reconsider the appropriateness of the security countermeasures adopted.
“This privileging of military thinking is myopic”, B. Cronin and H. Crawford wrote already in 1999 endorsing the use of the IW in “civilian” contexts. “Information warfare concepts deserve to be liberated from their military associations and introduced into other discourse communities concerned with understanding the social consequences of pervasive computing.”
As Baskerville reports, the shifting context of many organizations has increased the appropriateness of the warfare paradigm in non-military settings.
Why? Which are the characteristics of the IW that make it so suitable with this changing environment?

First, as Baskerville says, the so-called “information operations” within the IW are not only conducted during times of war: they are performed every day with “military readiness”, proving that IW is a *response* paradigm, an ongoing activity that leads the information security to be agile and always ready to react and, even better, foresee the attack.
Risks are one-shot. Attacks take the opponent by surprise.

For this reason, in order to be effective, IW safeguards must be emergent, "invented on-the-fly", unpredictable as the risks are.
In BISS risks are static, quantifiable through probability theory, labeled in risk matrices. The aim is *prevention*, via passwords, intrusion detection systems, standard compliance (all the technicalities discussed above) and rules established *ex-ante*.
If risks are unpredictable, the relationship of safeguards to them cannot be determinate, as in BISS paradigm, but consequential. The link between risks and countermeasures is necessarily dynamic.
Given the impossibility to estimate and asses the risk that is a "unicum" and the consequent impossibility to use the probability theory, Baskerville suggests looking at the "OODA" loop as conceived by USAF Colonel John Boyd.

The "Observe-Orient-Decide-Act" Cycle, implying offensive *and* defensive information operations, is applicable to both military and business strategies. *A different battlefield, the same strategy*. (Bell, 2003).

First step in the loop is *observation*. Looking at the success (in terms of battles won) of the American F-86 fighter planes compared with that of the Soviet MIG-15, Boyd noticed that, although the latter was faster and could turn better, the former was far superior because of the improved field of vision granted to the pilot, who could out-maneuver the enemy pilot, displacing him. American planes had a competitive advantage, given by the availability of better visual.

In ISMS, at the initial stage of the loop it's necessary to collect updated information from as many sources as possible and to be aware of unfolding circumstances.

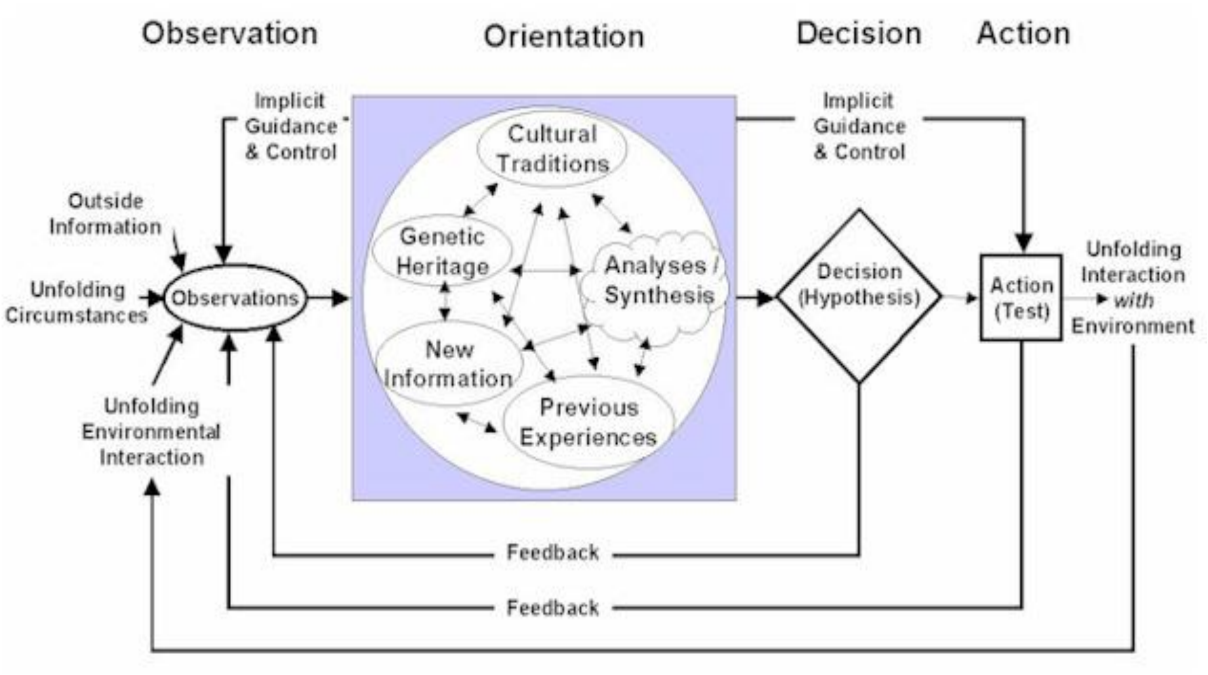


Figure 8. The OODA loop (Baumgart, 2010).

Outside information and unfolding circumstances are the inputs of the Observation-stage. Here, the more information has been obtained, the more accurate the perception will be.

In the second stage, "Orient", information are analyzed and filtered in order to update the current reality. Orientation is essentially how a situation is interpreted. One of the main problems that can occur here is related to the inevitable bias of the human perception. In this regard, Boyd has identified five main influences:

- Cultural traditions
- Genetic heritage
- The ability to analyze and synthesize
- Previous experience
- New information coming in.

The Orient-stage leads directly to the decision. According to Boyd it's the most important part of the loop, as it shapes the way people observe, decide and act.

The Decide-stage is the determination not just of a single action, but of a *course* of action. Decisions should be considered fluid works-in-progress, resulting from the previous stages of observation and orientation.

The loop often gets stuck at the "D", as D. G. Ullman, President of Robust Decisions Inc., writes in his work <<"OO-OO-OO!" the Sound of a Broken

OODA Loop>> (2005). "*Getting stuck* means that there are no decisions and thus no actions"*:* time is given to enemies to prepare the attack.
This must be absolutely avoided.

As the OODA Loop is a cycle, new suggestions keep arriving: these can trigger changes in the decisions and subsequent actions. It's a continuous learning cycle whose results are brought in during the Orient phase, which in turn influences the rest of the decision making process (Mindtools.com).

The Act-stage implies the implementation of the decision taken. "The proof of the success of the OODA loop is in the success of the action" (Ullman, 2006).
Then the cycle starts again from the Observe stage, where the effects of the action are judged.
It is fundamental to learn from what the opponents have done in the meanwhile.

It has been shown that the OODA loop is not a static model, but a smooth and continuous process. One of its main goals is to increase the speed with which to orient and reorient the decision as new information come in, in order to surprise the enemies. Of course, the faster an information security is in reporting (or even better foreseeing) an attack, most likely the faster the safeguard will work. Speed or *agility*, as Baskerville calls it, may help in limiting attack damage. "IW values agility higher than quality".
Anyway organizations must be careful: a loop mustn't mean *routine*. The abovementioned cycle helps in gaining speed in observing, orienting and then acting, that is in performing these actions, not in doing always the same things. Routine is highly dangerous in IW, as routine can be intercepted and easily attacked.

According to this paradigm, which are the countermeasures an organization should adopt concretely? Are they just technical?

2.2. Information Security: a major management responsibility

Today information security is finally recognized from a management perspective: given its importance and the serious aftermath related to an eventual breach, it can't be left to technical experts. It is a matter of general interest and should be seen as such by everybody in the company. As J.F. Van Niekerk and R. Von Solms (2009) assert in their homonymous article, there is a strong need for an *Information Security culture* that permeates the whole organization.

This in fact is key to manage the *critical and decisive human factors* involved in information security.

Statistics sadly show that too many times employees have been the main cause of security breaches. *How*?

A 2002 study of American corporations ("Corporate Security: Protecting Productivity") conducted by business intelligence firm Cutting Edge Information reports that 70% of business security breaches are caused by employee actions, whether intentionally or through negligence.

"Improper training is the true culprit behind corporate America's overwhelming lack of security" Jason Richardson, Cutting Edge Information's CEO, asserts.

"Employees ignore security because they have never heard of the *policy",* Joan Goodchild, senior author of CSO online, adds (Techworld.com).

As a report by RSA (the Security Division of EMC, leading provider of storage hardware solutions) reveals, *a majority of workers polled said they regularly feel the need to dodge corporate security policies in order to get their job done.*

So while companies are concerned in studying abstruse security measures, the real danger lies in its seemingly innocent employees. *Why?*

Among the most frequent violations, employees log into their email accounts or social networking sites, while they are at work.

According to Frank Kenney, a Gartner analyst, people in general don't know the rules.

Moreover, if there is a security policy in place and everyone is aware but no one is responsible for enforcing it, employees will keep on breaking the rules because there is no repercussion for their actions.

As mentioned in chapter 1, social networking sites have expanded the employers' risks. According to Sophos (US security developer and vendor of security software and hardware) and its Security Threat Report, in fact, cybercriminals have increased the focus of enterprise attacks using platforms such as Facebook and Twitter (J. Shinn, 2009).

Therefore organizations should become more concerned about malicious attacks originating from social networking sites and implement web security solutions that control every link and webpage as it is clicked on, in order to check if it contains malware or suspicious activity.

Nevertheless it has been proved that employers who implement a wholesale ban on these social networking sites don’t solve the problem at all (Sophos’ 2011 Security Threat Report). Employees will finish circumventing the employer’s protective measures and thereby opening up another layer of vulnerability to the organization.

People must be *motivated* to follow the rules, and security policies have to be equipped with a set of appropriate incentives and punishments.
At first, organizations should *educate* their workforce about e-risks**:** all employees must be aware of the impact that their actions could have on the corporate network.
Second, it might be appropriate to allow the access to popular social networking sites only at specific times (e.g. to Facebook during lunch break).
However multi-layered security, at both the gateway and the endpoint, must be applied.
All the information employees have been posted online should be checked. If the organization discovers that sensitive business data are shared, it has to evaluate the situation, and then act as appropriate.

2.3. A closer look at the TFI model

The TFI model proposed by Åhlfeldt, Spagnoletti and Sindre (2007) seems to fully understand this point, stressing the importance of formal and informal aspects within an information system.
Which are in particular these aspects? Are they firm-specific or mostly common to all ISs?

In all organizations, the widely accepted InfoSec model shows that Information Security has two faces: one technical, the other administrative.
While the latter has no ramifications in the original model, the former is subdivided into IT security and physical security, each one with its own countermeasures.
Supported by the results from three different case studies, the Authors have extended the InfoSec model as shown below:

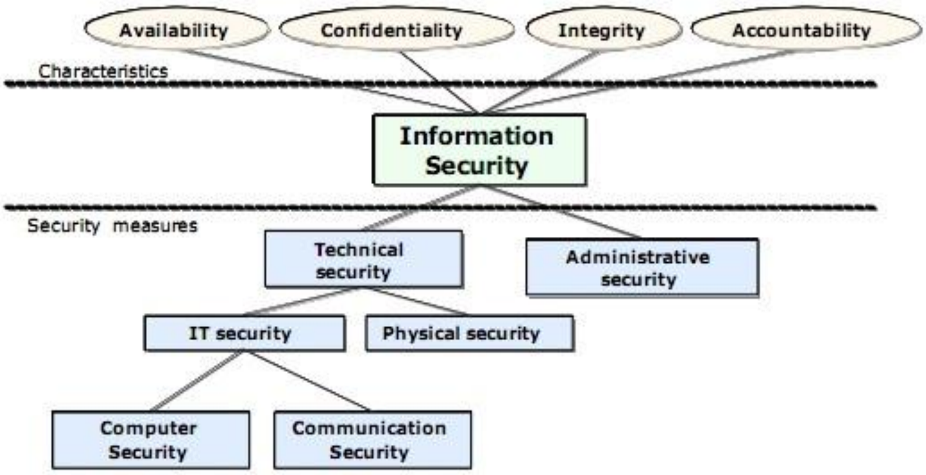


Figure 9.a. The original InfoSec model (Åhlfeldt *et al.*, 2007).

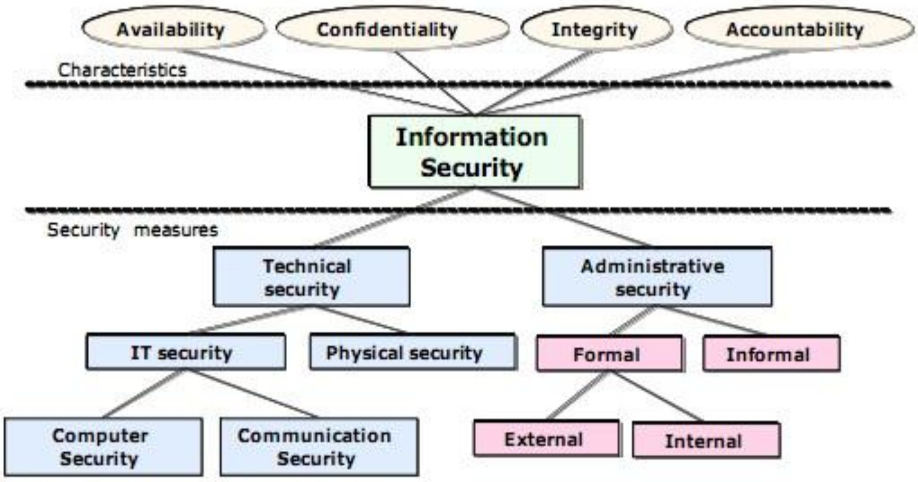


Figure 9.b. The extended InfoSec model (Åhlfeldt *et al.*, 2007).

Starting from the left side, the technical level, while physical security embraces all the tools used to protect the overall infrastructure (e.g. alarm system, fire prevention, surveillance, etc.), IT security is divided into Computer security and Communication security. Actually they are the most debated aspects in literature.

2.4. IT security solutions: requirements and main technologies

E-Business environments are forcing organizations to move away from private communication to open public networks, first of all the Internet. It has been seen that increasing the availability of corporate information to an unlimited number of users also significantly increases security risks. New requirements and methods are then necessary in order to keep an e-Business infrastructure safe from attacks.

Regarding the *computer security safeguards*, all sensitive information, laptops, and removable storage devices should be encrypted with a password. In this way, even if the hacker overcomes all the countermeasures adopted, he/she won't be able to read the content of them, and so compromise the confidentiality of the information.

Furthermore, in disaster recovery, backing up important data is essential, but not enough. The information on those backup tapes or disks could be stolen and used by someone outside the company. Many IT administrators make the mistake of keeping the backups in the server room, while they should be locked up at all times, in a drawer or safe or, ideally, in a secure, offsite location.

In general, all printers, servers and workstations that store important information should be located in safe locations and bolted down so nobody can walk off with them.

However, security experts believe that the greatest threats occur at the *network* and *communications* level (Kizza, 2009).

According to the British Standards Institution, the five requirements for application-level security are (BSI, 1999):

- Authentication
- Authorization
- Message integrity
- Confidentiality
- Operational defense.

In order to ensure them, a number of technologies is available, the most basic of which is *message encryption*.

Currently three cryptographic techniques are used: symmetric (sender and receiver use the same key), asymmetric (two different keys, one of which is public, and the other private) and hybrid encryption.

Combining the advantages of both, the hybrid encryption, used together with a digital signature, meets the requirements of authentication, confidentiality, integrity and incontrovertibility.

Lastly, XML Encryption, a W3C standard, provides end-to-end security for applications that require secure exchange of structured (both XML and non-XML -e.g. binary) data (for additional details about Encryption and Public Key Infrastructure, see Papazoglou, Ribbers, *e-Business: Organizational and technological foundations*, John Wiley & Sons, Ltd., 2010, pp. 372-385).

Since networks have grown more complex and difficult to manage and increasingly have multiple entry points, organizations should design “ad hoc” network level solutions that however rely on the following main technologies: firewalls, intrusion detection systems (IDS) and vulnerability assessment.

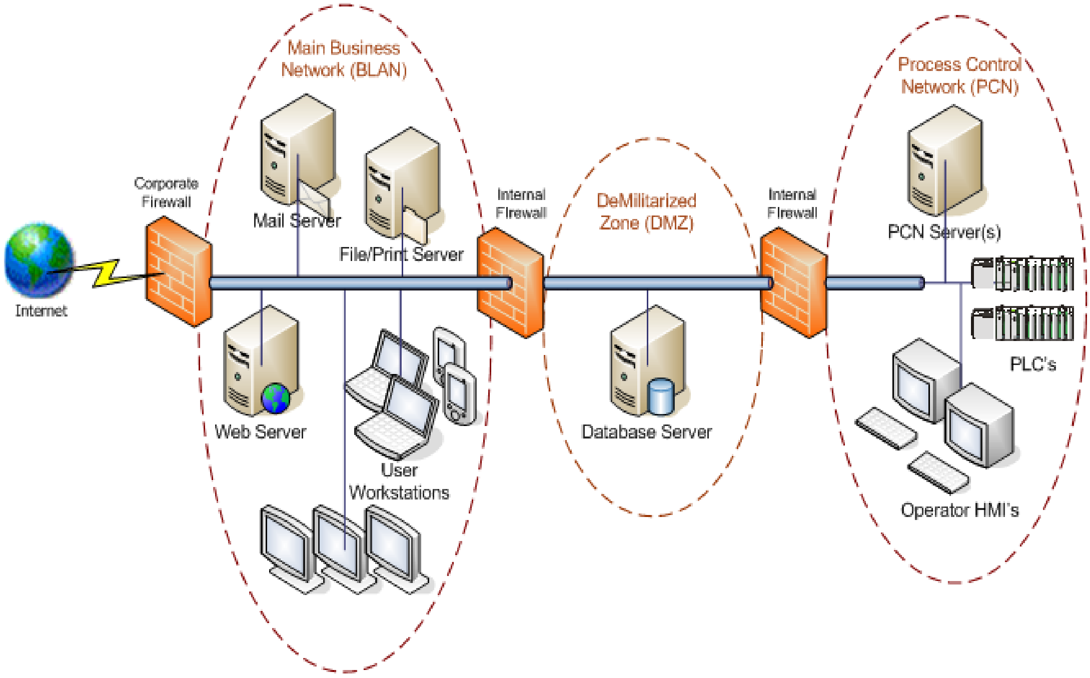


Figure 10. A typical use of firewalls within an enterprise network (Cimconcepts.com).

In figure 10, the process control network (PCN) is separated from the enterprise network (EN, or BLAN) on a separate subnet using firewalls. Today in fact enterprises need to separate critical manufacturing functions from the general business network. The DeMilitarized Zone (DMZ) is the local area network where enterprises typically host assets such as web servers.

IDS can be network based or host based. In the first case, NIDS detect attacks by checking the normal traffic and analyzing the content of packets as they cross the network.
HIDS instead detect attacks against web servers by analyzing logs in real time.
Figure 11 provides a clearer understanding of their functioning:

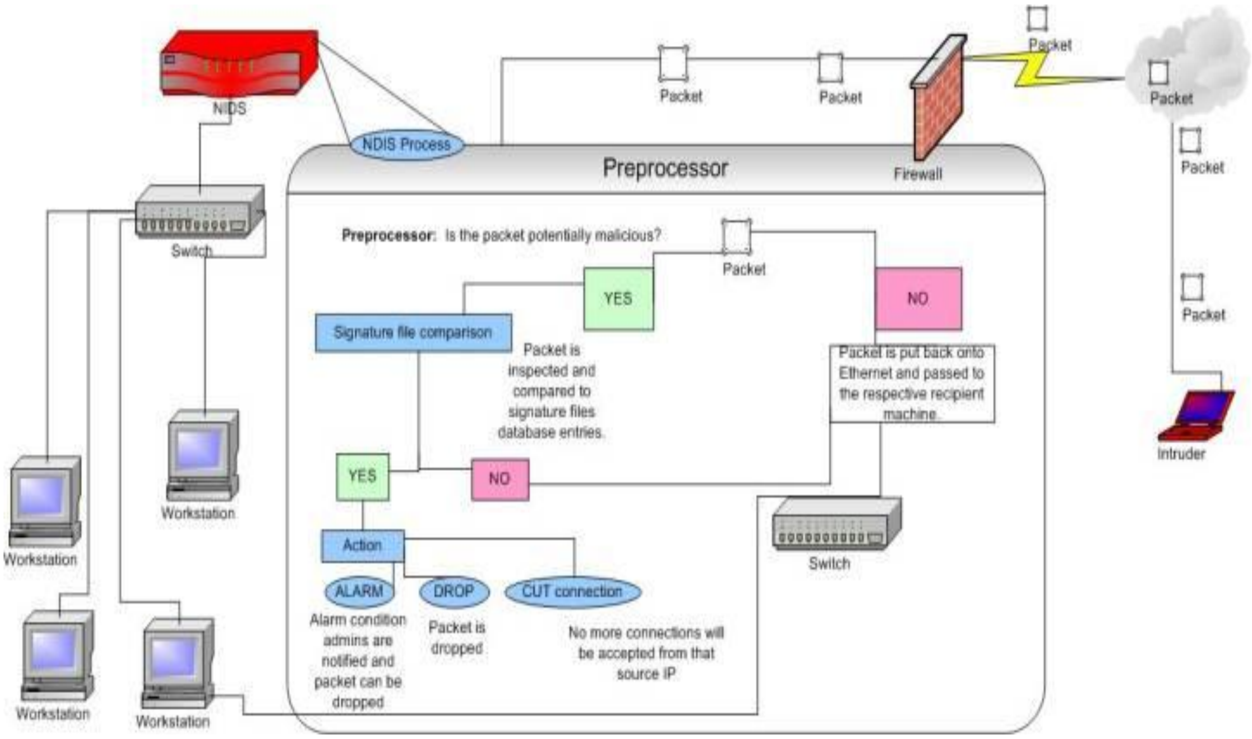

NIDS
NDIS Process
Packet
Packet
Packet
Packet
Packet
Packet
Firewall
Preprocessor
Switch
Preprocessor: Is the packet potentially malicious?
Packet
YES
NO
Signature file comparison
Packet is inspected and compared to signature files database entries.
Packet is put back onto Ethernet and passed to the respective recipient machine.
Intruder
Workstation
Workstation
YES
NO
Action
ALARM
DROP
CUT connection
Alarm condition admins are notified and packet can be dropped
Packet is dropped
No more connections will be accepted from that source IP
Switch
Workstation
Workstation

Figure 11. Network Architecture for a stand-alone NIDS (Magalhaes, 2003)

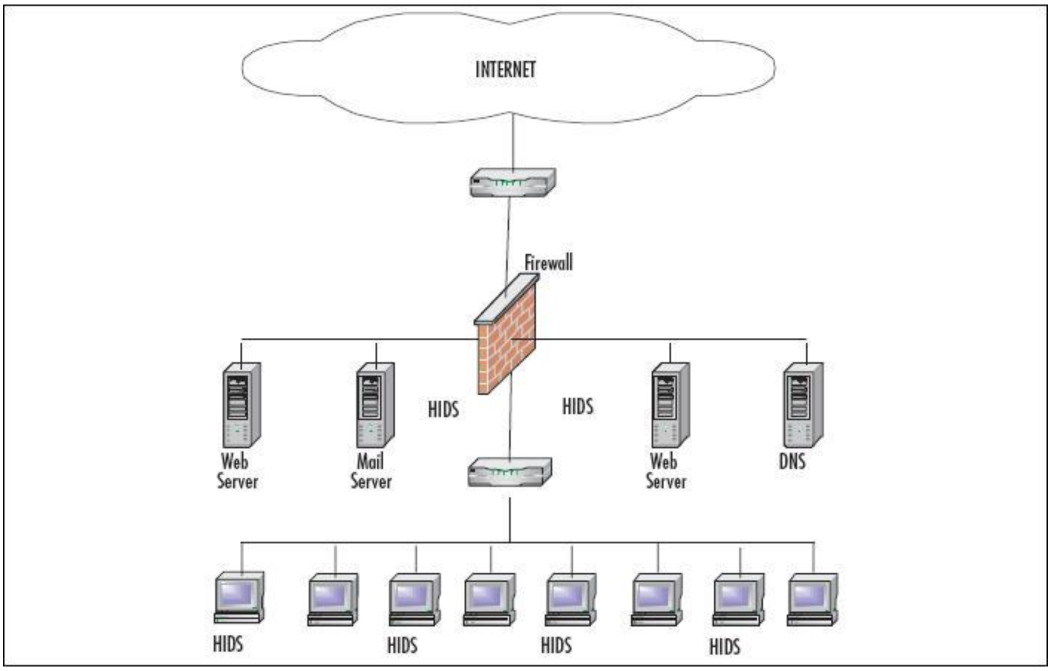


Figure 12. Host-based IDS (Tabone, 2011)

In the following table the most relevant differences among the two systems are highlighted:

NIDS (Network IDS)	HIDS (Host IDS)
Watches all network activities (Broad in scope)	Watches only specific host activities (Narrow in scope)
Better for detecting attacks from outside	Better for detecting attacks from inside
Near real-time response	Usually only responds after a suspicious log entry has been made
Easier setup	More complex setup
Less expensive to implement	More expensive to implement
Detection is based on what can be recorded on the entire network	Detection is based on what any single host can record
Examines packet headers	Does not see packet headers
OS-independent	OS-specific
Detects network attacks as payload is analyzed	Detects local attacks before they hit the network
Detects unsuccessful attack attempts	Verifies success or failure of attacks

Table 1. Main differences among Network and Host IDS (Han-Ching Wu, 2009)

Finally, vulnerability assessment is a methodical approach by which vulnerabilities are identified and prioritized, and enterprise networks are tested, in a non-intrusive manner, from the hacker’s perspective. This approach is preferable to the IDS, because it determines susceptibility to attacks before networks could be compromised.

Working hand in hand with antivirus, firewall and IDS, it identifies vulnerabilities, network misconfigurations and *rogue* devices, then detects and prioritizes vulnerabilities exposures, providing remedies for *known* vulnerabilities.

Now a question could arise: which is the relationship among a risk analysis and a vulnerability assessment? What is a risk and what instead a vulnerability?

If a vulnerability has been identified, the organization is exposed to a risk.

Vulnerabilities *imply* risks.

Then, it is possible to conclude that vulnerability assessment is part of a well conducted risk analysis.

But what about new, unexpected attacks to organizations that didn’t think to be vulnerable?

Risk analysis and vulnerability assessment are common tools used by organizations that embrace the BISS paradigm and drawn their organizational learning from exploitation.

But exploitation learning strategies are for things *already known*, as Baskerville states. They yearn for refinement, high quality achievable through reliable safeguards.

They seek to eliminate *variation* –incrementally achieving better and better security (Levinthal, March, 1993), the same variation that the IW paradigm instead promises to explore, or even transform into a *weapon* against the opponents.

Therefore, as today the technological remedies are the most standardized within the Information Security, where could a firm create this variation (understood as *differentiation*), at what level?

2.5. Administrative security

The right side of figure 9 has been investigated and enriched of elements that are *vital* for managing information security. Too often underestimated and neglected, they can be classified in formal and informal aspects, according to the TFI-model.

This provides, as the Authors underlines, a more holistic view of the phenomenon. The administrative security in particular is so context-specific that all organization should design and monitor it carefully.

As Bruce Larson (security director at American Water) said in an interview to CSO online after the Welchia worm, there is a difference among *good Security* and *OK Security* (Berinato, 2006).

Formal and informal aspects make this difference.

2.5.1. Formal aspects: how they become effective

Formal aspects refer to a set of rules, policies, standards, controls, etc. put in place by the organization in order to define an interface with the technical level.

As previously mentioned in chapter 1, Prof Basie von Solms in his work "Information Security- A multidimensional discipline" (2001) asserts that, before any information security implementation can start, the first aspect which must be in place is *at least* a Corporate Information Security Policy that in turn includes sub policies, procedures and standards that govern all relevant actions in information security.

"You cannot start enforcing any information security controls, the author goes on to say, if you do not have a mandate and reference framework to do so - the Corporate Information Security Policy is your mandate and basic reference framework".

A lot of websites and IS providers suggest templates, guides, procedures to build and implement successful information security policies.

But which should be the main objective of an information security policy? What should it contain to be effective and observed?

Actually, recent surveys and researches show that employees *seldom* comply with information security procedures. Policies are in fact perceived as mere guidelines rather than "hard and fast rules". (Herath, Rao, 2009). Enforcement of security policies is a critical challenge for organizations today.

As explained in chapter 1, the determination of responsibilities and their punishments is essential.

In literature there is a strong debate about the type of punishments to be adopted.

For instance, "Failure to comply with this policy may subject you to disciplinary measures.

For University employees, failure to comply could result in termination". These are the steadfast words of Princeton University, Office of IT (Princeton.edu).
Nevertheless, sometimes the severity of punishment may have a negative effect on security behavior intentions.
Which are then the motivators employees have in following the rules?

In their work, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", Herath and Rao (2009) evaluate the relative importance of three incentive mechanisms: penalties (extrinsic incentive), social pressures (extrinsic incentive), and perceived effectiveness (intrinsic incentive), under the following assumptions:

- Hypothesis 1a. Increased severity of penalty will be positively associated with intention to comply with organizational information security policies.

- Hypothesis 1b. Increased certainty of detection will be positively associated with intention to comply with organizational information security policies.

- Hypothesis 2a. Normative beliefs will be positively associated with intention to comply with organizational information security policies.

- Hypothesis 2b. Peer behavior will be positively associated with intention to comply with organizational information security policies.

- Hypothesis 3. Employee perceived effectiveness of his/her security behavior will be positively associated with the intention to comply with organizational information security policies.

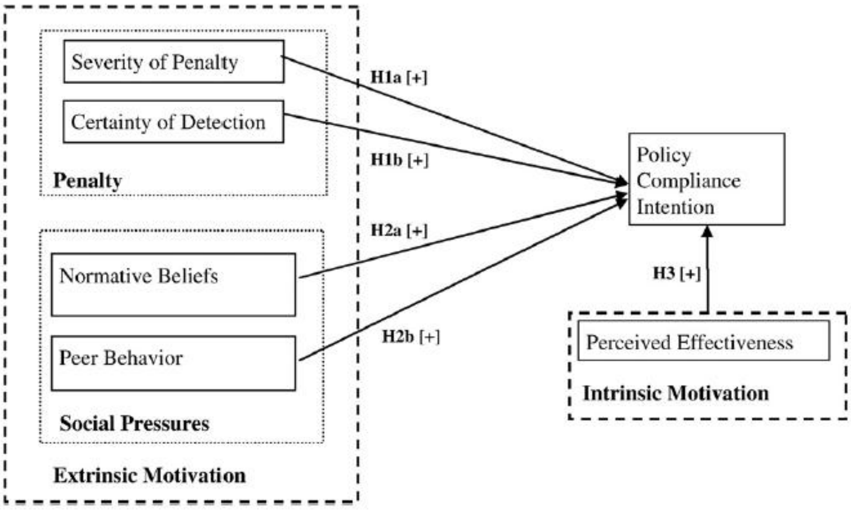


Figure 13. Extrinsic and intrinsic motivators in information security behaviors (Herath, Rao, 2009)

Some of these findings are useful for the current discussion:

- Both intrinsic and extrinsic motivators influence employee intentions of security compliance: in particular, “if the employees perceive their security compliance behaviors to have a favorable impact on the organization or benefit an organization, they are more likely to take such actions”.
- Social influence also plays a role in security behaviors. The beliefs regarding expectations of superiors, IT management and peers seem to have the most impact on employee security behaviors.
- Employee perceptions of others complying with the security policies are also significant contributor in employee intentions to comply with the policies themselves.
- Certainty of detection has a positive impact on security behavior intention. “If the employees perceive that there is higher likelihood of them getting caught if they violate security policies, they are more likely to follow the security policies”.
- Surprisingly, severity of penalty was found to have a negative impact on the security behavior intentions.

In conclusion, it’s already very difficult (and it could take a long time) to build a tailor-made policy. However, at the end, all efforts could result *vain* and the policy *ineffective* if there is no *awareness* of its content among *all* the employees, and the set of effective punishments is just a set of mere threats of punishments.

However, the severity of penalty is a double-edged sword that must be related and commensurate with the mission of the organization, its values, attitudes and beliefs.

This leads the discussion to the informal level security, the most intimate (and decisive) aspect of information security management.

2.5.2. The inner domain of Information Security

While formal aspects present external influences, such as laws, industry regulations, agreements with other policies, etc., at the informal level the unit of analysis is solely the organization with its *behavioral issues*.

All the previous discussions about security do not stand if informal aspects are neglected, as they have often been. Unfortunately many organizations keep on being blind, stubborn in the research of the best technology solutions and meticulous in the observance of one or another standard. As previously said, too often they forget their own employees.

In BISS paradigm and information security literature in general, little emphasis has been placed on informal aspects. The result is that too many organizations that embrace these *gothas* fall because of their negligence.

Therefore the need for a corporate culture of security at each level of the workforce is increasingly urgent.

But what is an information security culture? What its benefits?

The above mentioned work of Niekerk and Von Solms (2010) rightly states that, while in normal definitions of *organizational culture* the job-related knowledge is generally ignored, because it can be assumed that the average employee would have the required knowledge to do his/her job, the required information security knowledge is not necessarily needed to perform the employee’s normal job functions, but having adequate knowledge regarding information security is a *prerequisite* to perform any normal activity in a secure manner.

A culture is made by artifacts, espoused values and shared tacit assumptions (Schein, 1999).

Artifacts are what actually happen in the organization: visible and measurable organizational structures and processes. For the day-to-day tasks to happen in a secure way, people in the organization must have sufficient knowledge of how to perform them securely.

The team responsible for designing the policy will include in it the espoused values, such as espoused strategies, goal, philosophies, justifications, official viewpoints, etc.

Shared tacit assumptions involve unconscious, taken-for-granted beliefs, feelings, perceptions, thoughts, and so on.

These three levels together build the *knowledge*.

The IW paradigm seems to reflect this orientation, in particular when it comes to the *perception management*. According to Baskerville, managers have a strong ascendancy on employees, influencing their behaviors through fear, desire, logic and other mental factors.

All employees then must be devoted to the cause of Information Security.
In this field in fact even one weak soldier can compromise the integrity of the grid opening a dangerous loophole.
IW is first of all knowledge warfare. For an organization this means knowledge of its enemies, but before knowledge of itself.

"Know thy self, know thy enemy. A thousand battles, a thousand victories", Sun Tzu wrote almost 2500 years ago. "*Regard your soldiers as your children, and they will follow you into the deepest valleys; look on them as your own beloved sons, and they will stand by you even unto death".*

These are probably the most important lessons for any manager, the starting point for building anything in the organization.

3. The relationships between BISS and IW paradigms and TFI security measures: research methodology

What makes the two paradigms different? The use of a type of countermeasures rather than another? The adoption of a certain policy or the conformity to a standard?
No. *What makes them different is the way of understanding the risk.*
This will be the beginning of my case study.

According to Yin (2005), the case study is one of the ways of conducting a research in social sciences. It is particularly useful in a contemporary context, when there's no control over events, and most of the questions are about the "how" and "why".
So far literature has investigated and compared the two paradigms, especially from a theoretical point of view.
My aim is to show the practical application of the two paradigms through the TFI countermeasures, technical, formal and informal.
For my interview I've chosen a *business* organization, in order to prove that BISS and IW paradigms live and work well together in a non-military setting.
Prevention and response are complementary and feed off one another.
In fact high-risk business organizations may find great benefits from the IW-response paradigm.
But how?

As soon as the threat environment changes, prevention principles (drawn from the knowledge of those risks that have already occurred and past mistakes) are still necessary, but not enough. *Reliability* and *exploitation* are a good strategy in *stable* and *recurrent* environment, as Baskerville notices. Looking at the future, in a post-incident situation, other principles should reinforce the prevention ones.
In this regard, *validity* and *exploration* elements must be investigated. After a security breach a *response strategy* is required.
Given the speed of technological progress, even in non-military organizations unexpected security incidents can happen easily, coming for example from a technical oversight, a heedless employee, and the like.
In order to manage information security today a better balance between prevention and response is strongly advised.
So why is it difficult to obtain?

Which are the fundamental differences between prevention and response InfoSec models?
The following table is useful in order to stress the peculiar aspects (previously described) of BISS and IW paradigms necessary for the upcoming case study:

	BISS **(Prevention)**	**IW** **(Response)**
Risk features	Predictability Measurability Persistency	Unpredictability Not-measurability Transiency
Orientation	Past	Future
Strategic goal	Quality	Agility
Relationship among risks and safeguards	Static Determinate	Dynamic Consequential
Learning strategy	Exploitation	Exploration
Risk analysis	Probability theory	Possibility theory
Basic principle	Reliability	Validity

Table 2: Comparing the two paradigms.

Given these characteristics, BISS-prevention main domain is the “pre-incident”, while the IW-response one is the “post-incident”.
Nevertheless, both of them are present before, during and after the incident. How?

In the second chapter TFI model has been shown to provide valid countermeasures in a holistic approach of the security breach (the incident). Is it possible to combine in practice these countermeasures with BISS and IW requirements? How?

The interview is structured in order to sink in the inner mechanisms of the organization’s InfoSec management.
First, which are the reasons that drive the organization to adopt countermeasures? This will reveal the *focus* the organization has in InfoSec management: if it is the before or the after incident. And this is a *clue* too for understanding the main orientation that is prevention (before) or response (after) to security attacks.

At this point the peculiarities of the organization will determine the type of risk it faces, if they are predictable/unpredictable, measurable/not-measurable, persistent/transient. Why are these risks cataloged in this way? What does the organization put in place to handle such risks?
Is it possible to foresee them? Which are the instruments used from the technical, formal and informal point of view?

Predictability, measurability and persistence. Three faces of the risks.
Are they constant or changing characteristics?
Is it possible for a risk to become from predictable unpredictable, from transient persistent, or vice versa for instance? If yes, which are the factors that trigger this change?

Moreover, in case of violation, how does the organization react? How fast is it in the response?

“One of the best ways to develop risk awareness is to learn from others’ mistakes” (www.erisks.com). Is this motto applicable in InfoSec management?

Once the two models are clear in terms of main characteristics, let’s compare them with the TFI model. In mathematic terms, which is the result of TFI (BISS, IW)?

3.1. Interview structure: the *contextualist approach*

Given the complexity and novelty of its subject, the analysis is drawn on the *contextualist approach*, as A. M. Pettigrew (1985) defines it.
Foremost qualitative research is appropriate in this kind of research because of its characteristics of being exploratory, flexible, and context-sensitive (Mason, 2002).
In this way, the contextualist approach is adopted in combination with different theoretical lenses (the two paradigms), with the aim of reaching a comprehensive, process-oriented understanding of the organization’s InfoSec management.
The interview is the key part of this thesis as it is capable of producing well-founded cross-contextual generalities by showing how things work in a particular context.
Emphasis is on *the context*, and of course the interview questions arise from it.

Many process-oriented IS studies are contextualist in the sense that they are typically case studies investigating how a phenomenon is situated and unfolds in its context.
Moreover, Pettigrew suggests the contextualist analysis in studying strategic changes in organizations, as it allows understanding the emergent, situational and

holistic features of a process in its context, rather than dividing the process into limited sets of variables separated from context.

Here there are three analytical categories: context, content and process.
Context has two branching: outer and inner.
Outer context refers to the *external* circumstances and conditions where the organization operates, i.e. the social, economic, political, and competitive environment. Inner context is about the *intra-organizational* circumstances and conditions: structure, organizational culture, political circumstances and the like. *Context is not conceived as a static, descriptive background against which an innovation occurs* (Cho, 2007).
Context is constantly affected by the content, and vice versa.

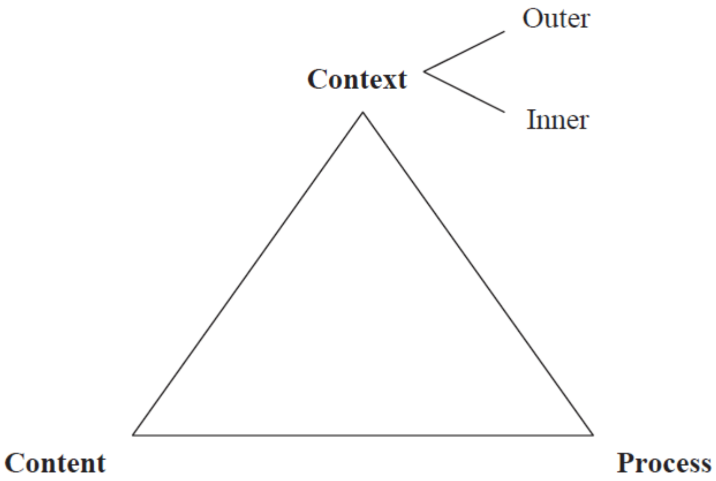


Figure 14. The contextualist approach according to Pettigrew

The interview structure is divided into clearly delineated levels of analysis: the TFI model is seen as a function of three “variables”.

First, there are the reasons why the organization adopts certain measures: to summarize it, the TFI (why).

Second, the threats perceived by the organization receive a label: risks are identified one by one: the TFI (what).

Once risks are classified as predictable/unpredictable, measurable/non-measurable, persistent/transient, the organization is required to assign countermeasures (at the technical, formal and informal level) according to each feature of the risk: the TFI (how).

These are theoretically and empirically connectable analysis levels, as shown in the revisited figure.
The business context of the organization determines the threats, the *concerns and motives* of the information security measures. The context influences the type of

risks and vice versa. According to their predictability, measurability and persistence, countermeasures from the TFI model are chosen, and a process (of prevention or response) is triggered. Depending on how the process works, an incident may be well prevented and most of its damage can be minimized.

The efficiency of a process might change the features of a risk (as it has been well curbed), and the risk evaluation according to the new perception the organization has.

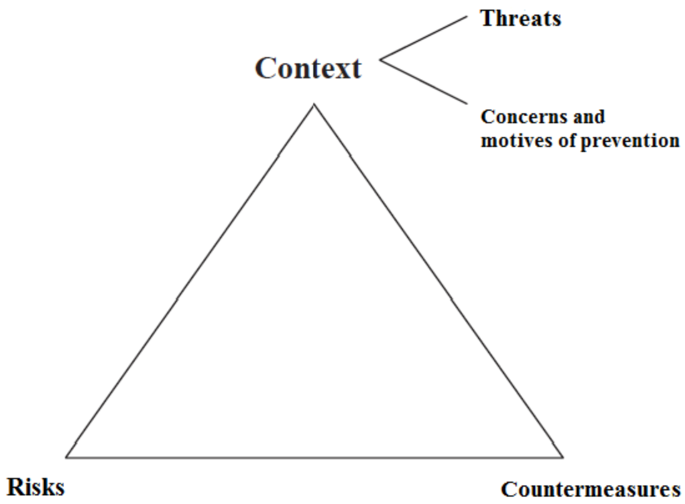


Figure 15. Pettigrew's research scheme revisited.

Interview Questions

1. Which are the concerns and motives of the information security measures at your organization?

2. Talking about an eventual cyber-attack, is your organization directed towards the prevention or the responsiveness?

3. Regarding the risks the organization has to handle, is it possible to prevent them?
If yes, how does the organization do this from a technical viewpoint?
Which are the instruments (from surveillance systems to passwords, firewalls, IDSs, etc.)?
How is prevention at the formal level, i.e. compliance to a certain standard, policies, and the like?
Lastly, what about the informal level and the prevention among non-security staff? Are there unwritten rules?
If these risks are unpredictable, how is the prevention at all the level above mentioned?

4. Is it possible to measure such risks? How?

5. Do the risk features change over time? If so, how and what factors determine this change?

6. The IS of your organization has been violated. How does the organization react?

7. Do you think that your organization's information security focus has changed over time, before/after the security incident? If so, please describe the changes.

4. Data analysis and findings

The 30-minute interview was useful to have a look at the practical applications of what has been shown above in theoretical terms.

The interviewee is a big company, an Italian holding that delivers a multitude of services, such as postal services, banking, insurance, mobile, etc. all over this country. It will be addressed as merely company “UPostBank” throughout the text.

UPostBank is a complex reality.

Regarding its InfoSec Management, the first distinction to stress is between a section devoted to governance, security organization and all what concern *internal policies and advices*, and another section that instead is about *Security Development*.

These are the two souls of Security in UPostBank. They are separated even from an organizational point of view: there is a structure- a central management called “Business Protection”- that oversees all issues of governance and security, both physical and logical. Within Business Protection there are the field of information security, the one of physical security and other sectors.

Given the fact UPostBank provides such different services and is active on a lot of businesses, there are many facets under which the security issues must be addressed: from the security of the SIM card, to the bank transaction security, the physical security of the agencies scattered throughout the territory, till the internal security infrastructure, also with respect to potential attacks and damage that may be caused by employees.

Which are the concerns and motives of the information security measures at UPostBank*?*

UPostBank is a continuously evolving structure, made of diversified and independent areas, i.e. post office interest-bearing bonds, national and international money orders, currency exchange services, post office current and savings accounts, mobile, and the like. All these realities lead UPostBank to operate on different businesses, each of which involves different risks.

UPostBank keeps on expanding into different lines of business and developing new applications.

Of course new technologies, new services and spaces bring new risks. Security risks are always around the corner.

UPostBank shows to have a strong commitment on Security that is considered one of its strengths.

Even UPostBank’s CEO is very concerned with all the security activities performed. There is a continuous flow of information between the InfoSec area and the “upper floors” of the company.

UPostBank has vast resources. In order to better manage them, a reorganization of all the IT infrastructure has been planned, also with a view of cloud computing. This will bring the necessity of investigating all the aspects related to the use of a private cloud.

Talking about an eventual cyber-attack, is UPostBank *directed towards the* prevention *or the* responsiveness*?*

In UPostBank there are both prevention and responsiveness. In which way?
UPostBank has developed a series of important activities: one of them is the European Electronic Crime Task Force (Eectf), promoted in order to aggregate technical skills and expertise even from other industries.
This is a unique example among the Italian companies. UPostBank wants to join all the subjects that are interested in exchanging their operational information, in order to have a continuous update of the evolution of security, new threats and risks, and then decline them internally, through guidelines, corporate policies and everything that has been defined above among the “formal” aspects.

This is about *prevention*.
Talking about *responsiveness*, there is a certainly not negligible effort. All transactions and current risks are monitored and analyzed. UPostBank has very sophisticated systems, a control center, a security control center, with groups of around forty people that monitor 24 hours a day, 7 days a week, denouncing all the anomalous accesses. Alarms are highlighted, accounts are locked and all *technical* actions are taken in order to protect the customers, interpret the weak signals and always have a r*eady answer*.

Down to detail, how is the *prevention* at the *formal level*, i.e. compliance to a certain standard, policies, and the like?

Policies are internally defined, spread and monitored by “Business Protection”. They are valid for the entire group. There is a specific unit that monitors the security policy, making inspections in a sort of *information security audit*. It checks if there are irregularities or any gaps to be filled with respect to the ongoing procedures, and suggests improvement actions.

Lastly, what about the informal level *and the prevention among non-security staff? Are there unwritten rules?*

Yes, there are. An example is provided by the clerks that manage all the banking services and even suggest to the customers, give them advises about the security practices, the use of the instruments and the authentication mechanisms (not really user friendly). Customer support is an essential and continuous need.
Security experts in fact do not talk to customers. They "build" security *from the inside*. Regarding the front-office there is a big effort of formation, communication, training with frequent inspections.
UPostBank's Research Center has developed a course about frauds to follow on the Internet. Typical scenarios of fraud are described, and scores are given according to how the user decides to act.

Which are the risks the organization has to handle? Is it possible to predict *and* measure *them?*

The risk information is perceived as very strong.
A census of all business information archives (which are some hundreds of thousands) has been made recently. Their compliance with respect to the ISO 272001, the minimum requirements and the evolution of the Privacy Code has been verified.
There were two statements of the Guarantor for the protection of personal data, one in 2009, the other in 2011.
The former is about System Administrators, essential figures for the security of databases and the proper management of computer networks. Maximum transparency is required on their work. The serious events occurred in recent years have highlighted a worrying underestimation of the risks that may arise when the activities of such experts are carried out without the necessary control. Each company or public entity must include in the security policy or in another internal document (to show in case of inspections to the Guarantor) the identification of system administrators and a list of the functions assigned to them. The experience, skills, and reliability of the person called to fill the role of System Administrator have to be carefully assessed, because such person must be able to ensure the full compliance with the regulations, the protection of personal data and the security profile.
The latter (2011) is exclusively for banks. In particular it requires all employees' access to banking information to be recorded.

The two statements lead to a restructuring of all the archives in order to handle such need for compliance.

This is about *prediction*. Talking now about the *measurability,* in the abovementioned census a risk measurement has been conducted. Present vulnerabilities have been studied and the impact of each one of them measured (business impact analysis). In this way, UPostBank's InfoSec management can highlight those areas where risks are highest and *action* is a priority, and take corrective actions, not particularly complex, but able to greatly reduce those risks.
The census with its analysis provides a model that the company aims to achieve within a year. It leads to associate each risk to the single information cataloged -in quantitative terms- and implement improvement actions. These in turn are evaluated on the basis of the new impact registered on the business area affected.

Now, what about unpredictable *and* non-measurable *risks? What does* UPostBank *do to handle them?*

For unforeseeable and non-measurable risks there is a structure of "Monitoring & Reaction". Reaction to security attacks.
Even if nothing appeared on the newspapers, UPostBank has been victim of DDoS attacks during the year, like many other companies.
UPostBank is a big company and its business information archives have significant value. If only someone had been able to tamper with them, certainly newspapers would have spoken at length about it.
UPostBank has been attacked. They were not very sophisticated attacks, so UPostBank's 24x7 monitoring framework was enough to detect weak signals and mitigate the risks. For instance, DDoS attacks- without going into technicalities-often come from IP address classes that are always the same. Once a suspicious traffic has been intercepted coming from those IP addresses, the provider is asked to stop it. In this way services are not compromised and safe.

Do the risk features change over time? If so, how and what factors determine this change?

Vulnerabilities change, as the technological scenario and the landscape of service delivery evolve, resulting in constantly updated and innovative products. Even the impact of each vulnerability changes: this is the case, for example, of a technology initially used for a small cluster of users, and later exploited on a larger number of users, with a different expertise required and new vulnerabilities potentially opened.
The impact of the single vulnerabilities recorded in the first instance changes too.
Risks go along with the evolution of technology.

Nowadays for example there is much talk about cloud computing or even all the applications developed on mobile phones. These are almost blank fields from the point of view of the security. Nevertheless it’s no longer possible to avoid this discussion: the market requires following these trajectories. So information security must follow them too, but not in a passive manner: it should properly *address* the evolution of technology.

UPostBank cannot give up these business opportunities and be cut out of the market, but still cannot give up its security.

Predictability, measurability and persistence. Three faces of the risks.

Are they constant or changing characteristics? Is it possible for a risk to become from predictable unpredictable, from transient persistent, or vice versa? Which are the factors that trigger this change?

Transient risks can definitely become persistent for instance, as technology and services that are provided, but even internal and service delivery processes change. Risks change their nature.

It is important to carry out more risk analysis. The census for instance is a considerable work, a *snapshot* of the current situation. But maintenance and continuous updating are compulsory, because risks evolve, even remaining the same, and their impact might be different from time to time. In this regard, in UPostBank’s InfoSec management an entire unit is dedicated to risk analysis. This is held in high regard within the company.

The IS of UPostBank *has been violated. How does the company react?*

Foremost, what kind of violation? An analysis of what happened is the first step.

In UPostBank anyway there are *ad hoc* business continuity and disaster recovery plans. They come into action as soon as the violation is discovered.

However, even in case of tampering, the essential services for customers and the functioning of the internal structure must be guaranteed. UPostBank has almost one hundred and fifty thousand employees. Even if the violation was only of the Archive Employee, and not the Archive Clients, however it would be a *massive* damage. These large numbers require a very strong focus on all the aspects of security.

As mentioned earlier, UPostBank *has not been immune to attacks***.** *Has the InfoSec focus changed over time? Before or after the security incident?*

The structure must be always ready and reactive. In UPostBank there is a first-level monitoring framework that is in contact with transactions and protects the infrastructure layers on which the applications and services are based, and from which alerts come. UPostBank's InfoSec manages these alerts in the *response domain*, implementing countermeasures.

In UPostBank history there were attacks that technically did not lead to the loss of any data. For example some years ago there was a website defacement: the web page layout had been modified, reporting these words: "This site has been hacked". Just the layout had been changed: hackers hadn't tempered with the corporate information archive. Nevertheless there was a huge reputational damage.

In that case the first thing to do was a first-level, quite cursory analysis of the macro impacts, then another, more detailed analysis about the countermeasures to adopt. Lastly there was a *communication action*, in order to make UPostBank's stakeholders aware about UPostBank's commitment. UPostBank invests a lot on security and has a very strong structure.

Moreover it promotes collaborative actions with other companies that actually are competitors, in order to keep pace with innovation and share information.

Something different happened once to the system that manages all the shipments, post office and agencies. For four entire days there was an operational block. Newspapers said that Anonymous, LulzSec, and the like had penetrated UPostBank's information systems. Actually it was simply a technological upgrade, planned for those days, which had led to an overload of the infrastructure. A technical problem in service delivery, at the end, not external/internal hacking. In that case of course no security assessments were carried out. That wasn't an attack, so nothing could have been done to prevent it.

Given the recent attacks to the CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) and other security violations of many Italian Universities, is UPostBank *safe?*

No company is safe today. It would be *naïve* to feel safe.

Rather, UPostBank feels motivated to continue the path taken. UPostBank is however on the forefront of Security. In a recent national ranking about safe home banking, UPostBank's products are the second.

Through the Competence Center where the Research on Information Security is conducted, the scenario of evolution of the security landscape and logical security is continuously monitored.

UPostBank is very sensitive to the issue of violations of company archives, because it is aware about the endless value of its information assets. It is as great as attractive to hackers or just people that are looking for momentary glory.

Attacks occur every day, and certainly they are not underestimated. However, the fact that so far they weren't able to penetrate its systems doesn't make UPostBank safe or quiet.

And, for the future, *how does* UPostBank *learn from its own and other companies' past mistakes?*

UPostBank shares information and best practices with other similar companies but also with firms from other industries that can bring significant experiences.
The aim is to pool the knowledge of what happened to other organizations as much as possible, and not just what can be read on the newspapers.
UPostBank organizes two three hour sessions where technical information about the dynamics of the incidents and new attacks are exchanged.
It's important to have the ability to always be "on the frontier".
Information Security shouldn't be thought as the security of a closed and barricaded castle, but as the security of an airport, crossed by millions of people, where the exact control of who enters and leaves is not possible, but however security of processes and smooth operations must be guaranteed, so that the whole machine has to work regardless of who enters and leaves. Nevertheless processes that recognize and block the anomalies must be activated. *Response* must be quick.

The interview highlights the relationships among the two paradigms and the countermeasures related to the TFI model. In fact it answers to all the following questions:
- What does UPostBank do to handle *predictable, measurable and persistent risks* from the *technical* point of view? What at the *formal* and *informal* levels?
-What does UPostBank put in place to fight against *unpredictable, non-measurable and transient* risks at all the above mentioned levels?

This is going to be much clearer building a matrix like the one below:

	BISS *Prevention* *(for predictable, measurable and persistent risks)*	**IW** *Response* *(for unpredictable, non-measurable, transient risks)*
T	-Risk analysis - *In the abovementioned census, a* risk measurement *has been conducted. Present vulnerabilities have been studied and the impact of each one of them measured (*Business impact analysis*).* -Vulnerability assessment -Improvement actions	- Business continuity and disaster recovery plans. - The 24x7 Security Control Center denounces all the anomalous accesses. -Two three hour sessions where technical information about the dynamics of the incidents and new attacks are exchanged. -Alarms are highlighted, accounts are locked and all technical actions are done to protect the customers, interpret weak signals and always have a ready answer. -Corrective actions. *In DDoS attacks, for instance, once a suspicious traffic has been intercepted coming from those IP addresses, the provider is asked to stop it. In this way services are not compromised and safe.*
F	-*“Business Protection” defines* policies and guidelines *valid for all the group.* -*Compliance with respect to the ISO 272001, the minimum requirements and the evolution of the Privacy Code is constantly verified.*	-*A sort of “*Information Security audit*” checks if there are irregularities or any gaps to be filled with respect to the ongoing procedures.* - *In “Business Protection” there is a specific unit that monitors the security policy and makes inspections.*
I	-*Regarding the front-office there is a big effort of* formation, communication, training *with frequent* inspections. - *UPostBank’s Research Center has developed a course to follow on the Internet about frauds* -*Clerks are trusted*	- *In “Business Protection” there is a specific unit that monitors the security policy and makes inspections.* -*Like in the after-attack described before,* communication actions *reassure stakeholders about UPostBank’s commitment on Security and mitigate the reputational damage.* -*Sharing of information and best practices with other similar and non-similar companies.*

Table 3: Combining BISS and IW paradigms with TFI countermeasures

5. Conclusion

The Business Information Systems Security (BISS) and the Information Warfare (IW) paradigms (even addressed respectively as *prevention* and *response* paradigms) have usually been opposed in literature, associating the former to non-military contexts, while the latter to the military ones.

Nevertheless, these classic associations are becoming improper as the features of the risks that are fought by the two paradigms have remarkably changed.

The *threat environment*, as Baskerville (2005) notices, has changed, and today commercial, government, and not-for-profit organizations (the non-military contexts) face security risks whose characteristics are typically ascribed to the IW paradigm.

In this way, BISS and IW, prevention and response, coexist within the same organization and feed off one another.

Choosing the security attack as focus of the analysis, it has been displayed that the main domain of BISS-prevention is the "pre-attack", while the IW-response one is the "post-attack". Nevertheless, both of them are present before, during and after the security attack.

Through the interview it has been shown how the *tangible* evidence of the paradigms in the organization is represented by the countermeasures used to handle the security risks.

As demonstrated in the case study, both prevention and response pass through the TFI countermeasures.

Åhlfeldt *et al.* (2007) expanded the commonly accepted model to stress the three souls of Information Security. Technical, formal and informal levels imply different countermeasures that should be adopted by those organizations (like the one studied in the case) that aspire to make information security an asset, a strength to brag about with its stakeholders.

The common mistake is to focus just on the technical part, neglecting the other two. Media and newspapers have been reporting unpleasant episodes that occur to organizations where a violation at the informal level (i.e. unawareness on the internal security policy by employees) has a *domino effect* on the entire information system security.

But depending on what is a countermeasure chosen rather than another?

As well outlined in the matrix at the end of chapter 4, the characteristics of the risk- *predictability, measurability, and persistency*- determine the use of a specific countermeasure.

While predictable, measurable and persistent risks refer to the BISS-prevention paradigm, unpredictable, non-measurable and transient risks lead to embrace the IW-response paradigm. The latter ones are increasing, and will increase even more as an organization (like UPostBank) expands its horizons. When there are many lines of business, diversified and unexplored, new technologies and new services to delivery, organizations inevitably face new risks, or just old ones with different (changed) features.

For all these reasons the contextualistic approach suggested by Pettegrew seemed particularly suitable. Context is decisive. The emphasis put on it is entirely justified. As in UPostBank, the business environment changes and is changed: the context affects the content (risks), and vice versa. Therefore the processes (countermeasures) dynamically change.

Risks might become from predictable unpredictable, from measurable non-measurable, from persistent transient, and vice versa.

Elsewhere I've read that *strategy* is learning, positioning, but above all forgetting the past successes and foresight (Hamel and Prahalad, 2004). IW moral is pretty much the same.

The best fighter is the one who frustrates the plans of the enemy, Sun Tzu stated. This is prevention *and* response. To prevent the enemies' moves but also to be able to respond, *quickly*.

In this *war* an organization needs allies that are the other organizations: its direct competitors, but also firms from other industries, as the activities and coaching sessions promoted by UPostBank demonstrate.

Future research should therefore provide further *practical applications* of the two paradigms in order to devise a recipe for supporting the information security management. Organizations are still reluctant in coming out and revealing themselves for fear of losing public confidence and new attacks that exploit the same vulnerabilities.

Against unpredictable, non-measurable and transient risks the best thing to do is to pool the knowledge as much as possible, share operational information about the security attacks occurred, and so build a common front against the enemy.

To feel safe is naïve, even for an organization whose structures and commitment in information security are strong.

A company should always be on the frontier of Security.

References

Åhlfeldt R.M., Spagnoletti P. and Sindre G. (2007), *Improving the Information Security Model by using TFI*. In "New Approaches for Security, Privacy and Trust in Complex *Environments*", IFIP Springer Series, Springer Boston, Volume 232/2007, 73-84

Arbor Networks, 2011. Network Infrastructure Security Report. Available from: www.arbornetworks.com [Accessed 12 November, 2010].

Aron J. (2011). *Hackers in China target US government Gmail accounts* [online]. Available from: http://www.newscientist.com/blogs/onepercent/2011/06/chinese-hackers-target-us-gove.html [Accessed 20 June, 2011].

Australian Government- Department of the Prime Minister and Cabinet (2010). *Guidelines for Cabinet Submissions and New Policy Proposals.* Available from: http://www.dpmc.gov.au/implementation/policy.cfm [Accessed 4 July, 2011].

Baskerville R. (2005). *Information Warfare: A Comparative Framework for Business Information Security*. Journal of Information Systems Security, 1(1), 23-50.

Bell, V. (2003). *A different battlefield, the same strategy. How the OODA Loop applies to business* [online]. Available from: http://www.thefabricator.com [Accessed 5 July, 2011].

Business Dictionary, 2011. Security breach. Available from: http://www.businessdictionary.com/definition/security-breach.html [Accessed 20 June, 2011].

Cho S. (2007). *A Contextualist Approach to Telehealth Innovations.* CIS Dissertations. Paper 13. Available from: http://digitalarchive.gsu.edu/cis_diss/13.

Cronin B., Crawford H. (1999). *Information warfare: Its Application in military and civilian contexts* [online]. Available from: http://indiana.edu/~tisj/readers/full-text/15-4%20cronin.pdf [Accessed 1 July, 2011].

Cutting Edge, 2002. *Corporate Security: Protecting Productivity* [online]. Available from: http://www.cuttingedgeinfo.com/Reports/FL53_Security.htm [Accessed 21 June, 2011].

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2008. Comunicato Stampa- 14 gennaio 2009. *Amministratori di sistema: occorre massima trasparenza sul* *loro operato. Il Garante fissa i criteri, quattro mesi per mettersi in regola* [online]. Available from: http://www.garanteprivacy.it/garante/doc.jsp?ID=1580831

Ghacks, 2011. *Firefox 4 Supports Content Security Policy*[online]. Available from: http://www.ghacks.net/2011/05/08/firefox-4-supports-content-security-policy/ [Accessed 4 July, 2011].

Hamel G., Prahalad C.K., (2004). *Competing for the future* (p. 3) [online]. Available from: http://www.altfeldinc.com/pdfs/Competing%20for%20the%20Future.pdf [Accessed 15 July, 2011].

Herath T., Rao H.R. *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.* Decision Support Systems 47 (2009) 154–165. Available from: www.elsevier.com/locate/dss. [Accessed 14 July, 2011].

Ibrahim M, Ribbers P.M.A. (2009). *The impacts of competence-trust and openness-trust on interorganizational systems*. European Journal of Information Systems (2009) 18, 223-234

International Organization for Standardization, 2011. *ISO/IEC JTC 1 Information Technology Standards* [online]. Available from: http://www.iso.org/iso/jtc1_home.html [Accessed 4 July, 2011].

Keizer, G. (2011). *DefenseNews hacked* [online]. Available from: http://www.databreaches.net/?p=19330 [Accessed 21 June, 2011].

Kizza J.M. (2009). A GUIDE TO COMPUTER NETWORK SECURITY. Computer Communications and Networks, 2009, Part II, 63-88, DOI: 10.1007/978-1-84800-917-2_3. Available from: http://www.springerlink.com/content/m241t851w46j6388/ [Accessed 11 July, 2011].

Levinthal D.A., March J.G. (2003). *The myopia of learning.* Strategic Management Journal, 14, 95-112.

LulzSecurity, 2011. Releases. Available from: http://lulzsecurity.com/releases/ [Accessed 28 June, 2011].

Magalhaes R.M. (2003). *Host-Based IDS vs. Network-Based IDS (Part 1).*

MilitaryTimes, 2011. *A message to subscribers* [online]. Available from: http://militarytimes.com/news/2011/06/gannett-cyberattack-statement/ [Accessed 2 July, 2011].

Neal, D. (2011). *Lulzec hackers warn NHS over its security* [on-line]. Available from: http://www.theinquirer.net/inquirer/news/2078004/lulzec-hackers-warn-nhs-security [Accessed 28 June, 2011].

OWASP, 2011. *OWASP Top 10 Project* [online]. Available from: https://www.owasp.org [Accessed 3 July, 2011]

Papazoglou M.P., Ribbers P.M.A. *e-Business Organizational and Technical Foundations*, John Wiley & Sons, Ltd., 2006. ISBN-13: 978-0-470-84376-5 or ISBN-10: 0-470-84376-4

Pastebin, 2011. Final release. Available from: http://pastebin.com/1znEGmHa [Accessed 28 June, 2011].

Perez, S. (2009). *Top 8 Web 2.0 Security Threats* [online]. Available from: http://www.readwriteweb.com/enterprise/2009/02/top-8-web-20-security-threats.php [Accessed 30 November, 2010].

Pettigrew, A.M. (1985). "Contextualist Research and the Study of Organizational Change Processes" in: *Research methods in information systems: proceedings of the IFIP WG 8.2 Colloquium,* E. Mumford (ed.), and Elsevier Science Pub. Co., Amsterdam; New York: North-Holland; New York.

Porter M.E., Millar V.E. (1985). *How Information gives you competitive advantage* [on-line]. Available at http://zaphod.mindlab.umd.edu/docSeminar/pdfs/Porter85.pdf [Accessed 15 July, 2011].

Princeton- IT Security Office, 2011. *Princeton University Information Security Policy*. Available from: http://www.princeton.edu/itsecurity/policies/infosecpolicy/ [Accessed 11 July, 2011].

Schwartz, M.J. (2011). *Schwartz On Security: First, Know You've Been Breached* [online]. Available from: http://www.informationweek.com/news/security/attacks/229000160 [Accessed 16 June, 2011].

Scambusters, 2011. *The 5 Most Common Social Networking Scams* [online]. Available from: http://www.scambusters.org/socialnetworking.html [Accessed 30 November, 2011].

Shinn, J. (2009). *Digital Security Report: Social Networking Sites Expand Risks for Employers* [online]. Available from: http://jshinn.wordpress.com/2009/07/26/digital-security-report-social-networking-sites-expand-risks-for-employers/ [Accessed 1 July, 2011].

Siddiqui, B. (2002). *Exploring XML Encryption, Part 1*. Available from: http://www.ibm.com/developerworks/xml/library/x-encrypt/ [Accessed 11 July, 2011].

Sophos, 2011. *Security threat report 2011* [online]. Available from: http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/sophos-security-threat-report-2011-wpna.aspx [Accessed 1 July, 2011].

Spagnoletti P., Resca A. (2008). *The duality of Information Security Management: fighting against predictable and unpredictable threats*, Journal of Information Systems Security, Vol. 4 - Issue 3, 2008.

TechCrunch, 2011. *Identity Theft*. Available from: http://www.crunchgear.com/2010/02/10/identity-theft-costs-rise-overall-while-costs-per-victim-decline. [Accessed 20 June, 2011]

The official Google blog, 2011. Ensuring your information is safe online [online]. Available from: http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html [Accessed 21 June, 2011]

Twitter Engineering, 2011. *Improving Browser Security with CSP* [online]. Available from: http://engineering.twitter.com/2011/03/improving-browser-security-with-csp.html [Accessed 1 July, 2011].

U.S. Department of Health & Human Services, 2011. HIPAA Security Series. 6 *Basics of Risk Analysis and Risk Management.* Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf [Accessed 6 July, 2011].

Valtiovarainministeriö (2008). Hankkeen tietoturvaohje. VAHTI, vol. 9, p. 23 [online]. Available from: http://www.vm.fi [Accessed 1 April, 2011].

Van Niekerk J.F., Von Solms R. (2009), *Information security culture: A management perspective* [online] Computer & Security 29 (2010) 476-486. Available at www.sciencedirect.com [Accessed 15 July, 2011].

Widman J. (2011). *10 Massive Security Breaches* [online]. Available from: http://www.informationweek.com/news/galleries/security/attacks/229300675?pgno=1 [Accessed 21 June, 2011].

Wilson, D. (2010). *Employees consistently breach security policies, report finds* [online]. Available from: http://www.techeye.net [Accessed 1 July 2011].

Wikipedia, 2011. *ISO/IEC 27001.* Available from: http://en.wikipedia.org [Accessed 4 July, 2011].

Yin R. K., 2005. *Lo studio di caso nella ricerca scientifica*. ISBN 88-8358-687-5.