Università degli Studi di Salerno
Dipartimento di Informatica

DOTTORATO DI RICERCA IN INFORMATICA ED INGEGNERIA
DELL'INFORMAZIONE
CICLO XV - NUOVA SERIE

Tesi di Dottorato in Informatica

Cyber security and ubiquity: an human-centric approach

Candidate
Antonio Colella

Coordinator
Prof. Alfredo De Santis

2016/2017

To my wife and my daughters

Abstract

Information and communication technology systems have become indispensable parts of our lives up to become the main strategic dimension to be protected by the State. Nonetheless, we have seen so far that the technical security is not enough for protecting the global cyberspace. The vast development of Information and Communication Technologies and the innovations applied in the field of governance and management push the researchers to change their perspectives in finding new security paradigms. The major effort regards the capability to identify some appropriate tools that have the characteristic of better fit with the object to protect in the real world. One of main aspect that can ensure the success in this operation is the correct integration and harmonization of the human factor with all remaining factors of a security system. The CIA (Confidentiality, Integrity and Availability) paradigm is no more valid and able to perform its effect in a post-modern world, and why Cloud and Pervasive Computing requires a new approach in which the user become the main actor of the entire security system. A valid complement (usable) to technical solutions has been found in a Societal Digital Security Culture (SDSC) as a set of collective knowledge, common practices, and intuitive common behavior about digital security that the members of a Society share. The idea is that members of the Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions. Under this prospective, trust and co-partnership are two main components of the SDSC approach that can boost the security of Information Systems. Trust and co-partnership can be applied to risk analysis based on Bayesian Network and allow the human factor to be considered the main element

of Information Security Management System (ISMS).

Contents

List of Figures

Chapter 1

Introduction

"One day the machines will be able to solve all the problems, but none of them will deliver us one."

— Albert Einstein, *1452-1519*

1.1 Introduction

Cyberspace is a borderless new universe in which all actors, including States, share information and communications technologies, now indispensable to the modern lifestyle. Since the beginning of the 21st century, the ability to leverage cyberspace has become the most important source of power. Due to the proliferation of ICT systems into all aspects of life, the importance of information for political matters has increased awfully. State and non-State actors can use this power to achieve objectives into cyberspace and physical world. Low cost and high potential impact make cyber-power attractive to all actors. In fact, cyber threats have grown exponentially with the proliferation of the cyberspace infrastructures. Consequently, cyberspace has become a warfighting domain with the potential to destroy or make useless logical, physical, technical, and virtual infrastructure, damaging in fact critical National capabilities. This scenario forces all national institutions to a review of their defense strategies, because of the difficulties to identify the actors of a cyber-attack. It then becomes necessary to gain a broader view of the problem to acquire more detailed information, useful

to identify such sources of cyber-attacks. This new point of view can be achieved by using the analytical method applied to data streams flowing across the cyberspace. Furthermore, in the age of globalization, countries and their tissue business are increasingly dependent on Internet so that the JIT (Just in Time) production model forces the producer to adopt production control systems like SCADA (Supervisory Control and Data Acquisition Systems) now permanently interconnected to the Network. Moreover, the policies of integration of web contents such as the ones present in Web 2.0 which is a network that has the ability to merge contents of individual sites in a single organically indexed content are being superseded by the more futuristic Web 3.0, where content can be indexed on the basis of the semantic meaning, and probably in the next ten years, from the Web 4.0 or Metaweb, where information will be analyzed and evaluated automatically from the Web. In this context, it is important to fully investigate the meaning of globalization, interdependence and cooperation in Security, in order to understand the structures and mechanisms that characterize the new international context. It is important to recall that the development of the Society has always a direct impact on the definition of the security paradigms. In this thesis we intend to fully investigate how support the technical solutions, taking into consideration the net-centric position of human factor and the preeminent rule of Societal Digital Security Culture (SDSC) with regard to Digital Security Culture (DSC). The measure that affect the SDSC, in fact, have much stronger impact on enhancing the security readiness because of the individuals tendency to imitate each others behaviors and due to the major strength of the efforts at societal level. In order to improve the SDSC, we are aware of the importance of enhancing the trust and co-partnership of the people towards the ISMS even national and private, drawing the attention on the importance of security measures as an economic fly-wheel and to protect the common privacy rights. Here we present a new perspective on the validity of current security models compared to the evolution of technology. Our starting point, in fact, is that it is very hard, if not impossible, to set up a security organization forgetting that the main weakness of all security systems is the human factor. For example, recent security infractions, such as the Stuxnet or Duqu malware, have confirmed that the security based on technology and organization is very hard to reach without the

full involvement of the human being. Starting from this perspective, we discuss on the current security models and their validity. The attempt to humanize the security is even more urgent if we consider some new technology such as, for example, Cloud Computing as we will see later, and its limitations in terms of investigations and the tracking of criminals. In this thesis we propose a novel model based on trust and the co-partnership that are presented as the stronger glue among the factors. The presented model is based on Hassells organizational and user behavior security model and the needs of an integrated system based on the societal digital security culture approach. At the end, our goal is to reach a redefinition of risk analysis based on Bayesian Network for maximizing trust and co-partnership as engine of human behavior.

1.2 The cyber-dimension and its relevance for national security

Within the last two decades, the spread of the internet and ICT have led to the digital revolution, i.e. the process that consists in the translation of information into computer language. This digitalization is affecting every sector of our life to the point that the so called cyber-dimension, i.e. that intangible and virtual place made my computer networks, has gained more and more importance within our society. Initially, computers and communication networks had not been developed for the purposes for which nowadays we use them. Indeed, as many other inventions, they have been conceived at their origins as military tools. The military sector has given a great impulse to the development of such technologies. It was during the second world war that two of the most quoted mathematicians laid the foundations of the computer science: John Von Neumann and Alan Turing. The former was working to the Eniac project at the Ballistic Research Laboratory of the Usa for the development of a system able to solve computing problems for the launch of ballistic missiles. He developed a scheme which is still the one whereby computers are put together: central processing unit (CPU), memory unit and input/output devices, all connected each other through cannels called busses. Alan Touring, instead, worked for the English Department

of Communications to decode the German communications encrypted with the system Enigma. He invented a computing machine, based on its previous studies, whose mathematics fundaments are still those on which computers are built. If at the beginning of its history the computer was a mere calculus elaborator, it gained success thanks to many developments: its memory capacity was increased as well as its calculating capacity; the operation time was reduced permitting this way to elaborate some calculus otherwise impossible for the human being; finally, its functions were incremented as well its usability. In the sixties, the Silicon Valley saw the rise of many companies such as the Hewlett-Packard and the Apple increasingly projected towards the production of computers for mass consumption with a particular attention to design and functionality for leisure and free time. Many other technological devices have been developed over time and the people have started to use the computer and its derivatives to work and carry out their daily activities, also due to their cheaper and cheaper costs. But this increase in the spread of many different electronic devices such as computers, mobile phones, tablets probably would not have been possible if computer science had not met telecommunication technology. Indeed, all these devices are connected to the web. The Internet roots date back to the late 50s. At the time of the start of the cold war, a nuclear explosion would have paralyzed the telecommunications networks of the time, making impossible to the strategists to communicate with the troops and react to the aggression. Moreover, in that period the URSS put into orbit the first artificial satellite (Sputnik I), so that in the USA grew the fear of being overtaken by the Russian technology. The Rand an institute dedicated to furthering and promoting scientific, educational, and charitable purposes for the public welfare and security of the United States was dealing with this problem. Paul Baran, a Rand researcher, started working on his idea of a decentralized communication network. Up until then, the communications networks were based on a centralized system in which the message flew from the centre to the periphery. Of course, if the enemy had destroyed the centre the military would not be able to communicate to organise the counterattack. A decentralized communications network would permit to solve this problem. Indeed, in a network in which a message can be sent from each node the system could keep on working even if an enemy attack had destroyed a

part of the network. So it was necessary to create a redundant communications network (multiple back-up communication modalities) in order to connect any two centres of command. Another important idea proposed by Baran was that the transmission of the information should not flow in the form of a single block, but fragmented in smaller and separate parts (packet switching) that can travel independently, perhaps even through different channels. What Baran conceived, was a mechanism capable of retransmitting a large amount of data through a cheap channel, strong enough to overcome a nuclear attack. The Barans idea was revived by an ARPA project directed by Bob Taylor in the second half of the sixties. ARPA was the Advanced Research Projects Agency whose aim was that of maintaining the US technological capabilities to the step, and possibly at the cutting edge, with respect to those of the enemies. The agency would try to connect a small number of computers and create a network through which researchers could interact. The goal was that of improving transfers of scientific results as well as developing the necessary military administration network techniques. The network described by Taylor would later become known as ARPANET. The 29th of October 1969 at 10:30 pm a machine placed at UCLA communicated with another machine at the Stanford Research Institute. That was the first ARPANET transmission. A further step in the development of ARPANET was to connect it to other networks, PRNET and SATNET, respectively based on cable and satellite communications. Quickly many other computers were connected to ARPANET. But since there were different kind of computers connected to the network, it was necessary to make them interact following clear communication protocols, i.e. the strict rules that every node of a network had to take to dialogue with other machines. The Network Control Protocol (NCP) and the File Transfer Protocol (FTP) were the first protocols developed and were born at the early seventies. Not only it was important to make different kind of computers interact within the same network, but after the birth of other networks the goal was that of making these different networks interact. In 1973, the transmission control protocol (TCP) was conceived to make computer networks communicate and led to the possibility of communication between networks of different nature such as the telephone, satellite TV and radio. In a short period of time, another protocol was conceived, the Internet Protocol (IP): while the TCP managed the

packet creation and control, the IP managed the data flow. The TCP/IP protocol is still the base of the internet. The number of computers connected to networks grew a lot so that it was difficult for the Darpa to go ahead with the military project which required confidentiality. So, the agency dismembered from ARPANET a closed network, called MILNET, for the military affairs. ARPANET continued to serve the scientific research and remained open. The service providers multiplied over time. ARPANET was dismissed in 1990 and the National Science Foundation was responsible for managing the entire academic network in the Usa. Even though the basics of the internet were laid in the United States, it was in Europe at Cern that the internet (as we know it) was conceived. Tim Berners-Lee, a computer scientist at Cern, started working on a software, called Enquire, that would permit to keep track of all the different projects. That was the first step to the internet development. Berners-Lee prosecuted with its project and developed a hyper textual language, HTML. Moreover, he invented a client software composed of a browser and an editor to create and modify HTML files. Finally, he created a server to host HTML files. The world wide web was born. An important characteristic of the web was the access freedom: indeed, all the people could use it. This fact and many innovations connected to the web arisen later such as search engines (Yahoo! above all) permitted the expansion of this new technology. In particular, the reason for which the utilization of the web has spread so much is to be found in its many opportunities; just to mention some of them:

- The possibility to communicate in a fast way with people all over the world, thanks to instant messaging services (such as e-mail), social networks and the voice over IP (VoIP) technology. It is estimated that the number of active profiles on the social networks are just a little less than ten billion and they are going to increase again. Many people use them to get in touch with other people all over the world and or to communicate. For what regards the VoIP technology, it has a very low cost compared to any other phone service. This possibility to communicate is not used only for leisure, but also and especially for business: in fact, the e-mail was born in the ARPANET context to exchange messages between universities.

- The possibility to get a great amount of information. Regardless of the quality of the information, the number of news and the amount of shared knowledge in the network are huge. Especially, this is thanks to the raise of numerous online encyclopaedias and newspapers. A couple of years ago, internet passed the number of one billion of websites.

- The possibility to buy an increasing quantity of outputs. Indeed, in the last few years e-commerce has been growing. It achieved record numbers especially in China and US (respectively 395 and 264 billion of euro in 2014) . Although most of the purchased goods are physical goods, it is also developing a kind of online business related to the service industry. Moreover, not only the citizen can rely on the internet for private interests, but also it can access to many public services. Indeed, also the public administration has been digitalizing its activity, the so called e-government.

But as for any other tool, the opportunities can transform into threats and vulnerabilities depending on the utilization made by the user. The concern about the risks posed by the malicious use of the internet has reached a very high degree to the point that the cyber-issue has entered the political agenda of many countries. The reason why cyber security has reached the top of the political agenda in many countries is to be found in the role that the cyber-dimension plays within our society:

- an increasing amount of information is digitalized; the secrecy of both the government and the business sector information is threatened;

- almost the totality of the critical infrastructures relies on it; indeed, the electricity grid, the rail system, telecommunications, any kind of pipeline, and many other critical infrastructures are all connected to networks;

- more and more people use computers and have access to the internet; consequently, their privacy is jeopardized.

The cyber domain is still a largely unexplored area and this has consequences that cannot be underestimated. Governments around the world, but especially those of the most advanced countries, are facing an issue that grows hand in

hand with technological development. Technological progress could become then a double-edged sword if adequate measures are not adopted. The concept of cyber security has always been linked to the problem of information: the interdependence between different software-based control systems has always been a sensitive target that required appropriate protection for allowing to the post-industrial economies continuous and reliable operation as well as for ensuring national security. Then, from this consideration, the critical information infrastructures emerged as a referent object. Information, in turn, has always been an aspect related to power, diplomacy and armed conflict. Therefore, in light of this, the cyber domain falls perfectly into logics of geopolitics and international competition. The development of a National Cyber Security policy has to deal with many challenges both known and unknown. Furthermore, since both the national and international environment brings with it a large set of pre-existing treaties, the obstacles to the freedom of policymakers increase. For this reason, it would be an optimum if all the cyber security policies would be connected to a homogeneous architecture, which is entitled to manage the Information Security System, and at the same time reducing redundancies and overlapping legislations. In this regard, NATO has recently increased its focus on cyber security and its cooperation with non-NATO nations, the European Union and International Organizations as well. But, unfortunately, there is still a lot of work that has to be done before achieving the so long-wished smooth synergy between all actors involved in cyber security. Estonia, known for the cyber attacks endured in 2007, gave birth to a framework purely imbued on resilience. Since 2009, a number of important decisions that have been taken have allowed Estonia to become today one of the reference countries with regard to progress in the cyber security field. The central body that deals with cyber security is the RIA (Estonian Information System Authority) and it is also noteworthy its close cooperation with NATO CCDCOE of Tallinn, through which play a crucial role in cyber defense.The main objectives are improving Estonian defense of critical infrastructure, investing substantially in the military, and improving resilience. Although, the defense budget for 2016 was fairly modest, it is set to rise year-on-year by around 7%. Estonias achievements in cyber security have also benefitted from a strong IT partnership between the public and private sector. This conjunction gave birth to the Cyber

Defence League. However, the real key to Estonian cyber security lies in the inherent safety and security built-in to every single Estonian e-Government and IT infrastructure system. Estonian citizens and businesses operate with confidence, knowing that their data is safe and their transactions are secure. Indeed, the best kind of cyber security is one that everyday people never have to think about. For the United States, although the problem is not unknown nor has recent origin, it has long been at the center of debates. The same American concept of cyber threat has changed a lot over time, going hand in hand with the attacks and events that involved the country over the years. The emphasis has shifted from non-state terrorism to state actors activities, and predominantly from a political to an economic matter. Terrorism has always been a top-priority threat to address for United States, but the improvements made in the digital field have brought US to reconsider the securitys global framework giving to cybercrime the proper credit. The same former President Obama has identified cyber threats as one of the more serious economic and national security challenges of all times. Although the US governmental architecture assigned to cyber security is very complex and bureaucratically articulated, with an unspecified number of agencies, offices, commissions, boards, the federal effort to protect US communications and information infrastructure and securing Americas digital infrastructure is remarkable as the amount of resources planned to invest in cyber security. However, the major hindrances to development continue to be the wide dispersion of power among the various stakeholders and the persistent lobbying activities carried out by those opposing the regulation of private networks to facilitate the protection of critical information infrastructures, because its considered profitless.

1.3 The persuasive effect of thecnology in our world

Pervasive Computing is based on the idea that embedding computation into the environment and everyday objects would enable people to interact with information-processing devices more naturally than they currently do, and in a way that suits whatever location or context they are involved. For that reasons,

when referring to Pervasive Computing we intend the following meanings:

- Ubiquitous Computing
- Cloud Technology
- Things that Think
- EveryWare
- Pervasive Internet
- Ambient intelligence
- Proactive Computing
- Augmented Reality

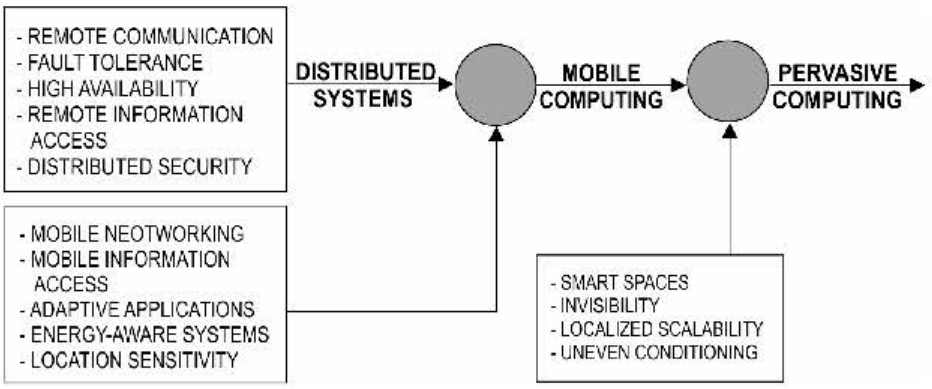

Figure 1.1: Taxonomy of computer systems research problems in Pervasive Computing.

In other words, Pervasive Computing represents the major evolutionary step from mid-1970s in the field of Distributed Systems. Figure 1.1 presents a taxonomy of computer systems research problems in Pervasive Computing. In terms

of Security, the human factor is the main point to be considered and there is little empirical evidence about how human, organizational, and technological factors impact IT Security Management (ITSM) [3]. Even in Cloud Computing environment, the human factor is vital. A Cloud Service Provider, for instance, has to develop a strategy to manage several security issues that derive from the developing capabilities illustrated in Fig 1.2.

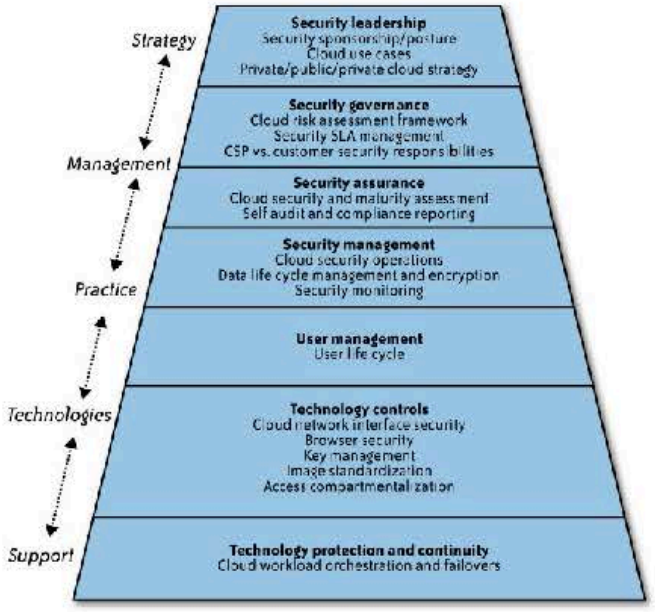

Figure 1.2: An enterprise security architecture for Cloud Computing.

Security Leadership is overall the most important factor which has to be present. In particular, it is important for the Management Staff to have a deep understanding of the issues involved in Cloud Computing and it is vital that they are educated on the latest solutions and challenges related to it.

The traditional security paradigm is different for Cloud Computing, so it is essential for the top managers to fully understand the complexities and the capabilities of solutions into the cloud. Hence, the application of traditional security techniques is not enough [4].

1.4 Internationalizzation and globalization of security

When considering the phenomena of globelization and internationalization, the "consumerization" has a big role in a possible security paradigm. Despite the impression that business and IT leaders are reluctent to accept the IT consumerization, the survey conducted by Avanade [5] has shown that companies are actually willing to embrace change and that the main supporters are the highest-level executives within organizations.

Consumerization has two main advantages:

- a full involvement of users, who feel more in charge of security issues even when the assets for personal use (direct participation in security issues);
- incorporate the user communication tools (computers, tablet, mobile phone, etc.) in Information Security Management System (ISMS).

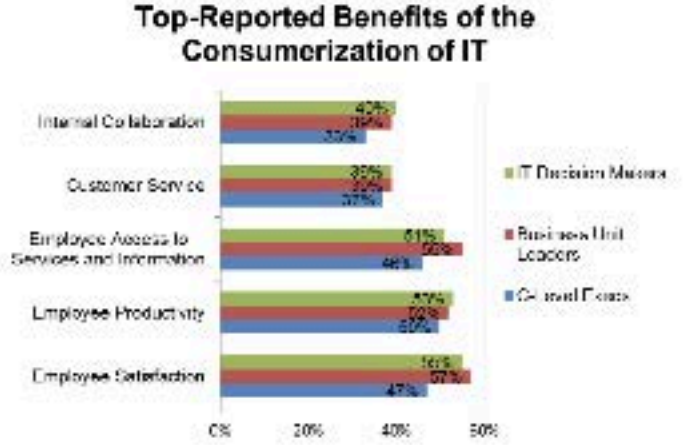

Figure 1.3: Avanade Global survey 2011.

Here almost 73% of C-level executives said that the increasing use of technology owned by employees is a top priority of their organization. From large enterprises to small businesses, in all sectors covered by the survey, the study showed high rates of adoption of personal computer tools in the workplace. Globally, 88% of executives said that the employees currently use their own tools for professional purposes (see Fig. 1.3).

In the approach of the Fluid Information System, an infrastructure moves data and applications dynamically on the hosts into the network [6]. This perspective is important in order to give dynamism to our models.In fact, nowadays criminals do not attack IT infrastructures, they attack the users. Users are attacked by using information they reveal usually on OSNs. Users have become nonchalant over the amount of personal information they effectively broadcast to all and sundry: what we like or dislike, what we do, what we want, where we are, where we are going. Armed with this information and basic social engineering skills, it is easy for criminals to trick us to do something we should not like, for example, go to a compromised website or open a poisoned attachment. The malware itself stays ahead of us thanks to rapid and automatic changes designed to defeat every signature-based defense.The rise of social networking, in fact, combined with the consumerization of devices and mobile computing, means that we like to socialize at work and we like to work at home. There is no longer a virtual boundary between work and home. All these aspects lead to the consideration that more than one single security paradigm exists and we need a "Multi-Paradigm Composition Analysis." approach [7].

1.5 Confidentiality, Integrity, and Availability

Confidentiality aims to prevent unauthorized access to information. The preservation of confidentiality is linked to development of modern Cryptography. Looking, for instance, to phone systems [8], [9], we are not sure that Cryptography may overcome the intrinsic and (probably) insurmountable weaknesses deriving from the use of an open system which may be considered the Internet.

It is still true that the primary advantage of symmetric-key cryptography is efficiency [10], but even the hybrid cryptosystem, where both asymmetric and symmetric Cryptography can be used, has big problems with the "Man-in-the-Middle" attacks. Whereas confidentiality deals with the prevention of unauthorized reading, integrity is concerned with preventing unauthorized writing. As for the confidentiality even for the integrity, Cryptography is the main means for assuring such features. It is important to keep in mind that while data are ciphered nothing can guarantees that malicious or inadvertent codes have altered

the original data. This fact is equally true in the Cloud and Pervasive Computer environment. At the end, if considering the perspective availability of data, it will be realized that is becoming the main security challenge due to exponential growth of DoS and DDoS attacks. The availability of data is mainly the first requirement for using Internet to boost business and services. Unfortunately, to ensure the availability of data, Cryptography is not enough. Moreover, Availability is one of main attributes in security models like CIA, Parkerian Hexad and Cyber Forensics Assurance Model (CFAM) [11] and, with integrity attribute, it is key for hypervisor to guarantee a public cloud built on a virtualized environment. One of the main approach for safeguarding the availability of a system is based on a robust Availability Management infrastructure [4], even if the latest cyber-attacks have showen that such efforts are not enough.

1.6 Contributions of This Thesis

In this thesis we provide new insights on the importance of the human factor for every security system. Recent security breaches showed that every attack begins with the involvement of users and continues with exploiting technology bugs. In almost all cases, without human collaboration, conscious and unconscious, it would be really difficult to reach the criminal goal. Our approach has mainly three characteristics:

- Centrality of the human factor;
- The ability to mold to the scenario to be protected;
- Dynamic adaptation to external and internal threats.

The First step is to deal with the identification of a set of attributes to be used for the construction of a security system fitting to a given context, going beyond the strategy of the pre-established paradigms (CIA and similar). More precisely, in this thesis we focus on idea that members of the Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions, has lead us toward a integrated model based on a cultural approach in which the trust and co-partnership of the security system are the main

focal point. This model implies that technology solutions separated from the surrounding environment are completely inadequate. Social, organizational, and psychological factors have to be considered when implementing security within an organization. A valid complement (usable) to technical solutions has been found in a SDSC as a set of collective knowledge, common practices, and intuitive common behavior about digital security that the members of a Society share. The conjunctions among social factors, technological factors trust co-partnership culture motivation and organizational models will be better harmonized in a single system. In this thesis we analyze *Trust in Security Environment* setting up on a rational component, based on information built on experience and an irrational element, a so-called leap of faith made out of pure instinct, without any logic. We found that Trust and Risk are two inseparable concepts whose binding is supported by rational and irrational character of confidence. We than focus on correct approach to risk management that, by considering the holistic character of the problem, would at same time adequately support the internal working relationship as well as the relationships between organizations. Moreover, we clarify why technology solutions alone are completely inadequate to ensure security. Social, organizational and psychological factors must be considered when implementing security within an organization. Indee, we need to consider how people build communities and to take into account how communication patterns affect interactions. The above consideration guided us at the model that includes the cultural approach where both trust and co- partnership of a security system have a very important role. Security behaviors fostered by information organizations must be achieved by pursuing the motivation and desire as cultural factors. The model considers the societal elements as the most important part of the security system. Trust and co-partnership help to create a strong security culture that serves as a framework to the information security system. At the end of the thesis, we will applied Trust and co-partnership to introduce a predictive cyber security risk assessment model based on Bayesian Networks and hybrid methodology. The motivations underlying this thesis are mainly based on two observations. The first observation is that Trust and co-partnership imply a full involvement of the whole management style. In order to gain co-partnership, the human factor needs to be the pivot of security model. The second observation is

that an hybrid risk assessment model can help to provide a strong foundation for dynamic security modeling. The accuracy of such model wouild be related to the number of scenarios available and for the use of the ability od Bayesian networks to learn parameters from data.

1.7 Organization of the Thesis

In this introduction we have provided an overview concerning the scenarios, the cyber-dimension and their relevance for national security. We investigate the persuasive effect of thecnology in our world and the internationalization and globalization of security. In particular, we discuss why the CIA (Confidentiality, Integrity and Availability) paradigm that is no more valid and able to perform its duties in a post-modern world, and why Cloud and Pervasive Computing require a new approach in which the user become the main actor of the entire security system. Under this perspective, it's paramount to draw the attention on trust and co-partnership as the two main components of the Societal Digital Security Culture (SDSC) as a set of collective knowledge, common practices, and intuitive common behavior about digital security that the members of a Society share. At the end, an hybrid risk assessment model is necessary to improve cybersecurity through human system integration. The results presented in this thesis are based on joint works with Alfredo De Santis, Francesco Palmieri and Aniello Catiglione. The organization of the rest of this thesis is as follows.

- **Chapter 2**: In this chapter we proposed an approach beyond CIS paradigm that has mainly three characteristics: centrality of the human factor; the ability to mold to the scenario to be protected; dynamic adaptation to external and internal threats. The results presented in this chapter have been published in [12].

- **Chapter 3**: In this chapter we analyze the hypothesis of an adaptable model based on consumerization [12]. The basic idea that the members of the Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions. This idea has lead us toward a integrated model based on a cultural approach in which the

trust and co-partnership of the security system are the main focal point. Our model implies that technology solutions separated from the surrounding environment are completely inadequate. The results presented in this chapter can be found in [13].

- **Chapter 4**: In this chapter we deal with integrated Societal Digital Security Culture. The results presented in this chapter can be found in [14] [13].
- **Chapter 5**:In this last chapter we propose improving cyber security through human System integration and propose an hybrid risk assessment model.
- **Chapter 6 - General Conclusions**: Finally, in this chapter we conclude the thesis, by providing discussions and some final remarks.

Chapter 2

Beyond CIA: Confidentiality, Integrity, and availability

" think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. Weve created life in our own image"

— Stephen Hawking

2.1 Introduction

Confidentiality, Integrity, and Availability (CIA) are only the beginning of the Information Security story. When a user logs into a computer, how does the computer determine that the user is really who claim to be and not an hacker? And when the user logs into his account at a specific online bank, how does the bank know that the user is really him and not the hacker? Although these two authentication problems look similar at first glance, looking in a deeper way they are completely different.

Authentication on a stand-alone system requires that the user password is verified. To do this securely, some clever techniques from Cryptography are required [15]. Authentication over a network is open to many kind of attacks. The

messages sent over a network can be viewed by an hacker. To make matters worse, he can not only intercept messages, he can alter messages and insert messages of his own making. He can also replay old messages in an effort to, say, convince a online bank that he is really the legitimate user. Authentication in such a situation requires careful attention to the protocols that are used. Cryptography also has an important role in security protocols. Once the user has been authenticated by the bank, then the bank must enforce restrictions on user actions. For example, the user cannot look at another account balance or install new accounting software on the system. However, system administrator, can install new accounting software on the system serving the online bank. The enforcing of such restrictions is the goal of Authorization. It is important to note that Authorization places restrictions on the actions of authenticated users. Since both Authentication and Authorization deal with the access to resources, is well lump them together under the heading of Access Control.

All of the information security mechanisms discussed so far are implemented in software. Modern software systems tend to be large, complex, and rife with bugs. These bugs often lead to security flaws. What are these flaws and how are they exploited? How can online bank be sure that its software is behaving correctly? How can online bank software developers limit the number of security flaws in the software that they are developing? It is a good practice to examine the development of these software when discussing about software security. Although bugs can (and do) lead to security flaws, these security flaws are created unintentionally. On the other hand, some software are written with the intent of doing evil. Such malicious software, or malware, include the all-too-familiar computer viruses and worms that plague the Internet today. How do these nasty beasts do what they do, and what can the bank do to limit their damage? What can the hacker do to increase the nastiness of such pests? It is well to consider these and similar questions when studying software security.
The user also has many software concerns. For example, after entering the password on a PC, how does one know if that password has not been captured and sent to the hacker? If the user conducts a transaction on *www.onlinebank.com*, how does he know that the transaction he sees on the screen is the same transaction that actually goes to the bank? In general, how can a user be confident

that the software is behaving as it should, instead of as the hacker would like to behave?

It is well to consider these questions as well. When discussing software and security it is fundamental to consider the OS issues. OSes are themselves large and complex pieces of software. They also enforce most of the security in any system, so some knowledge of OS is necessary in order to better appreciate the challenges of Information Security.

2.2 Resilience is More than Availability

The security paradigms are to move toward resilience with respect not only to performance and availability but also to confidentiality and integrity at the higher levels. This is not to say that robustness is not always desirable many of our traditional computer architectures attempt to provide these qualities (for example, checksums allow us to detect and delete corrupted packets, encryption makes our traffic robust to eavesdropping in transit, and automatic failover lets us accept the failure of a single machine). In addition, we believe there are significant opportunities for work that provides resilience (that is, essentially, recovery) at the higher levels. Furthermore, some level of combined robustness and resilience is possible in both the confidentiality and integrity domains. Viewing the system holistically is critical when we consider attack resilience, as is viewing the goal of the attacker more widely. Solutions have to be broader than simply focusing on service provisioning regardless of the operational conditions. They must also provide service while maintaining other significant aspects of service expectations, such as keeping a transaction confidential while still providing some level of attribution and non-repudiation. Ellisons technical report [6] directly requested this, but the concepts seem to have been sidelined at best, and ignored at worst, by the mainstream security researchers. The nature of resilience changes depending on the problem being addressed. If a computer system were tasked with producing a simple yes or no answer to a question, there is no good enough performance. Such a system will either work or it will not, and the best we can hope for is an acceptable error rate (which will also vary depending on context). In contrast, a system designed to control the temperature of a room or control a bipedal robot

can work acceptably with inexact solutions. Therefore, an essential part of building resilient systems is thinking about the problem at hand and recasting it from a discrete (and hence brittle) problem to an analog problem. This alone opens the door to solutions that provide the benefits of information technology without its inherent tendency toward failure under unexpected conditions. Furthermore, depending on attacker motive, a more analog view of the world may allow us to protect the confidentiality of data even in the presence of a breach. Resilience for availability, integrity and confidentiality ultimately refer to the overall goal of the system. Complex systems are highly interdependent and the effects and implications of these properties are not necessarily trivial. Bishop at all [16] propose that resilience, robustness and survivability are systemswide properties, not necessarily achievable with the individual specification of component properties and requirements. Local violations of these properties at the component level may not only be acceptable but sometimes necessarily for the resilience of the overall system. One of the issues we encounter in security is that a mostly secure approach is not good enough. This tendency to reject solutions is a huge issue for those working in the resiliency space. Despite attacker adaptation, if an approach removes options from an attacker, it is an incremental step toward a truly resilient system. We argue that systems that provide incomplete protection are not necessarily evolutionary dead ends, and we would do well to explore why our adoption curve seems to follow what is hot as opposed to what is proven, at least within certain bounds. In the process of writing this paper, we have identified many papers on resilience and related topics, yet when looking at real world systems, the adoption of these techniques is very low. Where we have used technology to stave off disaster, we are often trading availability or integrity for con fidentiality. Solutions that provide more resiliency seem to be economically impractical. Our sense is that truly resilient computer systems are possible, but will not be adopted any time soon for pragmatic purposes, despite the high value assets computers control. History speaks pretty loudly about our actual desire for security versus our hunger for functionality (even for purely cosmetic features), and the stochastic nature of a resilient system does not bode well for its adoption. Quite possibly, it is this economic hurdle which is preventing progress, not a technical one. Overall, there are certain properties that a system should possess

in order to be considered resilient. It seems likely that redundancy is key that is, that the failure of any discrete component should not cause systemic failure. In addition, the ways in which information is stored, accessed, modified, and transferred will all need to be carefully crafted so that a single failure or manipulation does not cause downstream consequences that are detrimental to the system as a whole or that allow for exploitation/modification of information. These methods are unlikely to look like traditional computer systems; instead, they are likely to appear less predictable at the component level, and have properties that are emergent rather than implicit. Data is unlikely to exist in just one spot, and different parts of the system will have to collaborate to decide what the ground truth actually is. Such work will be challenging, and lack of meaningful metrics will make comparison of approaches difficult. However, just because it is hard does not mean it is not worthwhile.

2.3 CIA and Big Data file Systems

Big data deals with massively large data sets that need to be transported, stored and processed. Sheer size of big data sets precludes the use of conventional hard disk storage devices, whose size is typically limited to just a few Tera bytes. Even if Peta byte single storage devices were to become available, such solutions will be plagued by the single point of failure phenomenon. Moreover, since computations have to operate on massive data sets to extract actionable intelligence, storage system must also support concurrent computations. File systems, such as the Hadoop [17] and the Google File System (GFS) [18] have been designed to meet the requirements mentioned above. Both these file systems follow a similar architectural concept designed around the use tens or hundreds of commercial-off-the-shelf (COTS) hard disk drives that are interconnected via high speed network links. Furthermore, these architectures incorporate high degree redundancy and replication of data blocks to mitigate single of point of failure problems and to support concurrent processing multiple data blocks. Data driven decisions derived from big data have assumed critical importance in many application domains, e.g., helth, commerce, finance, marketing, military, etc. For these types of applications, data has become a highly valued resource, requiring appropriate

security guarantees. High value associated with big data sets has also rendered big data storage systems attractive targets for cyber attackers. These attackers are constantly exploring new ways to detect and exploit vulnerabilities in a cyber infrastructure, including big data storage systems. A cyber attack seeks to compromise one or more of the following three basic security attributes:

- Conf identiality (C): Ability to ensure privacy by preventing theft of confidential and proprietary data;
- Integrity (I): Ability to prevent unauthorized alteration of data;
- Availability (A): Ability to prevent denial of access to data by authorized users.

Data analytics involves collection, transportation, storage and processing of massive volumes of data or big data for delvering intelligent decisions. This has made data a valuable resource that needs to be protected from cyber attacks. As discussed earlier, high degree of redundancy employed in GFS and Hadoop can provide significant defense by tolerating only the Availability comprising attacks. One other notable commercial effort is called the SHadoop [19] and its focus is mostly on preventing attacks by combining strong authentication and the SCALA programming language for describing Map-Reduce [19] query processes. However, on numerous occasions attackers have been successful in defeating even the strongest preventive methods, requiring subsequent time-intensive malware scans, detection and recovery from attacks. Therefore, defensive cyber security strategy, at best is costly, and at worst may not be acceptable for time critical data driven decision making applications, e.g., health care, high speed trading, military operation, homeland security intelligence operations, etc. We argue that the alternative strategy of incorporating intrusion tolerance in an architecture is more cost effective in the long run and is essential time critical applications. Big data is the basic raw material that is to be stored and used by data analytic engines and high value decision support systems. Therefore, security of such data in terms of confidentiality, integrity and timely availability has become a critical issue. Hadoop and GFS are the two most commonly deployed big data storage systems. High reliability and availability in the presence transient and

short duration failures resulting mainly from non-malicious events and software bugs were the dominating design criteria of these file systems. However, with ever increasing frequency of malicious attacks on information system, protection of confidentiality and integrity of data has become just as important. Almadahkah [20] have first shown that large scale naive redundancy employed in Hadoop and GFS designs leads to reduced protection against attacks designed to compromise confidentiality and integrity.He has addressed this drawback through smart redundancy based on the FCDR concept and have used the FCDR strategy to develop the AT-NFS architecture. Then he shows that this architecture, in addition to providing proactive and intrinsic attack tolerance capabilities, also leads to simultaneous reduction in Conf identiality, Integrity and Availability failure probabilities. It is also shown that these failure probabilities are a monotonically decreasing functions of the degree of redundancy.

2.3.1 Big Data In computer Cyber Security Systems

The great opportunity that big data presents for the enterprises by tapping into varieties and volumes of data ,Scientists ,product managers ,marketers , executives , and others can take benefit from informing plans and decisions , discover new chances for optimization, and deliver breakthrough innovations. Without the right security and encryption solutions the big data could be really big problem. In spite of the applications of big data analytics to security problems has significant promise, we have to mention some challenges:

- First challenge is the Privacy: advance in big data analytics brought us tools extract and correlate data, that would make data violation much easier.Furthermore it makes developing the big data applications a must without forgetting the needs of privacy principles and recommendations . All the activities produced in communications commission works like (telecommunications companies, Health Accountability data, and any Federal trade commissions) have been broad in system coverage and mostly could cause interpretation. The large scale collection and storage of data would be attractive to many people especially (whom using this data for advertising and marketing). This is maily valid for government (finding this data neces-

sary for the national security or for low prosecution), and for law breakers (they would like to steal the identities).

- Second challenge, the veracity: it's difficult to be sure that each data meets the trustworthiness that our analysis algorithms require to produce the accurate results. Therefore, we need reconsider the authenticity and integrity of used data in out tools whom we can take advantages from adversarial machine learning and from strong statistics to identify and moderate the effects of unkindly inserted data.

- Third challenge, the volume: volume which means (storage). The amount of data created every day through internet is in the order of Exabyte. Thats make the capacity of hard disks nowadays in the range of terabytes. Its large enough and it will get larger in future. The traditional RDBMS tools will be unable to store or process such as big data in order to solve challenge. Compression technology might be a good choice to compress the data at rest and in memory.

- Forth challenge, Analysis: Analyzing the huge size of data and the different in structure because the generated data to several types of online sites ,analysis the data may consume a lot of time and resources .defeating this, scaled out architectures could be used for processing the data in disseminated methods. Splitting data to small pieces and processing it in huge number of computers available during the network and the processed data is aggregated.

- Fifth challenge, limitations of traditional encryption approaches: However there are many of encryption offerings around, most of them engage in one specific aspect. The encryption in big data offerings not secure for the configurations information and also for the log files.

- Sixth challenge, Reporting: When huge amount of data are involved because the Traditional reports display of statistical data in the form of numbers. It would be hard to interpret by human beings. To get over this matter we need to represent the reports in a form that can be easily recognized by looking into them.

2.4 The Value of Trust in Pervasive Computing

The Pervasive Trust Foundation (PTF), is a model that involves Computer Security in Next Generation Networks [21], including the Future Internet. This reference model is based on the ISO OSI reference model, which among its 7 layers contains also the application layer. As a consequence, any distributed system can be seen as a network. Trust describes it as "the extent to which one party is willing to participate in a given action with a given partner in a given situation, considering the risks and incentives involved" [22]. This paradigm implies that truster (human or artificial) must decide whether to trust or not other (human or artificial) entities, which are called trustees. In this approach human factor is not in the center of the security system. This approach proposes a security model based on ISO OSI and the user can just decide to trust or not [23].

As said before, the application of traditional security paradigm to Cloud Computing and to other emerging technologies is not enough. We need a new approach in which the human factor is central and the Information Security Management System (ISMS) must be able to adapt itself to the scenario to protect. Under this perspective is essential for a Security Leadership to understand that the complexities and capabilities of technical solutions have to be integrated by involving the users. Figure 2.1 shows a schematic representation of this particular approach.

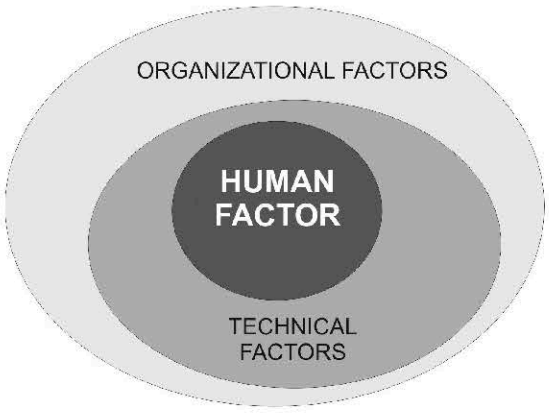

Figure 2.1: The relevance of Human factors compared with organizational and technical factors.

In our opinion, the human factor is the main element around which to set up

a dynamic model. The organizational and technical factors are still important, but alone they can not ensure an effective and efficient security system.

The recent experience of attack teaches that even if using all the available technological and organizational means, we remain still vulnerable. Everything changes so quickly that the security organization needs to adapt continuously to the internal organization and to external environment. A valid hint to design a good ISMS could be to start from some general factors adapting these to the organization. Some possible pillars on which base our security system could be the follows:

- awareness of users about security matters and participation to the organization problems;
- information technology used;
- capability of organization to receive policy;
- awareness of top management, etc..

What is important in our model is the capability to adapt constantly to internal end external changes through a deep sharing of objectives with users and leadership. In this model, consumerization could be a good starting point, and, data-centric security approach, is ideally suited to the challenges of accelerated data flows precipitated by cloud computing and virtual machine data storms. This approach also supports consumerization, extending data protection to the multitude of mobile devices now used by employees, giving customers back control over their data, wherever they resides. Even a pervasive computing system that strives to be minimally intrusive has to be context-aware. In other words, it must be cognizant of its users state and surroundings, and must modify its behavior based on this information [24].

The development of modern technology and their application to the totality of the objects which every day people interact with, obliges to find new ways in designing Security within an organization. One of main point to keep in mind is, above all, the importance of the human factor that is crucial for every security system. Recent security breaches, in fact, showed that every attack begins with

the involvement of user and continues with exploiting technology bugs. In almost all cases, without human collaboration, conscious and unconscious, it is really difficult to reach the criminal goal. The approach that we applied that have mainly three characteristics:

- centrality of the human factor;
- the ability to mold to the scenario to be protected;
- dynamic adaptation to external and internal threats.

However, we will later identify a set of attributes usefull for the construction of a security system fitting to a given context, going beyond the strategy of the pre-established paradigms (CIA and so on).

Chapter 3

Hypothesis of an adaptable model based on consumerization

"A proof is whatever convinces me."

— Shimon Even, *1935-2004*

3.1 Introduction

In a previous paper [12] we presented the human factor as the main element around which set up a dynamic model. The organizational and technical factors are still important, but alone they can not ensure an effective and efficient security system. We saw that applying traditional security paradigms to cloud computing or to other emerging technologies is not enough. Therefore, we concluded that we need a new approach in which the human factor is central.

Under this perspective it is crucial that:

- the Information Security Management System (ISMS) is able to adapt itself to the scenario;
- leadership understanding the complexities and capabilities of technical solutions that have to be integrated with the involvement of the users.

In this paper we intend to fully investigate how support the technical solutions, taking into consideration the net-centric position of human factor and the preeminent rule of Societal Digital Security Culture (SDSC) with regard to Digital Security Culture (DSC) [25] [26]. The measure that affect the SDSC, in fact, have much stronger impact on enhancing the security readiness because of the individuals tendency to imitate each other's behaviors and due to the major strength of the efforts at societal level. In order to improve the SDSC, we are aware of the importance of enhancing the trust and co-partnership of the people towards the ISMS even national and private, drawing the attention on the importance of security measures as an economic fly-wheel and to protect the common privacy rights.

3.2 Hypothesis of an Adaptable Model Based on Consumerization

We have learned that everything changes rapidly and that the security organizations needs to adapt themselves continuously to the internal and to external environment. Under this perspective some pillars on which base a security system are:

- awareness of users about security matters and their participation to the organization's problems;
- information technology adopted;
- capability of organization to accept policy;
- awareness of top management.

It is important to preserve the capability to adapt constantly to internal end external changes through a deep sharing of objectives with users and leadership. The basic model was based on consumerization as a starting point and data-centric security approach suited to the challenges of accelerated data flows due to

the introduction of cloud computing paradigm and virtual machine data storms. This approach extends data protection to the multitude of mobile devices now used by employees, giving back customers control over their data, wherever they reside. The main idea was to generate a sort of trust and co-partnership between customers and security organizations in order to enhance the awareness transforming users into stakeholders. As we point out in a previous papers about security paradigm in ubiquitous computing [12], even a pervasive computing system that strives to be minimally intrusive has to be context-aware. In other words, it must be cognizant of its user's state and surroundings, and must modify its behavior based on this information [24]. Figure 3.1 synthesizes a schematic representation of this particular approach [12].

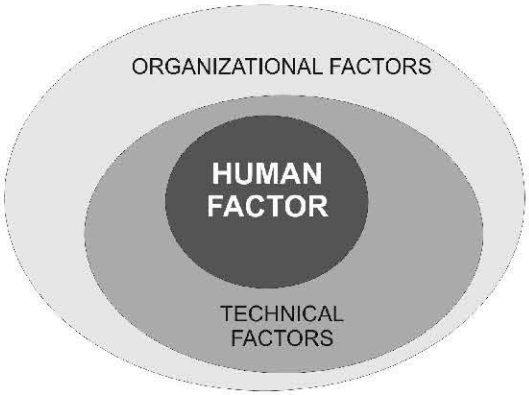

Figure 3.1: The relevance of human factors compared with organizational and technical factors

3.3 Overview on Trust and Co-partnership in Societal Digital Security Culture

3.3.1 Trust in Security Environment

Trust is set up on a rational component, based on information built on experience and an irrational element, a so-called "leap of faith" made out of pure instinct, without any logic: it is the emotional and intuitive interface that often guide our actions. It represents a fundamental link between past, present and future that

leverages expertise to build the future. That is one of the top reasons that create "engagement" in interpersonal relationships or group based on trust creates value: the trust must be seen as an investment that generates relational efficiency ratio, speeding work, making certain implicit elements of judgment, information about skills, knowledge do not require reconfirmation. Not only that, but trust speeds up the decision-making process as it lowers the threshold uncertainty: confidence on the reliability of the partner lowers the risk [27].

Trust and risk, in fact, are two inseparable concepts whose binding is supported by rational and irrational character of confidence. The problem is that the information considered "perfect", that would lead to the annulment of risk, does not exist. In the organizational relationships, as well as in today's society, the trust in the "organization" is the result of a mix of rationality and irrationality as intuition and logic that make a person a unique talent and a leader. Not only that, but trust being based on reciprocity creates value in the construction of process effectiveness strengthening the "commitment" in interpersonal relations: the opening of confidence becomes the current social currency of organizational relationships. This character is of utmost importance if we consider the development of team-work and the collaborative processes that pervade the new models of work: the relationship of trust generates cooperation, and thus opens the door to the development of ideas, innovation and overcoming diversity.

The trust also generates communication: it is true that communication creates trust, but it is also true that confidence leads to better communication: relevant, timely, and reliable. It is clear that all these aspects lead us to the topic of employment brand. The attraction of talent and their involvement as a fact generates confidence identification and then a sense of belonging. In addition, it leads to sharing values which are fundamental to the definition of organizational culture: the behavior and attitudes of people also result from such sharing. Trust, therefore, becomes not only a social glue inside, but, spreading virally, develops a chain of relationships of trust within the organization and outside, by the employee to the consumer, all stakeholders. In Fig. 3.2 has been reported a scheme that sums up this concept.

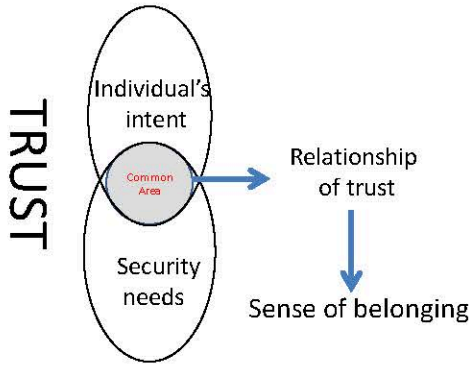

Figure 3.2: Schematic representation of the trust

3.3.2 Co-partnership in Security Environment

In the last years the way of managing risk analysis has changed due to the impact of pervasiveness of computing in our society. Today the main problem is to find out a correct approach to risk management so that considering this holistic and, at same time, adequately in support of the internal working relationship as well as of relationships between organizations. In fact, the way to handle a cyber-event rather a cyber-attack changes whether the managers operate on an individual base's decision-making or engage in a collectivist decision-making approach. The capability of the security manager to have firmer appreciation of how mitigate the risk is a main requirement to defend both from internal sources (insider threats [28],[29],[30]) and external environment (organized crime groups, stated sponsored organizations involved in computer hacking activities and so on). Another aspect to take into consideration is that managing risks involve both technology and human activities developing a significant risk assessment and analysis methodology. All these aspects allow the security manager to better explain the perceived risk as well as the way in which the top-management deal with it. For these reasons we are forced to change the way of rising security awareness within organizations and, most importantly, to endorse more widely the model of organizational learning [31].

3.3.3 Information Sharing and Organizational Learning

The organizational learning concept can be employed to provide an holistic approach to training and provide a foundation from which a project liaison team management structure can be built [32]. This being the case, a cyber-security culture can be developed to:

- strengthens security awareness;
- influences the organizational value system and the value system of partner organizations;
- encourages managers to be pro-active.

The managers can greatly improve a pertinent cyber-security systems leading their own the organization and letting this become more resilient than present. Sharing information and deploying the organizational learning concept are the main means through improving organizational communication, group work and planning. The advantage of this is that the main organizational stakeholders will be better informed about the possible risks and will also be more conscious of the need to engage and respond to messages in relation to the communication of risk. A well-crafted risk communication strategy takes informed the partner organizations about the state of affairs and the action being taken to resolve the situation. The transparency of communication is prominent for tackling a cyber-attacks in real time and put in practice a successful defensive strategy. Transparency and co-partnership are particularly important when building trust within and between organizations, and should be considered vital for the success [33]. The escalation in different forms of social engineering has resulted in various cyber-security attack vectors being exploited and as a consequence management need to pay more attention to the behavioral factors of those orchestrating such attacks and employees who may be susceptible to falling victim to this kind of manipulation. Although some corporations have implemented policies that govern the use of BYOD (Bring Your Own Device) at work and have required that employees enter into formal contractual agreements related to the use and to the storing of sensitive data and information, a lot of things have to be done as soon as possi-

ble. Preparing staff to deal adequately with both current (known) and unknown (future) cyber-attacks is something that requires stronger attention.

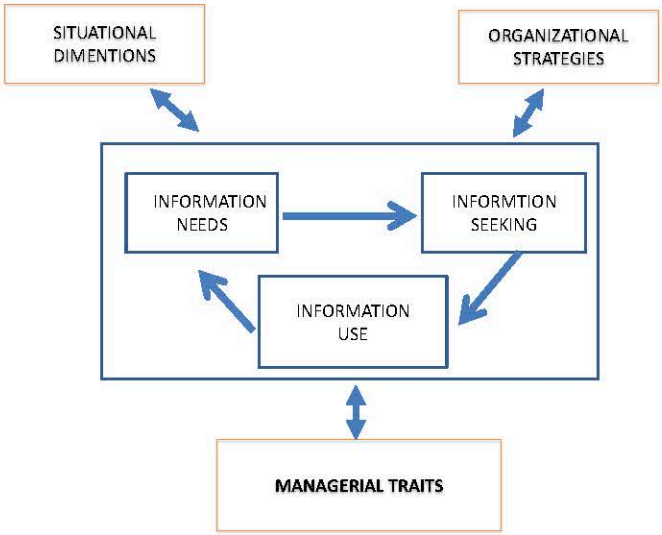

Figure 3.3: A conceptual framework for environmental scanning [1]

Bearing the above points in mind, we can return to the topic of risk. For example, it is necessary to develop knowledge and working practices that take into account the different ways in which organizational risk is assessed and also, how to link more firmly, emerging bodies of knowledge such as strategic marketing, corporate intelligence with corporate security. By doing so, it is possible that managers within organizations will commit more fully with their counterparts in partner organizations, and in the process develop a joint security approach that views security as a core activity across the partnership arrangement. Security of society and citizens, from the standpoint of the State-centric approach, is being observed in relation to the level of State security, based on the premise that people are safe if State is secured, and the level of their protection depends on the level of State protection, from which arises personal sense of citizens security [34].

3.4 Trust and Co-partnership Model in Societal Digital Security Culture

If this approach is correct, then it implies that technology solutions, alone, to ensure security are completely inadequate. Social, organizational and psychological factors must be considered when implementing security within an organization. We will have to consider how people build communities. We will have to take into consideration how communication patterns affect interactions.

3.4.1 Basic Model of Human Factors and Information Security

The use of models is particularly effective in IT field. In fact, the model creation allows us to define what is important to the domain in which we are working, abstracting from reality. As yet, no model of organizational security has arisen, nor a model of information systems security. Hassell et al. [2] propose a preliminary model of organizational security (of which information systems security is a part). Next, they propose a model of user security behavior. The rational choice model is more suitable to understanding information systems security. Under this model, people are to a greater or lesser extent guided by a rational tradeoff between the probability of the success of a behavior and the desirability of the involved choices [35].

Despite all of this is important, we must not forget that people act rationally and that not only the emotional part has a great importance in behavior. Consequently, the social systems are open, dynamic and composed of many elements that are not rational [36]. These elements should be taken into consideration when it comes to patterns of human interaction, including, perhaps most importantly, security issues.

Figure 3.4 shows the model of organizational security that best fit our needs. A number of elements must be highlighted. Management Support is the *sine qua non* for any successful business endeavor. Therefore, it influences both IT and user security behaviors. On the other hand, External Business Factors, such as business competition and product development are difficult to predict, but

Hassell et al. remain sensitive to their possibility to influence the Organizational Security. IT Factors and User Security Behavior are important and influential as well. We may assume that External Business Factors affect User Behavior insofar as they affect the business environment to which the user responds. Technology, obviously, influences IT. In an ideal world, there would be no technological innovations that were not addressed by IT. Physical Security affects information systems security but seems to be more addressed in professional conferences and magazines than in the academic sphere. External Global Factors, like cyber terrorism, all have an impact on Organizational Information Systems Security. The external business factors that influence users' behavior should affect the business environment.

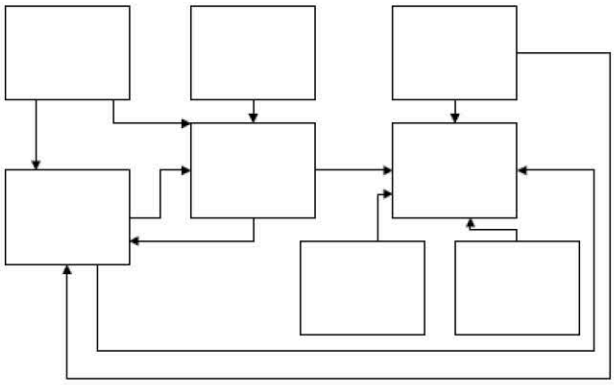

Figure 3.4: Model of organizational security [2]

Figure 3.5 depicts the characteristics presented by Hassell et al. that we need to study in both the end-user arena and in the IT arena. If their value, knowledge and commitment to the organization are not taken into consideration when placing all technological innovation, certainly will lead to problems. Personal values are as important as ever, for both the end-user and IT staff personnel. Both must have a collaborative work ethic, be team players, and have the awareness of the importance of other people. Here the value of co-partnership is clearly tangible. But what an individual views as common sense has to do with personal values and socialization. Let us adopt that most of what is written about technology

falls outside what we are referring to as IT Factors.

Apart the technical capability of the IT staff, then, the topic that is most often written about this regard is training. Making users aware of security mechanisms, according to this reasoning, is what we need to do to get users to comply with security procedures. The correlation between education and increased security has yet to be established experimentally. Schultz [37] calls for expanding the research into field of security training, pointing out the attention on skills and training. The principle of this sort of training is that all parties involved have some common ground or rather they share values, rules, and underlying knowledge.

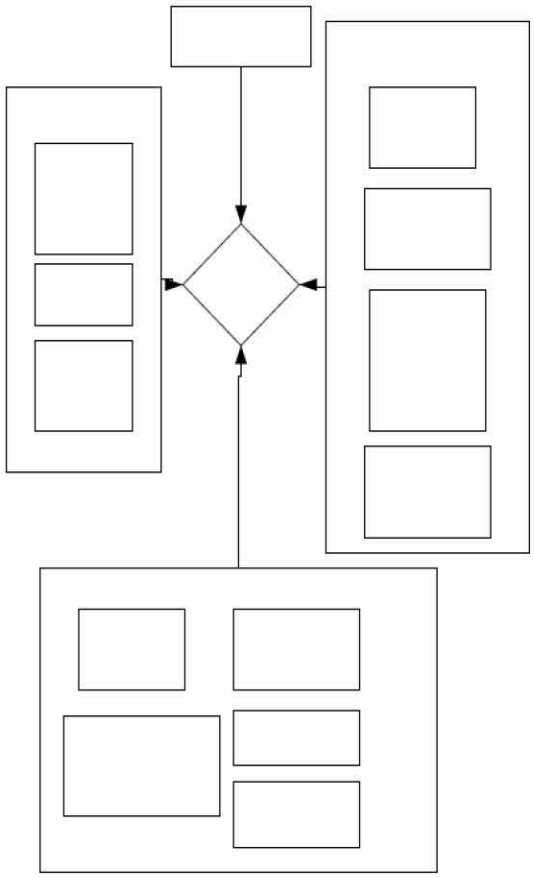

Figure 3.5: Model of user security behavior [2]

There is no doubt, therefore, that this form of education and culture transcend the IT department, something that is often lost on the IT staff. Considering what Doughty [38] says, an organization's culture is often imprinted not only into the

management practices (i.e., policy, procedures and directives) but also on its personnel, particularly if the personnel involved in system development, project and operational management have been long-term employees of the business. Rightly, this is not the case. The unit IT organization does not deal with the culture of the organization as a whole, and therefore its members are seen as outsiders.

The general reputation of the IT department within the organization is not considered safe. Safety is something holistic. When it comes to reputation, we go beyond the competence and dedication to their work. We are talking about the whole system. Probably does not deserve the bad rap it becomes [39]. On the other hand, it seems true that it has a bad reputation within organizations. Many anecdotes attest to the general lack of esteem on the IT groups within organizations. The fact that we tend deal with superficiality the issues regarding the of IT personnel in organizations has been shown in studies in which the success or failure of strategic information systems is determined by IT personnel and not "common" users [40].

3.5 Toward an Integrated Societal Digital Security Culture Approach

Since end-users are human beings, as well as the IT staff are, there is not so much difference between the human factors of the two. The only obvious difference is that with the end-users is the strength of the culture and values of the organization that is significant. An important question is how and to what extent the corporate culture and values are integrated. This question arises from the need of making distinctions. If the culture and/or organizational values are weak, then there will be more and more difficulties to force users to follow any organizational mandate. They will not be inclined to be team players. On the other hand, if the members of it are not identified in the first place with the organization, then you will not immediately trust and their ability to effect change will be decreased. Back then, the issue of trust is an element that holds the whole system. It must be recognized that influences and is influenced by Business Security home security system. In

this context, we have already addressed this issue in a previous paper showing how the model can be consumerization be a good starting point.

Hassell et al., in their paper show how an organization linked to a server machine at home via a VPN is just as secure as your home computer is. If the user is negligent at home by not considering safety/security best practices, then the home IT system, and as a result of the organization's server, can be compromised. This simple, yet powerful, fact is often ignored in discussions of corporate security, although not by the Computer Emergency Readiness Team (CERT). We do not directly included in our model since human being, at last, can be found in the behavior of people when working with the computer at work and at home [2] and it is also reflected into the network [41].

It is interesting, therefore, to note that the major impact areas of research potential models are not represented by nodes but the edges that connect the nodes. These nodes represent the "how" of the interaction of factors. And it is here that the equation becomes more complex, because the weights assigned to the various factors and their influence on the final equation, are taken into account. It seems that the factors are not simply additive but interact in multiplicative ways. Let us see the interface between the values held by the IT staff and organizational values held by the population of users, such as the area of a possible common ground for both parties. This intersection of values will also have an impact on what each view as common sense. Building this common ground is closely linked to the concept of diffusion of innovation, because only insiders who may be opinion leaders, change agents and change helpers. And where traditionally struggled, and security has remained strangely silent, is the creation of this type of partner for change among the population for the end-user. Research in other areas has outlined the possible roles of a change agent. Depending on your organization and the context, change agents can act as one or more of the following: enablers, catalysts, solution givers, helpers of the process, stimulator-innovators, resource linker, brokers, guardians, socio-interactions and supporters. Detailing the specifics of each role is alien to the purposes of this document. Suffice it to say that these roles must be taken by end-users, but must be supplied by IT. IT must recruit respected members of the community of end-users who are well-known, easy social interaction and fun. They must then provide them with the

knowledge and tools to make them supporters of successful information security. One should not think, however, that this eliminates the need for close alignment of values of IT staff with those of the rest of the organization. Nothing could be so far from the truth. Close alignment is crucial in order to recruit agents of change for the end-user to begin with [2].

Chapter 4

Integrated Societal Digital Security Culture Approach

"Defining [the] influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects"

— Joint Publication 3-13, Information Operations

4.1 Introduction

The basic idea that members of the Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions, have lead us toward a integrated model based on a cultural approach in which the trust and co-partnership of the security system are the main focal point. This model implies that technology solutions separated from the surrounding environment are completely inadequate. Social, organizational, and psychological factors have to be considered when implementing security within an organization. A valid complement (usable) to technical solutions has been found in a SDSC as a set of collective knowledge, common practices, and intuitive common behavior about digital security that the members of a Society share. The above consideration

Figure 4.1: Integrated Societal Digital Security Culture approach

guided us at the model adopted in this paper. Such a model includes the cultural approach where both trust and co-partnership of a security system have a very important role. Security behaviors fostered by information organizations must be achieved by pursuing the motivation and desire as cultural factors. Figure 4.1 synthesizes all these elements. We wont start from this above model considers the societal elements as the most important part of the security system. Trust, co-partnership help to create a strong security culture that serves as a framework to the information security system. All these aspects are part of our work [13] [42] in which the interaction between social and technical factor will be fully analyzed.

4.2 The case of Industrial Control System: Cyber Threats Indicators in Smart Grid Technology

Critical infrastructures, in particular those relating to the production of electricity, telecommunications, computing infrastructure and transportation converge more and more each other, leading to an increase of the interdependencies among them. These dependencies, especially between the electricity and communications infrastructure IT [43],[44],[45] in recent years, have given rise to numerous specific studies on risk analysis aimed at verifying the cascade Studies show that the interdependence between the major infrastructures of a Country and, in particular, the growing integration of electrical networks with the Internet, involving a significant systemic risk of apower outage. If it is true that we use Internet connections for control and communications in the electricity sector, it is also true that the functioning of the entire infrastructure of the Internet depends on the same electricity network, whose reserves are increasingly limited. However, apart from these considerations, for a complete discussion of the risks associated with the use of new technologies, it is necessary to take into account the extent of cooperation models, that see a number of actors (ISPs, outsourced services, etc.) and are at the base of the ambiguity of *who* is the control and govern the interdependencies between infrastructures. Moreover, the same cyber threats are generated at the intersection/interaction of different components, wrapped of dubious origin whose risks are difficult to estimate. To observe, however, that we can not disregard the fact that the realization of a intelligent' network (for that reason they call "smart" grid) requires a high level of connectivity to overcome the islands of automation that are created. To a large extent this connectivity is achieved by the IP protocol to facilitate real-time delivery of data via a two-way communication (that is essential for the smart grid) and allow the use of the Internet infrastructure already existing. This, in turn, brings further advantages in the reliability and functionality of a typical dynamic routing. The use of IP networks, however, not only brings advantages, as we can imagine. The fact of being, in fact, an open standard implies a high risk of cyber attacks, such

as Denial-of-Service (DOS) or strong vulnerability exploits (0-days), botnet [46], viruses or worms [47].

The physical presence of the risks linked to the Internet depends, too, on the specific implementations of security levels associated with the use of the IP connections and the specific adopted protection measures (such as encryption, access control, authentication, etc.).

In essence, what makes the use of IP networks a systemic risk factor is the widespread knowledge of his vulnerability, which also carry the large-scale exploitation. This is also true for the massive use in the field of hardware and software such as commercial-off-the-shelf (COTS) ones, including operating systems, or solutions available in the market to be purchased from companies interested in developing and to use them in their projects, instead of fully customized solutions.

This is a common trend in the electricity sector. Let us take the example of "smart meters" that use the IP protocol. These large-scale distributed sensors involve the risk that malicious hackers can, for example, turn them off all at once, creating a ripple effect with effects on the level of distribution of them. In addition, the infrastructure based on smart grid using ICT applications already existing in the electricity sector, the so-called "legacy systems" with their inherent vulnerabilities that pose a systemic risk to increase the entire infrastructure.

The mixture barely visible legacy ICT systems and use of technology "SMART GRID" implies an inherent difficulty in appreciating the foreseeable risks in the light of a large part of the ICT components from third parties and not controllable.

What has been said, it is also particularly relevant in the case of software updates when new versions of legacy systems are often the reason for IT incidents related to critical infrastructures.

Another source of systemic risk can be seen in the huge amount of sensitive data transferred via the smart grid, i.e., data relating to equipment for monitoring and control or administrative data and personal information, such as billing information or data controllers construction. Such transfers of data must be encrypted to ensure a basic level of safety and security. However, the high costs of maintaining a cryptographic infrastructure an the limited capacity of the adopted hardware do not allow, often, a high-performance encryption process that adversely affects the achievement of adequate protection goals. Futhermore, Smart

grid uses intelligent transmission and distribution network to delivery electricity, improving electric systems reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning. The smart grid technology is the next step in the evolution of energy distribution, by combining power system and IT communication system domains. Upgrading the electrical grid reduces greenhouse gas emissions, increases integration of alternative energy and electric cars into the electric grid, and allows consumers to actively monitor and regulate their energy usage. The current electric grid was designed over a hundred years ago to serve a smaller population with a lower energy demand. Originally, the grid focused on providing power to small communities with local generation plants, which led to personalized power needs and delivery in each region. In the past, the typical household used low energy appliances such as lighting, radios, and televisions, a model distant from the current structure of energy demand. Today, the typical household includes power-intensive technology that requires large amounts of electricity. Envisioning the needs of a more energy-intensive consumer base, the concept of the smart grid was developed. The development of such technology is driven by the desire to renovate energy infrastructure to be proactive in meeting an ever increasing energy demand. The smart grid outperforms the traditional electric grid in the ability to rapidly pinpoint and remedy causes of power outages: Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, enable the utility to centrally monitor and control many of its processes. Through SCADA, operators can utilize advanced location information provided by Outage Management Systems (OMS), and Geographic Information Systems (GIS) Asset Management Systems, to pinpoint malfunctioning infrastructure components. But while smart grids have great potential to benefit energy suppliers and consumers, a careless implementation of the enabling technology has just as much potential to be abused. In a post-Stuxnet world, it can no longer be argued that such systems can be successfully air-gapped and thereby made completely secure. In 2009, said Raj Samani (Cloud Security Alliance) [48], a team of researchers had identified a number of programming errors on smart meter platforms, which allowed them to assume full system control of smart meters. Although this impacts only individual meters, other demonstrati-

ons have shown that one meter can be used to spread a worm between meters, that, in turn, could result in a power surge or a shutdown of the entire grid. Without knowing exactly what technology will be used or how it will be implemented, it is difficult to assess what the risks will be. In any project, financial concerns typically outweigh others, so there is a very real risk that standard smart metering devices and networking techniques and equipment will be used as far as possible to keep down costs. Security was rarely the driving force behind any program that sought to network significant resources and a broad user base, he said, but the UK must ensure that in moving to a smart grid, security was central to the systems design, not an afterthought. Sarb Sembhi, chair of the ISACA Security Advisor Group, pointed out that manufacturers tended to use software components that had not been developed with security in mind and tended to believe that as security was not their expertise, security should be implemented at a network level rather than built into the product.

4.2.1 Human and Organizational Implications

In a previous paper [12] we presented the human factor as the main element around which set up a dynamic model. The organizational and technical factors are still important, but alone they can not ensure an effective and efficient security system. We saw that applying traditional security paradigms to cloud computing or to other emerging technologies is not enough (even in case of smart grid security). Therefore, we concluded that we need a new approach in which the human factor is central.
Under this perspective it is crucial that:

- the Information Security Management System (ISMS) is able to adapt itself to the scenario;

- leadership understanding the complexities and capabilities of technical solutions that have to be integrated with the involvement of the users.

In light of this, we consider vital the support to technical solution taking into consideration the net-centric position of human factor and the preeminent rule of

Societal Digital Security Culture (SDSC) with regard to Digital Security Culture (DSC) [26].

The measure that affect the SDSC, in fact, have much stronger impact on enhancing the security readiness because of the individuals tendency to imitate each other's behaviors and due to the major strength of the efforts at societal level. In order to improve the SDSC, we are aware of the importance of enhancing the trust and co-partnership of the people towards the ISMS even national and private, drawing the attention on the importance of security measures as an economic fly-wheel and to protect the common privacy rights.

4.2.2 Integrated approach

In a smart grid infrastructure, the role of cybersecurity policy and system communication in conjunction with each other is vital for an effective security strategy.

The above consideration guided us at the model adopted in this paper. Such a model includes the cultural approach where facilitating communication, communication systems and human and organizational factors are merged together in an integrated model. Security behaviors fostered by information organizations must be achieved by pursuing the motivation and desire as cultural factors. Figure 4.2 synthesizes all these elements. This above model considers the societal elements as the most important part of the security system. Trust, co-partnership help to create a strong security culture that serves as a framework to the information security system. In conclusion, the security in the energy sector is one of the major emergencies that are occurring in the last few months. We can say, after this careful analysis, which "Internet of Things", the so-called global environment that encompasses all the functional components of contemporary society (such as energy, commodities, etc.) elated systems to communicate with each other, is opening a new front that also involves critical infrastructures such as smart grid. For those reasons, an integrated and appropriate strategy becomes a priority in order to counter new threats. It is therefore necessary to direct the efforts and take appropriate measures to protect and contrast both in terms of organization and strategically.

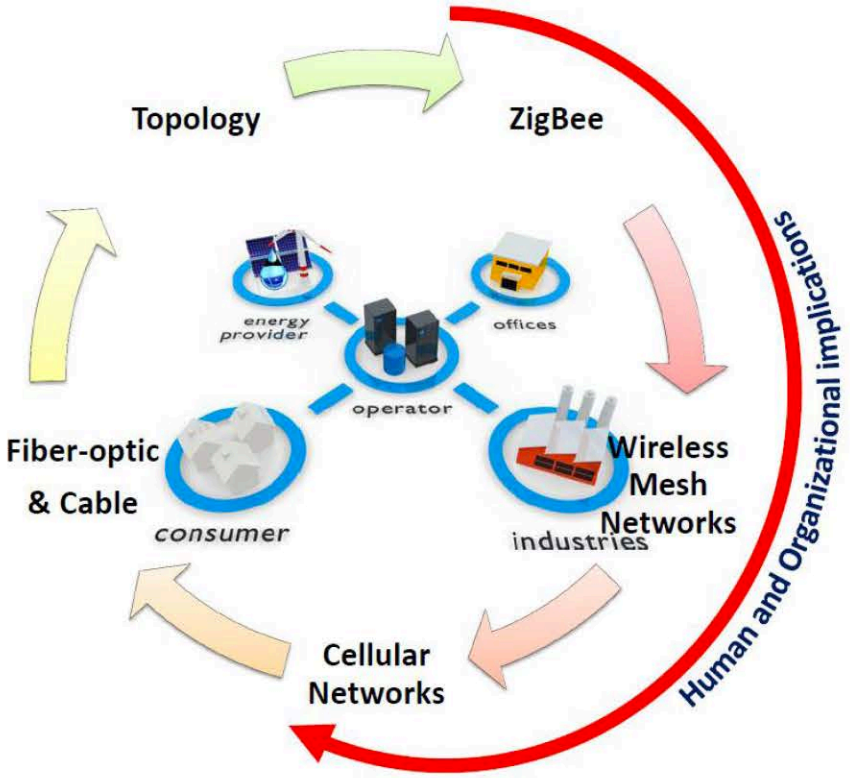

Figure 4.2: Smart Grid security integrated approach

4.3 The Role of Socio-organizational Factors

The increase reliance on information systems has created unprecedented challenges for organizations to protect their critical information from different security threats that have direct consequences on the corporate liability, loss of credibility, and monetary damage. As a result, the security of information has become critical in many organizations. the role of socio-organizational factors by drawing the insights from the organizational theory literature in the adoption of information security compliance in organizations. Based on the analysis of the survey data collected from 294 employees made by AlKalbani at all [49], we can see as management commitment, awareness and training, accountability, technology capability, technology compatibility, processes integration, and audit and monitoring have a significant positive impact on the adoption of information security

compliance in organizations. Several studies have investigated the problem of information security compliance in organizations in recent years. Herath and Rao [50], for example, investigate the factors related to behaviours, motivations, values and norms that affect employees intentions to comply with information security compliance in organizations. Siponen et al. [51] examine the factors related to normative beliefs, threat appraisal, self-efficacy, and visibility that influence employees intention to comply with information security policies in organizations. Ifinedo [52] assesses the social influence of changing individuals thoughts, actions, feelings, attitudes, and behaviours on information security compliance in organizations. These studies have focused primarily on understanding employees attitudes, and behaviour, Herath and Rao [50],on information security compliance in organizations. There are, however, other socio-organizational aspects that may influence the adoption of information security compliance in organizations. These aspects include information security governance, Smith and Jamieson [53], legislative requirements, Benabdallah et al. [54], information security strategies and policies, Smith and Jamieson [53], and implementation of advanced security technologies, Lambrinoudakis et al. [55]. This shows that there is a need to investigate more social-organizational factors for shaping the adoption of information security compliance in organizations, Bulgurcu et al. [56] e Dhillon and Backhouse [57]. It is important mainly to investigate the role of socio-organizational factors by drawing the insights from the organizational theory literature in the adoption of information security compliance in organizations.The results suggest that the adoption of information security compliance in organizations is influenced by the characteristics of technological and organizational contexts. This leads to the development of a conceptual model adopted by AlKalbani shown as in Figure 4.3 for the adoption of information security compliance for information security in organizations. The conceptual model hypotheses that technology capability, technology compatibility, management commitment, awareness and training, accountability, integration, and audit and monitoring will have a positive impact on the adoption of information security compliance in organizations at the organization level.

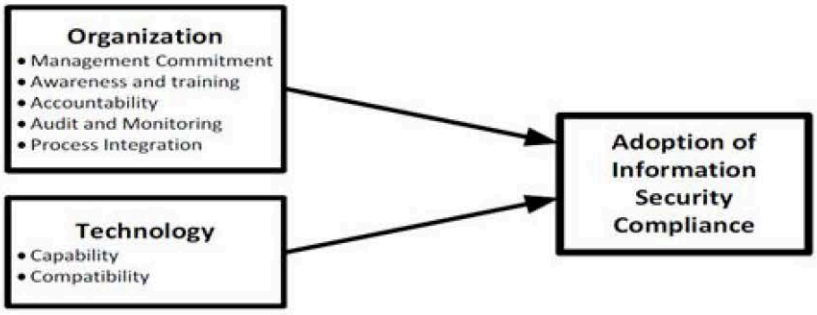

Figure 4.3: A research model

4.3.1 Hierarchical and Shared Key Assignment Schemes

This research contributes to the existing information security compliance literature in the following ways. First, the use of the TOE theory in this study extends the current understanding of information security compliance in terms of the value of socio-organizational aspects for information security compliance. Second, this study extends the current literature of information security compliance by investigating the factors at the organization level for adopting information security compliance, rather than predominantly focusing at the individual level using behavioral theories for changing employees attitude and behaviors towards information security compliance. Based on the exploratory factor analysis and the confirmatory factor analysis for the research model, seven factors are identified. These are management commitment, accountability, awareness and training, operational process integration, audit and monitoring, technology compatibility, technology capability. This result reveals that these socio-organizational factors at the organization level have high level of reliability and validity for the adoption of information security compliance in organizations. This offers valuable insights on how information security compliance could be adopted in organizations. Figure 4.4 presents the GOF strength for each single-factor model indicating a good fit between variables in the dataset, Hu and Bentler [58]. This research contributes to the existing information security compliance literature in the following ways. First, the use of the TOE theory in this study extends the current understanding

Factor	No. of Items	x/df <3	P >.05	CFI >.95	GFI >.95	AGFI >.80	SRMR <.09	RMSEA <.05	PCLOSE >.05
MangCom	4	0.655	0.519	1	0.998	0.989	0.0108	0.00	0.716
Accont	4	1.992	0.136	0.994	0.993	0.966	0.0211	0.058	0.330
AwarTra	3	0.014	0.907	1	1	1	0.0015	0.00	0.936
ProcInt	4	1.133	0.263	0.998	0.995	0.977	0.0198	0.034	0.489
AuditMoni	4	2.361	0.095	0.993	0.992	0.958	0.0196	0.068	0.263
TechCap	3	1.261	0.261	0.999	0.997	0.983	0.0111	0.030	0.419
TechCom	3	0.134	0.714	1	1	0.998	0.040	0.00	0.799

Figure 4.4: The GOF Results

of information security compliance in terms of the value of socio-organizational aspects for information security compliance. Second, this study extends the current literature of information security compliance by investigating the factors at the organization level for adopting information security compliance, rather than predominantly focusing at the individual level using behavioral theories for changing employees attitude and behaviors towards information security compliance. In conclusions we can assert that management commitment, accountability, awareness and training, process integration, audit and monitoring, technology capability, and technology compatibility, are significant factors for adopting information security compliance in organizations. These socio-organizational factors offer valuable insights at the organizational level on how information security compliance could be achieved in organizations. This suggests that for shaping the adoption of information security compliance in organizations, it is necessary to go beyond users attitude and behaviour.

4.4 Using Human Factors to Disrupt the Spearphishing Information Operation

Spearphishing yields information superiority to the APT attacker. The successful spearphishing attack gives the attacker access to information and can be used to disrupt the victims information processing systems. A defensive response that reduces the utility of email is a less devastating shift of information superiority

as the fear of spearphishing denies prospective victims the use of a very efficient means of disseminating information. NASA provides this model, Figure 4.5, of HF analysis [59]. The model depicts how people and systems interact, illustrating the flow of information between people and the machine components of the system. This Human Factors Interaction Model provides a different perspective of a spearphishing attack.

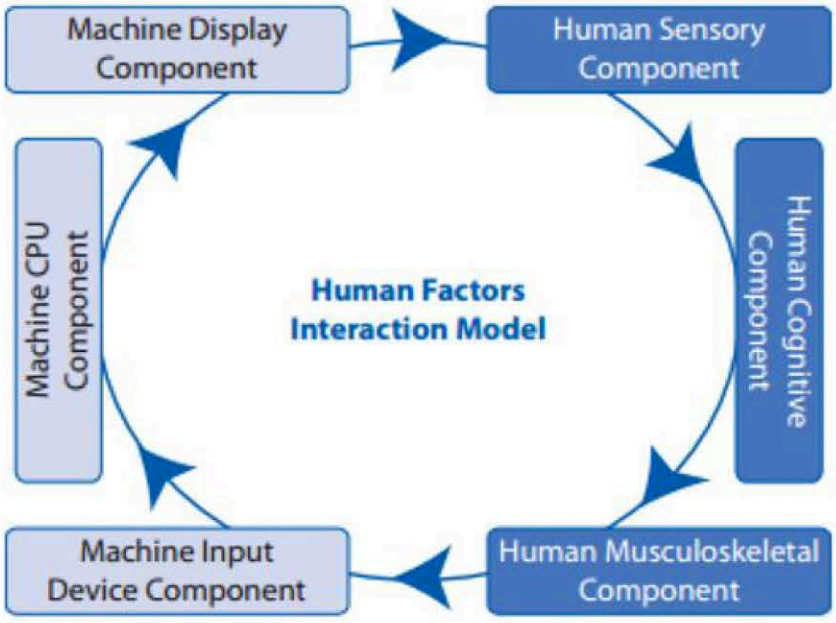

Figure 4.5: A research model

- Step 1. Machine CPU Component. The attackers deceptive email is received;
- Step 2. Machine Display Component. The deceptive email is displayed to the target audience;
- Step 3. Human Sensory Component. The target audience sees the deceptive email (See step of military deception);

- Step 4. Human Cognitive Component. The target audience is deceived in the information operation through the use of the cognitive factors discussed above (Think step of military deception);
- Step 5. Human Musculoskeletal Component. The user operates the keyboard according to the directions of the attacker (Do step of military deception);
- Step 6. Machine Input Device Component. The users keystrokes are converted to machine instructions that implement the attackers will.

In the spearphishing engagement, the attacker uses the HF tool of system, interface, and task design to engineer the HSI result of a compromised system. In response, none of the HF tools are being used effectively by the defenders. In order to take email back from the attackers, defenders must address the HSI factors that make email a malicious interface [60]. It is possible to leverage intelligence and existing email technologies to create an email interface which allows users to adopt new email processing habits which quickly and easily unmask attempts to infiltrate using stolen trust [61]. This simulated inbox demonstrates an inbox that provides differential marking of trusted senders. This interface uses the tools of:

- improved system, interface, and task design;
- procedure improvement to address the malicious interface issues of email.

The improved system, interface and task design tools are implemented in the modified interface which augments previously difficult to determine trust information with trust determinations from IT professionals, thereby simplifying the task of decoding email trustworthiness. The procedure improvement consists of placing ITs trust determinations in the users screen display, shifting the complex technical decisions from users to IT professionals. Instead of a vague admonition to avoid suspicious emails at the risk of your job or your freedom, the user is now provided with actionable warning intelligence that permits the intended victim to identify and report the attack rather than being tricked into compromising the system.

4.4.1 Integration of Humans

System learning based on self-learning and conversation requires a holistic integration of humans into the CPS. CPSs, like smart factories, are spread across physical and cyber environments. The two domains (physical and cyber) are represented by corresponding planes on the abstraction continuum. The physical domain correlates to the entity plane and encompasses all physical devices, communication media and physical signal passing. The cyber domain is realized on the relation plane as a kind of autopoietic network, which includes images, goals, decisions and their relationships to each other (Figure 4.6).

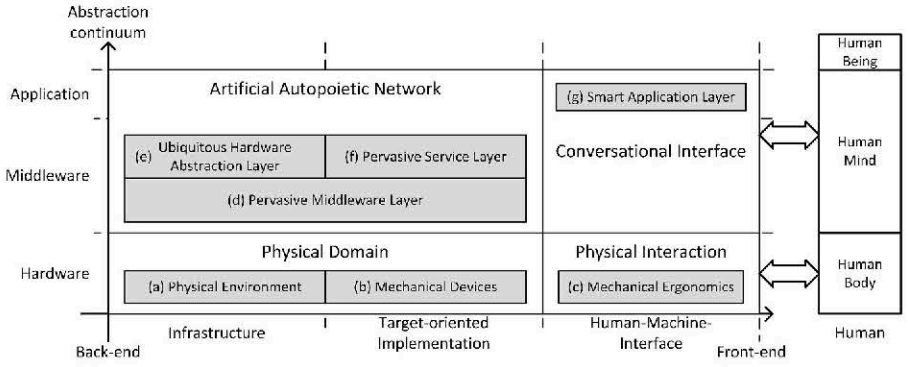

Figure 4.6: Integration of humans within CPSs.

The interface between a CPS and other enactive entities plays a central role in their integration. In the future this interface will also enable social cohesion between humans and machines. In study of B. Hadorn at al. [62] the interface between humans and smart machines is called the human-machine-interface (HMI). It separates the human from the machine interior and facilitates physical interaction and conversation between them. In the case of interaction within smart machines we would rather speak of machine-to-machine interfaces (M2MI). For simplicity, they use the term HMI, knowing that the counterpart of a smart machine may be a human or another smart machine. In classical systems an HMI encompasses some peripheral devices (screen, mouse and keyboard) and software implementing a graphical user interface (GUI). The HMI is much more extensive in smart machines. Any sensors and actuators which are in direct contact with human beings, belong to an HMI. Through the HMI each part of the CPS can

interact with the one corresponding to the human (Figure 4.6). On the entity plane,there's an interaction loop between physical devices and the human body. It expresses the concrete physical interaction between them. On the relation plane the conversation loop allows the CPS to share its subjectivity like images, goals and decisions, with the human. Conversation with humans can be realized through classical HMI components, like a touch screen. In such setups the screen can be seen as a "white board", where human and machine meet each other, visualize, manipulate and exchange their goals, models and ideas. A comprehensive conversation can be realized with the inclusion of each available sensor or actuator. This allows an entity (human or machine) to observe its opponent, to interpret their behavior and to react accordingly. For instance, if some of the results of a human-machine cooperation don't meet the requirements as anticipated, a conversation can be launched. The smart machine observes the instructions of a human operator, trying to understand and finally reproduce/reflect these instructions (or vice versa when humans learn from smart machines). In contrast to classical machine learning, where learning is limited to some selected topics and parameters, conversation allows humans and machines to build an adaptive learning organization, which is not limited to one topic. The conversation participants become designers of their collaboration.

Chapter 5

Risk analysis model base of human system integrations

"Risk analysis can cater to any sort of hazard, but their profession owes its existence to a relatively narrow band of possible dangers."
— Ian Hacking

5.1 Introduction

When considering digital networks as a space of conflict, traditional characteristics of conflict are overturned. Where in typical combat situations the defender has the advantage as they know the lay of the land and are able to set up adequate defenses ahead of time, the cyber attacker has the lead in digital realms. Attacks are easier to design, create, and launch from origins of the attackers choosing, while cyber defense efforts instead are challenged with predicting and detecting attacks while also attempting to develop new and effective defensive techniques. As a result, cyber defense is often very reactive in nature, where attackers set the pace in what becomes a chasing game. Furthermore, computational modeling informing organizational planning and execution relies on a fairly complete understanding of a domain, which is an unrealistic goal for cyber security wherein the problem space is so large [63] exploits can be automatically generated as to

be nearly impossible to predict or initially comprehend [64]. Cyber security risk assessment has been narrow in focus and based on a business risk assessment approach. However, given a defensive environment, cyber security risk needs to be more holistic, taking into account the user, information technology analyst, defender, and attacker. Cyber security risk assessment needs to consider the impacts well beyond the computers and network itself. To that end we have taken the 1996 Presidential Congressional Commission Framework for Risk Management [65] which incorporates standards from the environmental and human health risk assessment and framework and have applied those principles to the framing of cyber security risk assessment process. The adapted framework is as follows: context and problem formulation, system and human state assessment, threat assessment, characterization of risks posed to assets, agility options generated and decision-making process, action and agility, reassess state of system and humans, and finally determine where system is secure or additional security is needed. The successful implementation of this holistic cyber security risk assessment requires the development of measurement metrics for the information security attributes of confidentiality, integrity, and availability. A further challenge is determining what responses should be automated, and thus potentially subject to manipulation by attackers, and which decision-making remains fundamentally human. A behavioral component of the cyber security risk assessment accounts for the bounded rationality of human agents and for noisiness of the environment and decision-making process. In developing a holistic cyber security risk assessment, the Army Research Laboratory Cyber Security Collaborative Research Alliance (CSec CRA) aims to create a risk assessment framework that enables predictive and proactive defenses. The holistic assessment of cyber security risks is a complex multi-component and multilevel problem involving hardware, software, environmental, and human factors. As part of the on-going efforts to create this assessment model, the characterization of human factors, which includes human behavior, is needed to understand how the actions of users, defenders, and attackers affect cyber security risk. Trust and confidence are two similarly defined terms that are used to characterize the adherence to expected performance for hardware, software, and humans. Here we will focus primarily on trust given to defenders, but will also identify differences in characteristics between trust in

defenders, trust in users, and trust in attackers.

5.2 Trust versus confidence

To increase clarity in the nascent stages, the work group made by D. Henshela at al. [66] developing this new cyber security risk assessment model and framework within the CSec CRA has chosen to distinguish between trust and confidence by using "trust" only for human factors and "confidence" for all non-human factors (e.g. hardware and software). In this use of the terminology, then, there is confidence that a system or resource is functioning as expected, and there is trust placed in a person that they are performing their expected tasks and duties in a timely manner. Both confidence in nonhuman parameters and trust in humans can be considered as gradients.This gradient of trust is affected by perceptions of all involved parties. In a business network system, for example, the IT manager and analyst trusts the users to use and interact with the network safely, while the user trusts the defender to keep the system hardened and free of malware. Within a cyber defense team, different members of the team have to trust the other defenders to effectively, efficiently, and accurately conduct their work as a part of the defense team. Within the context of business and marketing, two of the main elements of trust focus on reputation and credibility [67], two key components of human trust. Characterizing the trust component of a holistic cyber security risk assessment allows for the incorporation of humans as positive and negative risk factors. Positive risk factors are factors that increase risk, while negative risk factors are factors that decrease risk. The degree to which a defender is a risk factor can be represented by the amount of trust given to the defender by superiors, the true intentions of the defender, and other inherent knowledgebased and behavioral characteristics. With respect to understanding humans as risk factors, it is difficult to paint a clear picture of the attacker beforehand, aside from the obvious fact that these humans present positive risk factors. A malicious user or foreign party is not going to make themselves known prior to an attack. Poorly designed policies that work counter to trusted workers goals [68], sparsely monitored systems that allow trusted users to circumvent established policies, or workers that are unaware of risks have the potential to create insider

threats. Insider threats are particularly insidious because most security concerns are focused on external threats. Thus, insiders are more likely to go unnoticed even after an attack has been detected; remaining unseen until the analysis of the successful intrusion is complete. In addition to malicious users–insiders or external–end users lack the ability to correctly evaluate potential risks. While this inability to correctly identify risk is modulated to some extent by the end users experience and perceived risk, the tools provided to users to inform their decisions are inadequate [69]. Moreover, users lack awareness of the information available to them, do not have the practical security experience, have been conditioned to accept information presented to them in a digital manner, and have an inflated trust in digital entities which drives them to override warnings [70]. As a result, it is best to assume and plan for the worst with regards to both attackers and end users. Defenders must assume that their enemies are at least as clever as they are and that end users in their system are, in general, vulnerabilities in order to prepare as best as possible. Therefore, the onus falls on the defenders to generate and maintain trust amongst themselves and with their users to push toward maximizing positive factors with minimal negatives. How teams within cyber defense roles accomplish this relies on a combination of the individual defenders skills, the communication of the team(s), and use of tools approaching an optimal result as best as possible. The nature of cyber defense work requires human agents to sift through vast quantities of data, implying a set (or sets) of qualifications necessary to warrant trust in a person as a capable defender who can understand and interpret the various information presented by systems and communicated among defense teams. In observing and conducting a cognitive task analysis of cyber network defense (CND) professionals across seven organizations, Whitley noted that while nuances and details differed, the overall missions and conduct overlapped and shared much in common. These analysts all had to sift through large amounts of data, drilling down from general information and alerts into the specific details of incidents and traffic in order to make judgment calls on what should be reported, what category or categories were relevant, and what actions were appropriate. Even assuming a level confidence (i.e. faith in the systems used) for all of the involved organizations, their observations highlight the relevance and importance of trusting these analysts

to use their tools effectively, leverage communication appropriately, and produce accurate and timely reports in order to support defensive efforts.

5.2.1 A trust framework

We have developed an initial framework for how to incorporate trust as a set of factors or parameters within a larger characterization of the human components (users, defenders and attackers) within cyber security risk (Figure 5.1). The goal of the trust framework is to enable a quantitative or semi-quantitative characterization of trust in the humans who interact with networks within a cyber security risk assessment model. Trust in the human factors is contributed by two main

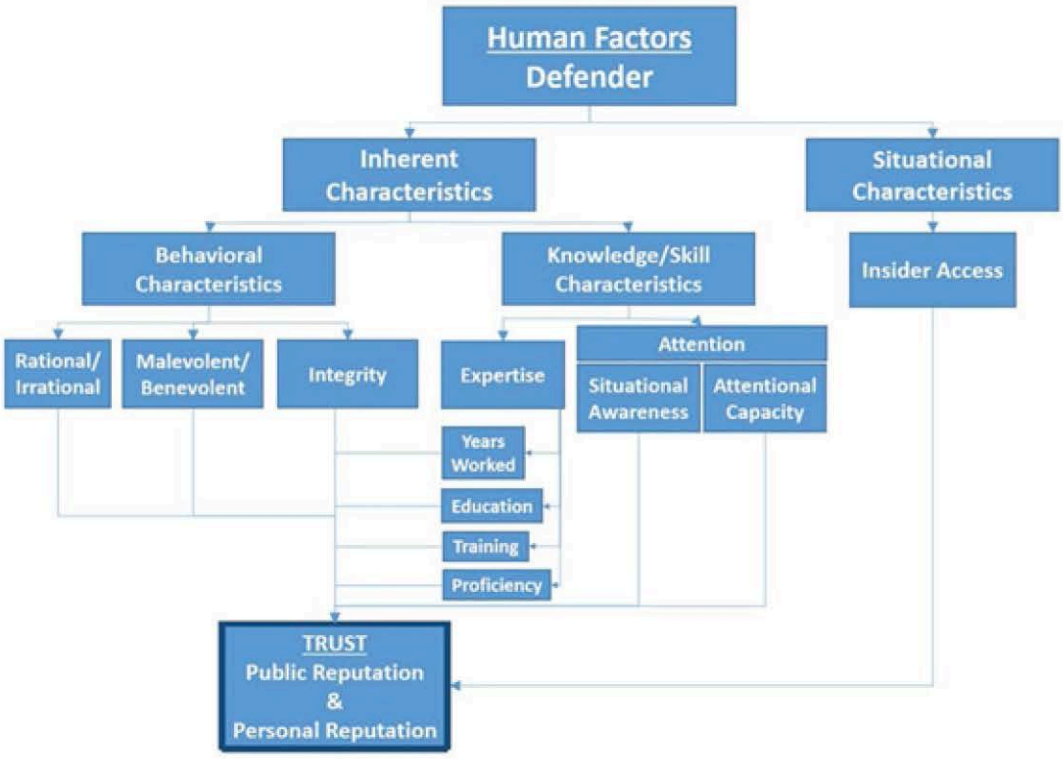

Figure 5.1: Defender/analyst trust framework

categories of factors: inherent characteristics, which are a part of the individual or given to the individual by the trust-giver, and situational characteristics, which are external to the individual. Inherent characteristics are further separated into

two categories: behavioral which captures rationality, benevolence/malevolence and integrity, and knowledgewhich captures expertise and attention-related factors. Situational characteristics capture the degree of insider access which is determined by access level determined by user policy, software, and hardware. Trust itself is captured by reputation, based on public reputation and personal interactions, which can be broken down into credibility, perceived honesty, and predictability.

5.2.2 Inherent characteristics

Inherent characteristics affecting trust include behavioral and knowledge characteristics. The behavioral characteristics include intention - expressed as a scale of benevolence to malevolence, rationality, and integrity, both of which affect predictability. The knowledge characteristics include both the expertise factors (reflecting experience, education and other training, and measures of proficiency) and attention, which is affected by and contributes back to expertise, particularly experience and training. The attention parameter incorporates both situational awareness and attentional capacity. All human characteristics can change in a given individual over time. They are affected by experience, and both internal and external factors, although people start from a different baseline for each behavioral characteristic. More rational people tend to behavior and respond more predictably which leads to increased trust. Rationality is affected by innate reasoning, ability, but is also affected by emotions and experiences, that is what is happening in ones life. For example most people behave more rationally when unstressed but can start to make more irrational decisions when highly stressed. Physical factors can also affected rationality. For example, hypoglycemia can cause people to behave irrationally. Malevolence implies evil or malicious intent. Malevolent behavior can be rational or irrational. An intent to harm can be driven by irrational emotions and can be induced transiently or for whatever period of time the inducing stressor exist. For example, seemingly rational, calm people who apparently have no intent to hurt other people can be taken over by an irrationally, malevolent intent that is typically called road rage. In intergroup conflict between self-identifying groups such as those defined by ethnic, political,

or religious characteristics, members can choose to harm other rationally if they see it as protecting or promoting their own group when they perceive their group is threatened by other [71]. Knowledge characteristics are those that change over time and contribute a great deal through experience to building credibility. Expertise characteristics include education, training, experience as partial quantified by years worked in performed related tasks, and are measured by metrics assess proficiency. Attention has two contributing components:

- situational awareness;
- attentional capacity.

Situational awareness is the extent to which a person perceives and understands the details and events occurring around them, and the ability to reason through the possible sequelae stemming from the known and possible dynamic changes. Attentional capacity is reflected by the length of time a person can maintain highly attentive state, and the amount of detail a person can track consistently for an extended period of time. While expertise is critical to the development of accurate and well-reasoned responses to a given situation, such as when an analyst is faced with indicators of malware threats, attention is more critical to being able to apply that information under the typically stressful, extended attack scenario. Whereas experience and training increase both situational awareness and attentional capacity there is some inherent reasoning capacity (baseline) that make some people inherently highly skilled and effective at situational awareness processing and or having extensive attentional capacity At the end, insider access is not authorized without initial trust and the trust must be maintained in order to gain additional insider access. The additional trust is gained by continued evidence of various characteristics of expertise, perceived benevolence, and perceived rationality. One problem with insider access, is that it is not always given (by policy, hardware, or software) but can be taken or forced by physical, hardware, software, or other invasive techniques. The increasing acceptance of Bring Your Own Device of course increases the potential for less control of access.

5.3 Use of the trust framework within cyber security risk assessment

Increased trust is given to a defender who can effectively communicate with superiors and other defenders, is able to accurately log incident reports (minimize the number of false positive and false negative reports), is able to provide and relay information in a timely manner, and is able to use cyber defense tools as intended with competency. In details, see Figure 5.2.

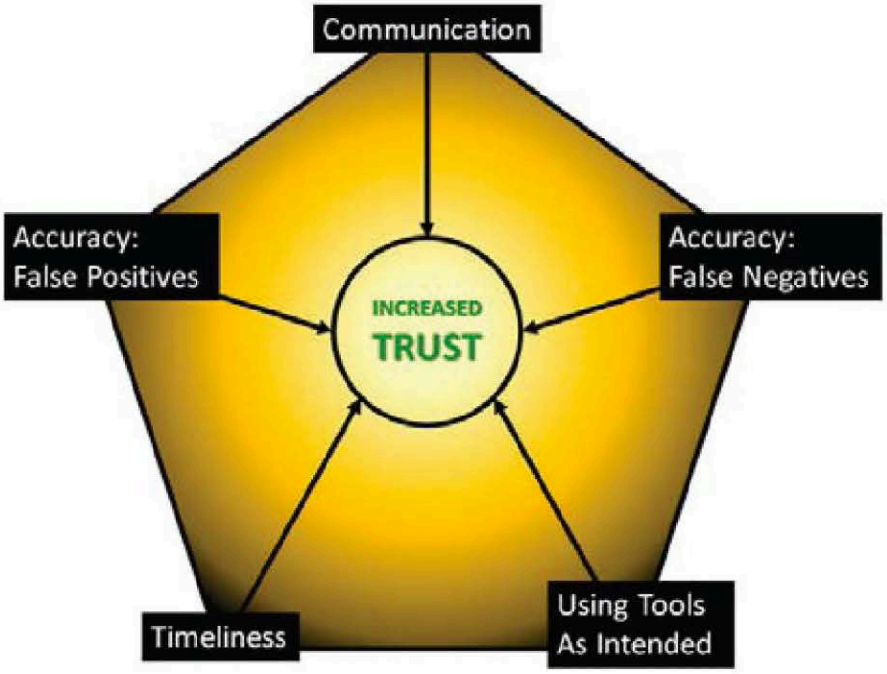

Figure 5.2: Factors affecting trust in defender/analyst

5.3.1 Communication

Whenever two or more parties are involved in communication, if they establish a common ground and build upon shared mental models they will be more effective and efficient. As a result, the interactions and collaborations shared among them should benefit and proceed as best as possible. Focusing on defender trust, we

separate communication into the subcategories of accuracy, thoroughness or completeness, timeliness, and honesty. Effective communication relies on a defender to accurately convey information with thoroughness and in a timely manner, affected by the amount of information, how tied the information is to a specific context, and how well the parties involved in the communication understand one another. Whether or not communication is sufficiently thorough relies on how well the information is processed by the receiver with minimal need to repeat or revisit previous information. For cyber defenders, timeliness is essential as any wasted time might give an attacker more opportunity to do damage or an attack the chance to escape detection. Lastly, honesty is important in building trust regardless of space, and dishonest communication will not only harm team effectiveness in the cyber domain but might harm how well and how accurately defensive efforts address intrusions.

5.3.2 Accuracy

The detection accuracy of a defender can be measured by the percent of false positive and false negative incident reports filed by an individual defender. It would be expected that a skilled defender with expertise would have lower false positive and false negative rates than those of a less skilled defender. The ability to trust the work the defender produces will increase as the percentage of false positive and false negative incident reports decrease.

5.3.3 Timeliness

Just as in communication timeliness, the timeliness of a defenders actions is critical to achieving successful agility actions and mitigating the effects of attackers actions. Timeliness considers:

- how quickly a defender is to detect intrusions;
- how quickly a defender is to relay critical and time-sensitive information to their superiors;
- how quickly the defender chooses appropriate, effective agility or mitigation actions.

5.3.4 Using tools as intended

For cyber security, intended tool use focuses on the competent matching of tools and tool feature use to task completion, be it in the detection of intrusions, reactions to successful attacks, or hardening of the network against potential future attacks. There are two aspects of tool use that can be evaluated: the effectiveness of training for defenders and the performance of defenders in their day to day work. Training for a cyber defender must include a combination of interacting with software and IT tools to establish familiarity with their function and relation to defensive tasks and learning and adhering to the policies that govern defense efforts. Training with software for cyber defenders takes two different forms:

- tool-based, focused on reviewing features and functions before running through exercises that use the discussed elements;
- narrativebased, where tool and software functions are discussed within the context of adversary tactics and techniques.

The evaluation of training can be seen in performance, as superior performance reflects superior training. Performance can be directly measured by combining the timeliness and accuracy elements discussed above. All things considered equal in a cyber environment, if two defenders report on the same intrusion with different quickness and accuracy the root cause is likely performance differences with tools. These differences may reflect training issues and knowledge gaps. For example, Stevens-Adams et al. [72] separated defenders into three teams, one getting narrative training, one tool-based training, and the third with a mixture of members who either received one or the other; after five days of training and three days of exercise the narrative-based team scored the highest of all teams, and the individuals with narrative-based training scored higher than the other individuals. Here, a controlled environment simulating real-world usage enabled team and individual performance to assess training and knowledge. Where these metrics reveal performance differences, the details of a CTA, constructing an understanding of the ways with which analysts complete work, also enable an evaluation of these methods and identify where tool use could be improved or

where training should be re-tooled and updated [73].

5.4 Hybrid risk assessment model architecture

Information systems concentrate invaluable information resources, generally composed of the computers and servers that process the data of an organisation. Given the number and complexity of attacks, security teams need to focus their actions on the most important attacks, in order to select the most appropriate security controls. Importance in our context is related to the risk the attack induces on the missions of the information system. The most impacting attacks are multi-step attacks. A multi-step attack is a complex attack composed of several successive steps. Each step may be illegitimate (e.g., the exploitation of a vulnerability in software) or legitimate (e.g., a user with administrators privilege accessing sensitive data). For example, an attacker first subverts a client computer using a spear-phishing email exploiting a vulnerability, then attacks the Active Directory to get administrator privileges, and, thanks to this privilege, accesses a database server that contains sensitive data. In order to defend against complex attacks, we need to model them and assess associated risks. But risk assessment, and in particular dynamic risk assessment (i.e., regular update of risk assessment in operational time, according to the occurring attacks) is not easy. Several models have been proposed in the literature to formalise multi-step attacks, mainly tree or graph-based models. An attack graph, for example, is a risk analysis model grouping all the paths an attacker may follow in an information system. Several tools to generate attack graphs exist. Their use is attractive because they leverage already available information (vulnerability scans and network topology). However, attack graphs are static and do not contain detections or attack status and thus are not fitted for dynamic risk assessment. Several extensions of static risk assessment models have been proposed in the literature to accommodate dynamic risk assessment, but they suffer from common limitations, such as existing cycles. According to the National Information Assurance Glossary, a risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood

of occurrence. As a result, the risk is generally considered in Information Security Management Systems (ISMS) as the combination of the likelihood of the exploitation of vulnerabilities and their impact on the system. Determining the risk in a system is the result of a 5-step process detailed by the National Institute of Standards and Technology (NIST), as shown in Figure 5.3. In this process the step (2.c) is the determination of the likelihood of occurrence of the attacks. It takes as input the potential threat sources and the vulnerabilities and attack predisposing conditions. Once the likelihood of attacks has been assessed, the next step is to determine their magnitude of impact. Finally, from likelihood and impact, we can compute the risk. In order to make risk assessment dynamic, the process is maintained over time and its results have to be communicated regularly to security management operators.

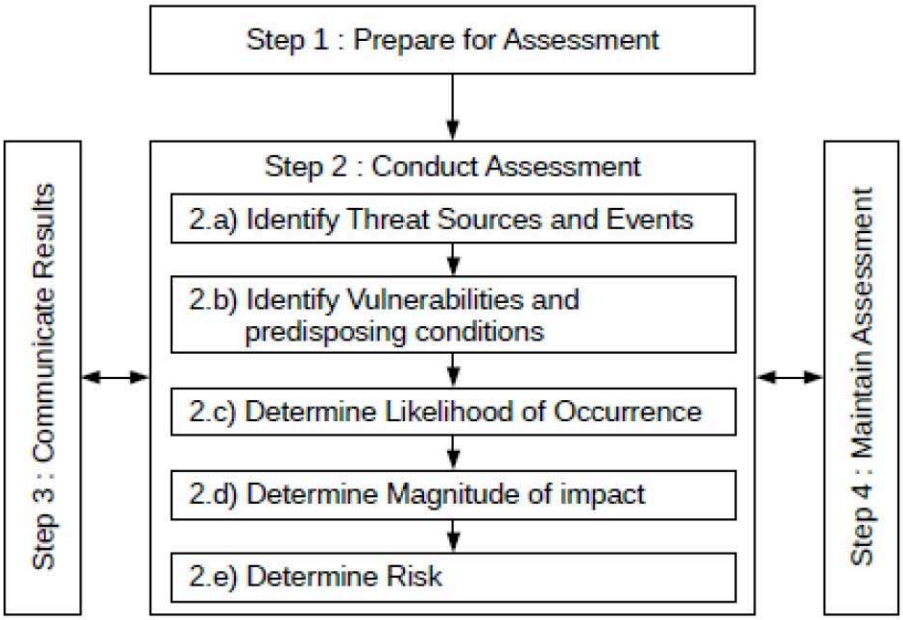

Figure 5.3: Risk Assessment Processl

At an organisational level, several methods help to analyse the risk of information systems and keep those systems secure. For example, ISO/IEC 27000 [74] is the ISMS Family of Standards providing recommendations on security, risk and control in an information system. In particular, ISO/IEC 27005 describes a

methodology to manage the risks and implement an ISMS. Another well-known method for the analysis of risks in information systems is EBIOS (Expression of Needs and Identification of Security Objectives). These standards present global methodologies to manage risks in organisations. They generally combine (1) technical tools (e.g., vulnerability scanner) to assess, for example, the vulnerabilities and the likelihood of attacks and (2) organisational methodologies (e.g., stakeholder interviews) to identify the critical assets and consequences of successful attacks. The technical tools for dynamic risk assessment usually do not include a model to detect the occurring multi-step attacks and assess their likely futures. In this paper, we build such a model that aims at assessing the risk brought by the exploitation of technical vulnerabilities in a system. This model mostly focuses on the step (2.c) of the NIST's risk assessment process of Figure 5.3: the determination of the likelihood of occurrence of attacks. Indeed, methodologies to estimate attacks likelihood do not depend on the system in which they are implemented, contrary to the impact assessment which may require adaptation for the target organisation. Thus, in our experimentations, we evaluate our risk model only by its likelihood results, by assuming that all compromised assets induce the same impact. The model we propose in this paper is a new hybrid model combining attack graphs and Bayesian networks for dynamic risk assessment (DRA). This model is subdivided into two complementary models:

- the Dynamic Risk Correlation Models (DRCMs) correlate a chain of alerts with the knowledge on the system to analyse ongoing attacks and provide the probabilities of hosts being compromised;
- the Future Risk Assessment Models (FRAMs) take into account existing vulnerabilities and the current attack status to assess which potential attacks are most likely to occur.

DRCMs aim at threat likelihood assessment, identifying where the attack comes from. It outputs probabilities that attacks are completed and that assets of the information system are compromised. These probabilities provide security operators with the capability to manage priorities according to the likelihood of ongoing attacks. FRAMs aim at threat mitigation, identifying the most likely and impacting next steps for the attacker. With respect to the current state of

the art, the contributions are twofold. First, we provide an explicit model for DRA and a process for handling cycles. Second, the model provides a significant performance improvement in terms of number of nodes and vulnerabilities over the existing state of the art, enabling scalability. While classic Bayesian attack graph models are usually demonstrated over a few nodes, we show that our model can be realistically computed at the scale of an enterprise information system.

5.4.1 State of art

An attack graph is a model regrouping all the paths an attacker may follow in an information system. It has been introduced by Phillips and Swiler in [75]. A study of the state of the art about attack graphs compiled from early literature on the subject has been carried out by Lippmann and Ingols [76], while a more recent one was made available by Kordy et al. [77]. Topological attack graphs are based on directed graphs. Their nodes are topological assets (hosts, IP addresses, etc.) and their edges represent possible attack steps between such nodes. Attack graphs are generated with attack graph engines. There are three main attack graph engines: (1) MulVAL, the Multi-host, Multi-stage Vulnerability Analysis Language tool created by Ou et al. [78], (2) the Topological Vulnerability Analysis tool (TVA) presented by Jajodia et al. in [79] (commercialised under the name Cauldron) and (3) Artz's NetSPA [80]. Attack graphs are attractive because they leverage readily available information (vulnerability scans and network topology). However, they are not adapted for ongoing attacks, because they cannot represent the progression of an attacker nor be triggered by alerts. Thus, they must be enriched to provide the functionalities needed to perform dynamic risk assessment, for example using Bayesian networks. A Bayesian network is a probabilistic graphical model introduced by Judea Pearl [81]. It is based on a Directed Acyclic Graph, where nodes represent random variables, and edges represent probabilistic dependencies between variables. For discrete random variables, these dependencies can be specied using a Conditional Probability Table associated with each child node. Bayesian networks are particularly interesting for computing inference, i.e. calculating the probability of each state of all nodes of the network, given evidences, i.e. nodes that have been set to a specic state. In

the general case, exact inference is a NP-hard problem and can be done effciently only on small networks, using the algorithm of Lauritzen and Spiegelhalter [82]. However, if the structure of the graph is a polytree, it can be done in quasi-linear time, using Pearl's Belief Propagation Algorithm [83]. A Bayesian attack graph, introduced by Liu and Man in [84] is an extension of an attack graph based on a Bayesian network, constituted of nodes representing a host in a specific system state (a true state means that the host is compromised) and edges representing possible exploits that can be instantiated from a source host to a target host. The major concern of building such a Bayesian network from an attack graph is due to the structure of a Bayesian network that must be acyclic, while attack graphs almost always contain cycles. To avoid cycles, Liu and Man assume that an attacker will never backtrack once reaching a compromised state, but do not detail how such assumption is used to build the model. In [85], Frigault and Wang use Bayesian inference in Bayesian Attack Graphs to calculate security metrics in an information system. Xie et al. present in [86] a Bayesian network used to model the uncertainty of occurring attacks. The Bayesian attack graph is enhanced with three new properties: separation of the types of uncertainty, automatic computation of its parameters and insensitivity to perturbations in the parameters choice. This model also adds nodes dedicated to dynamic security modelling: an attack action node models whether or not an action of the attacker has been performed, a local observation node models inaccurate observations (IDS alerts, logs, etc.). In [87], Cole uses a Credal network (a Bayesian network with imprecise probabilities) to represent parameters uncertainty and detect attack paths. He demonstrates that the uncertainty is too high for single-step attacks, but for multi-step attacks, it is possible to achieve high condence in the detections. However, the computational costs of inferences in a Credal network are prohibitive to use it with real network topologies. Bayesian networks add to the advantages of direct acyclic graphs powerful tools to compute and propagate probabilities between nodes of the graph. Moreover, the dependencies between nodes are not AND or OR relations anymore, but are probabilities of occurrence with a set of predecessors, which is much more expressive. It is thus a very interesting model for dynamic risk assessment. However, two important problems arise when we want to use Bayesian networks for modelling ongoing multi-step attacks:

- performance, as the inference in a Bayesian network can be very complex;
- a Bayesian network must be based on an acyclic graph, which is generally not the case of attack graphs.Heuristics allow to suppress cycles, but they also suppress paths that could be followed by an attacker.

5.4.2 Hybrid Risk Assessment Model

The approach distinguishes two sub-objectives of determining the likelihood of occurrence within dedicated models: Dynamic Risk Correlation Models (DRCMs) and Future Risk Assessment Models (FRAMs), , according to [88], combined to provide a complete Hybrid Risk Assessment Model (HRAM), whose architecture is presented in Figure 5.4. Building process The goal of the DRCM is to provide explanations for the alerts that have been raised by intrusion detection sensors. By explanation, we mean the identification of the likely source nodes that have been compromised and that have enabled the attacker to launch the detected attack. A DRCM is built from the most recently received alert, the target, and explains why this alert has been generated, taking into account past alerts. As soon as a new alert is received, a new DRCM is built. Older DRCMs are kept in parallel with the newly generated DRCM, to manage scenarios with several distinct simultaneous attacks (i.e., a new alert is not related to older ones). Probabilities of all kept DRCMs are reconciliated. Following the process described, we construct each DRCM in such a way as not to have any cycles, but to keep all possible attack paths directed to the target. The DRCM is built from the latest received alert. Then, they recursively add the attack steps and assets allowing to compromise the target. They store, in each DRCM Topological Asset, the path from this node to the target of the DRCM. This allows to ensure that the building process never comes back on a previously exploited node and thus the DRCM does not have cycles, but contains all possible causes of the latest received alert. Moreover, they design this building process in order to generate a graph structure of the DRCM which is a polytree (i.e., directed graph with no directed nor undirected cycles). This implies, for example, to duplicate the condition and sensor nodes (i.e., new conditions and sensors for each added attack step). The DRCM being a polytree satises the requirements of Pearl's inference

algorithm [83], which is quasilinear in the number of nodes. Thus, the inference in such a DRCM with a polytree structure containing duplicated nodes is much more effcient and consume less memory, in comparison with a directed acyclic graph structure with fewer nodes (no duplicates), for identical results.

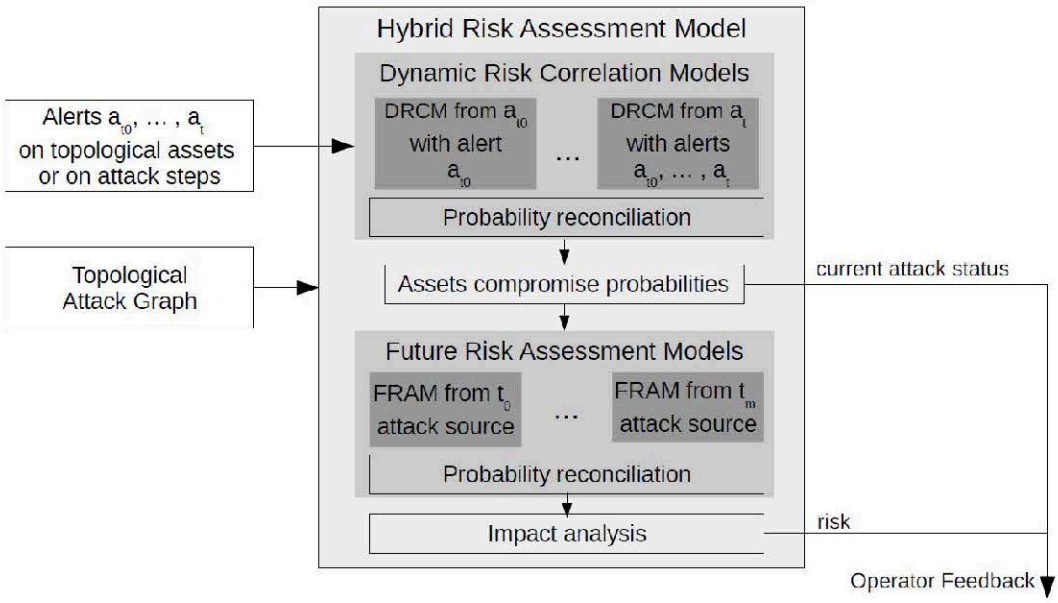

Figure 5.4: Hybrid Risk Assessment Model Architecture

Model nodes A DRCM is a Bayesian network with 5 types of nodes. Each one represents a Boolean random variable and is associated with a conditional probability table (CPT), representing its probabilistic dependency toward its parents.

- A DRCM Topological Asset represents the random variable describing the status of compromise of a specic asset of the TAG, in order to exploit the DRCM Target. It has one parent (DRCM Attack Step) of each type of attack that can be used to compromise it (i.e., there may be as many parent nodes as there are different attack types) and a DRCM Attack Source representing that this node may be a source of attack. Its CPT is a noisy OR: at least one successful attack is needed to compromise this node and it can also be compromised if it is the source of attack itself. Even if no parent is compromised, there is still a little chance that an unknown attack compromises this node.

- A DRCM Attack Source represents the random variable describing that a specic asset of the TAG is a source of attack. It is a node without parents. As such, it does not have a complete CPT, but only an a priori probability value. The a priori probability of having an attack coming from this asset has to be set by the operators knowing the probability that an attack starts from this threat source.

- A DRCM Attack Step represents the random variable describing that an attack step has been completed by an attacker. It has two types of parents: A DRCM Conditions, and a DRCM Topological Asset. At a minimum, the A DRCM Topological Asset is required, but the exact CPT depends on the type of attack step.

- A DRCM Condition represents the random variable describing that the condition of an attack step is veried. It does not have any parent. Its a prioriprobability is the probability of successful exploitation of the condition.

- A DRCM Sensor can either be attached to a DRCM Topological Asset or to a DRCM Attack Step. It represents the random variable describing that the sensor of an attack step or an asset has raised an alert. Its parent is the object monitored by the sensor. Its CPT represents the false-positive and false-negative rates of the sensor. The sensor corresponding to the latest received alert, and from which the DRCM is built, is the target of the DRCM.

Figure 5.5 shows an example of a DRCM built from an alert on host h1 (the node in dotted line on the left) in a topology of 3 hosts. DRCM Topological Assets are represented by a rectangle shape, DRCM Attack Sources by a vesided shape, DRCM Attack Steps by a diamond shape, and DRCM Conditions by an oval shape. Model usage As shown in Figure 5.5, we build the structure of the DRCM according to the TAG, starting from the latest received alert. Then, we set the states of the DRCM Sensors according to the previous security alerts received from the sensors:

- If the sensor of an attack step or an asset exists and is deployed in the

network, as long as it has not raised any alert, all related DRCM Sensors are set to the NoAlert state.

- If the sensor has raised an alert corresponding to this attack step or asset, the related DRCM Sensors are set to the Alert state.
- If the attack step or asset has no deployed sensor, there is NoInfo about this sensor. So, the related DRCM Sensors cannot be set in any state and these nodes can be safely deleted from the DRCM, with no impact on other nodes final probabilities.

Then, they use a Bayesian network belief propagation algorithm (e.g., Pearl's) to update the probabilities of each state at all the nodes.

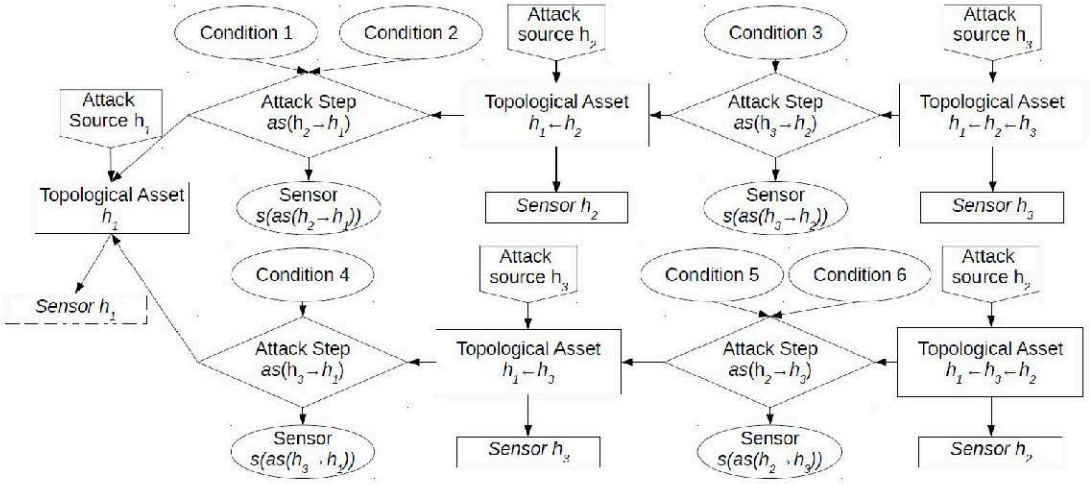

Figure 5.5: Dynamic Risk Correlation Model

5.4.3 Accuracy

To evaluate the accuracy of the results of the DRCMs (i.e., how close the compromise probabilities are from the truth), it has simulated an attack scenarios of up to 7 successive steps on random topologies of 70 hosts, as presented (results

are identical from 10 up to 120 hosts). It has added to the 7 true positive alerts of these scenarios, 10 randomly located false positives and 10 sensors with no information. This experimentation, according to [88], shows that the greater the number of attack steps in the scenario, the larger the recognition probability and the smaller the confidence interval. Moreover, it shows a large free space between the curve of compromised hosts and the curve of healthy hosts. This means that there are no false negative and false positive introduced by the DRCM. Finally, even if there are false positives and sensors without information, compared to the number of successive attack steps (up to 7), they retrieve only the real attack elements, thanks to our model built from the latest received alert and taking into account the order and relations between attack steps. Many people have proposed enhancements to improve attack graphs or trees with Bayesian networks, in order to use them for dynamic risk assessment [84] [86]. However, they do not describe accurately how they address cycles that are inherent to attack graphs. For example, in [86], Xie et al. present an extension of MulVAL attack graphs, using Bayesian networks, but they do not mention how to manage the cycle problem, while MulVAL attack graphs frequently contain cycles. In the same way, in [85], Frigault and Wang do not mention how they deal with the cycle problem when constructing Bayesian attack graphs. In [84], Liu and Man assert that to delete cycles, they assume that an attacker will never backtrack. Poolsappasit et al. in [89] use the same hypothesis. However, as detailed, they do not present how they deal with this hypothesis to keep all possible paths in the graph, while deleting cycles. We propose here novel models exploding cycles in the building process, in order to keep all possible paths, while deleting the cycles, to compute the Bayesian inference. Moreover, Aguessy at al. [88], also add several improvements (practical pruning, polytree structure, etc.) reducing the size of the graph structure and improving the performance of the inference. They thus constrain the size of the graph in which we do Bayesian inference, while conserving all paths by linearising cycles. The model presented by Xie et al. [86] and the one of Liu and Man [84] are made of a single model to describe the compromise status of assets of the information system. In a single model, an increase of compromise probability of an asset due to an already happened attack is mixed up with an increase due to a very likely possible future. However,

the distinction of these two causes is very valuable for a security operator, for example to select where to deploy a remediation. The hybrid model we propose separates the compromise information of the past alerts from those of the likely futures. It allows a security operator to know if a topological asset has already been compromised (thanks to DRCMs) or if it may be compromised in the near future (FRAMs). This work focus on the likelihood component of the risk assessment. Thus, it uses a simple impact function as output of the FRAMs, matching each compromised topological asset with a fix impact value. Other works of the state of the art rather focus on the impact component. For example, Kheir et al. in [90] details how to use a dependency graph to compute the impact of attacks on Confidentiality, Integrity and Availability. Models such as [91] use Dynamic Bayesian Networks to monitor and predict the future status of the system. It uses a sequence of Bayesian networks, which can be huge to process. The model proposed here keeps only the past information necessary to explain all alerts and to update the models to evaluate potential futures (FRAMs). Moreover, the building process and exploitation of DRCMs takes into account the temporality of raised alerts to determine attacks. Finally, contrary to other models based on Bayesian attack graphs, the model can distinguish several distinct simultaneous attacks in the alerts raised in a system, by analysing all kept DRCMs . The experimental validation uses simulated topologies far bigger than the state of the art. For example, Xie et al. assess their model on 3 hosts and 3 vulnerabilities [86], Liu and Man on 4 hosts and 8 vulnerabilities [84]. The real world examples used by Frigault andWang in [91] contain at most 8 vulnerabilities on 4 hosts. The test network used by Poolsappasit et al. in [89] contains 8 hosts in 2 subnets, but with only 13 vulnerabilities. Thanks to our polytree models, it successfully runs the HRAM effciently on simulated topologies with up to 120 hosts for a total of more than 3600 vulnerabilities.

Chapter 6

General Conclusions

"There are in fact two things, science and opinion; the former begets knowledge, the latter ignorance."

— Hippocrates of Kos, *460 BC - 370 BC*

The development of modern technology and their application to the totality of the objects which every day people interact with, obliges to find new ways in designing Security within an organization. One of main point to keep in mind is, above all, the importance of the human factor that is crucial for every security system. Recent security breaches, in fact, showed that every attack begins with the involvement of user and continues with exploiting technology bugs. In almost all cases, without human collaboration, conscious and unconscious, it is really difficult to reach the criminal goal. The digital profiling, for instance, is a new computer investigation tool with the aim of extracting information from memory of digital devices and assist computer investigator in their analysis and help them to identify a possible user/criminal digital profile. This type of analysis is suitable to all the devices: to all personal computers, mobile phones, smartphones, tablets etc. Futhermore, embedded devices are not excluded of this methodology: to give just one example, a GPS navigator, even though it may seems at first glance that may not contain data useful to find a solution of a crime, can provide valuable information on the movements of a subject, such as places where has gone, the usual route that, if compare with the position of his home, may help to delineate the aim of its activities. Digital profiling techniques can also

be applied to the contents of storage areas provided in remote provider and data streams selected for example in a certain time on a computer attack. The basic idea that members of the Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions, have lead us toward an integrated model based on a cultural approach in which the trust and co-partnership of the security system are the main focal point. This model implies that technology solutions separated from the surrounding environment are completely inadequate. Social, organizational, and psychological factors have to be considered when implementing security within an organization. A valid complement (usable) to technical solutions has been found in a SDSC as a set of collective knowledge, common practices, and intuitive common behavior about digital security that the members of a Society share. However, the embedded devices, such as satellite navigation systems, although at first glance do not seem to contain useful data to carry out an investigation, when subjected to analysis aimed at finding information useful to construct the Digital Profiling may provide data of interest, and cross-compared with those from other sources during an investigation, provide valuable information on the movements of a subject, such as, for example, the places where one has gone, his modus operandi, the verification of an alibi, the usual route that, when compared with the location of his home, can help delineate the scope of his activities. This type of analysis that may be of use are those fields where there is the need for targeted analysis of digital identification of the authors, as in crimes such as pedophilia, theft, robbery, alterations of ATM, extortion, smuggling, drug and weapons trafficking. Thus it can be particularly useful in operations against organized crime, anti-terrorism operations, intelligence operations, where it can interface with the statistical study in the prediction and prevention of criminal events. The security in the energy sector is one of the major emergencies that are occurring in the last few months. We can say, after this careful analysis, which Internet of Things, the so-called global environment that encompasses all the functional components of contemporary society (such as energy, commodities, etc.) elated systems to communicate with each other, is opening a new front that also involves critical infrastructures such as smart grid. For those reasons, an integrated and appropriate strategy becomes a priority in order to counter new threats. It is therefore necessary to direct

the efforts and take appropriate measures to protect and contrast both in terms of organization and strategically. Countering amplification DDoS attacks is an important security issue to be faced with in modern network-empowered organizations.

In Chapter 2, we proposed an approach beyond CIS paradigm that have mainly three characteristics:centrality of the human factor;the ability to mold to the scenario to be protected;dynamic adaptation to external and internal threats.

In Chapter 3, we analyze the hypothesis of an adaptable model based on consumerization. The basic idea that members of the Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions, have lead us toward a integrated model based on a cultural approach in which the trust and co-partnership of the security system are the main focal point. This model implies that technology solutions separated from the surrounding environment are completely inadequate.

In Chapter 4, we deal with integrated Societal Digital Security Culture.

In Chapter 5, we face the improving of cyber security through human System integration and adopting ann hybrid risk assessment model.

Appendix A

List of Papers Not Covered in this Thesis

A.1 Papers in Journals

1. Colombini, C. M., Colella, A. (2012). Digital scene of crime: technique of profiling users. JoWUA, 3(3), 50-73.

A.2 Papers in International Conferences

1. Colombini, C., Colella, A. (2011, August). Digital profiling: A computer forensics approach. In International Conference on Availability, Reliability, and Security (pp. 330-343). Springer Berlin Heidelberg;

2. Colombini, C. M., Colella, A., Mattiucci, M., Castiglione, A. (2012, August). Network profiling: Content analysis of users behavior in digital communication channel. In International Conference on Availability, Reliability, and Security (pp. 416-429). Springer Berlin Heidelberg;

3. Colombini, C. M., Colella, A., Castiglione, A., Scognamiglio, V. (2012,

July). The Digital Profiling Techniques Applied to the Analysis of a GPS Navigation Device. In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on (pp. 591-596). IEEE;

4. Colombini, C. M., Colella, A., Mattiucci, M., Castiglione, A. (2013, September). Cyber threats monitoring: Experimental analysis of malware behavior in cyberspace. In International Conference on Availability, Reliability, and Security (pp. 236-252). Springer Berlin Heidelberg.;

5. Colella, A., Colombini, C. M. (2014, September). Amplification DDoS attacks: Emerging threats and defense strategies. In International Conference on Availability, Reliability, and Security (pp. 298-310). Springer International Publishing;

6. Colella, A., Castiglione, A., Colombini, C. M. (2014, September). Industrial Control System Cyber Threats Indicators in Smart Grid Technology. In Network-Based Information Systems (NBiS), 2014 17th International Conference on (pp. 374-380). IEEE;

7. Colella, A. (2015). Smart Grid Technology. A New Challenge for Cybersecurity. In The Protection of Critical Energy Infrastructure Against Emerging Security Challenges (pp.75-84). IOS press;

8. Colella, A., Castiglione, A., De Santis, A., Esposito, C., Palmieri, F. (2016, September). Privacy-Aware Routing for Sharing Sensitive Information across Wide-Area Networks. In Network-Based Information Systems (NBiS), 2016 19th International Conference on (pp. 70-75). IEEE.

Bibliography

[1] Chun Wei Choo. *Information management for the intelligent organization: the art of scanning the environment.* Information Today, Inc., 2002.

[2] Lewis Hassell and Susan Wiedenbeck. Human factors and information security. *Manuscript. Available at: http://repository. binus. ac. id/content A*, 334, 2004.

[3] Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. Human, organizational, and technological factors of it security. In *CHI '08 extended abstracts on Human factors in computing systems*, CHI EA '08, pages 3639–3644, New York, NY, USA, 2008. ACM.

[4] Tim Mather, Subra Kumaraswamy, and Shahed Latif. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance.* O'Reilly Media, Inc., 2009.

[5] Avanade Inc. Global Survey: Dispelling Six Myths of Consumerization of IT, January 2012.

[6] Christian W. Probst and René Rydhof Hansen. Fluid information systems. In *Proceedings of the 2009 workshop on New security paradigms workshop*, NSPW '09, pages 125–132, New York, NY, USA, 2009. ACM.

[7] Sean Peisert, Matt Bishop, Laura Corriss, and Steven J. Greenwald. Quis custodiet ipsos custodes?: a new paradigm for analyzing security paradigms with appreciation to the roman poet juvenal. In *Proceedings of the 2009*

workshop on New security paradigms workshop, NSPW '09, pages 71–84, New York, NY, USA, 2009. ACM.

[8] John Harauz and Lori M. Kaufman. A new era of presidential security: The president and his blackberry. *IEEE Security & Privacy*, 7(2):67–70, 2009.

[9] Aniello Castiglione, Roberto De Prisco, and Alfredo De Santis. Do You Trust Your Phone? In Tommaso Di Noia and Francesco Buccafurri, editors, *EC-Web*, volume 5692 of *Lecture Notes in Computer Science*, pages 50–61. Springer, 2009.

[10] DIANE Publishing Company. *A Guide to Understanding Data Remanence in Automated Information Systems*. DIANE Publishing Company, 1995.

[11] Security Research Centre Glenn S. Dardick. Cyber forensics assurance. In *Proceedings of the 8th Australian Digital Forensics Conference*, ADFC '10, pages 57–64, Perth Western Australia, 2010. Cowan University.

[12] A Colella and C. Colombini. Security Paradigm in Ubiquitous Computing. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, pages 634–638, July 2012.

[13] Antonio Colella, Aniello Castiglione, and Alfredo De Santis. The role of trust and co-partnership in the societal digital security culture approach. In *Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on*, pages 350–355. IEEE, 2014.

[14] Clara Maria Colombini, Antonio Colella, Marco Mattiucci, and Aniello Castiglione. Network profiling: Content analysis of users behavior in digital communication channel. In *International Conference on Availability, Reliability, and Security*, pages 416–429. Springer Berlin Heidelberg, 2012.

[15] Mark Stamp. *Information Security - Principles and practies*. JohnWiley and Sons, Inc., 2006.

[16] Matt Bishop, Marco Carvalho, Richard Ford, and Liam M Mayron. Resilience is more than availability. In *Proceedings of the 2011 workshop on New security paradigms workshop*, pages 95–104. ACM, 2011.

[17] Konstantin Shvachko, Hairong Kuang, Sanjay Radia, and Robert Chansler. The hadoop distributed file system. In *Mass storage systems and technologies (MSST), 2010 IEEE 26th symposium on*, pages 1–10. IEEE, 2010.

[18] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. The google file system. In *ACM SIGOPS operating systems review*, volume 37, pages 29–43. ACM, 2003.

[19] Bharat B Madan and Yan Lu. Attack tolerant big data file system. In *ACM Sigmetrics Big Data Analytics Workshop*. Citeseer, 2013.

[20] Amani Mobarak AlMadahkah. Big data in computer cyber security systems. *International Journal of Computer Science and Network Security (IJCSNS)*, 16(4):56, 2016.

[21] Francesco Palmieri, Ugo Fiore, and Aniello Castiglione. Automatic security assessment for next generation wireless mobile networks. *Mobile Information Systems*, 7(3):217–239, 2011.

[22] Sini Ruohomaa, Lea Viljanen, and Lea Kutvonen. Guarding enterprise collaborations with trust decisions: the tube approach. In *In Proceedings of the First International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems (IS-TSPQ 2006*, 2006.

[23] Leszek Lilien, Adawia Al-Alawneh, and Lotfi Ben Othmane. The pervasive trust foundation for security in next generation networks. In *Proceedings of the 2010 workshop on New security paradigms*, NSPW '10, pages 129–142, New York, NY, USA, 2010. ACM.

[24] M. Satyanarayanan. Pervasive computing: Vision and challenges. *IEEE Personal Communications*, 8:10–17, 2001.

[25] Lotfi Ben Othmane, Harold Weffers, Rohit Ranchal, Pelin Angin, Bharat Bhargava, and Mohd Murtadha Mohamad. A case for societal digital security culture. In *IFIP International Information Security Conference*, pages 391–404. Springer, 2013.

[26] LotfiBen Othmane, Harold Weffers, Rohit Ranchal, Pelin Angin, Bharat Bhargava, and MohdMurtadha Mohamad. A Case for Societal Digital Security Culture. In LechJ. Janczewski, HenryB. Wolfe, and Sujeet Shenoi, editors, *Security and Privacy Protection in Information Processing Systems*, volume 405 of *IFIP Advances in Information and Communication Technology*, pages 391–404. Springer Berlin Heidelberg, 2013.

[27] G. Carullo, A Castiglione, G. Cattaneo, A De Santis, U. Fiore, and F. Palmieri. FeelTrust: Providing Trustworthy Communications in Ubiquitous Mobile Environment. In *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on*, pages 1113–1120, March 2013.

[28] D. Gollmann. From insider threats to business processes that are secure-by-design. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 3(1-2):4–12, 2012.

[29] D.A. Mundie, S.J. Perl, and C.L. Huth. Insider threat defined: Discovering the prototypical case. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(2):7–23, 2014.

[30] W.R. Claycomb, P.A. Legg, and D. Gollmann. Guest editorial: Emerging trends in research for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(2):1–6, 2014.

[31] P.R.J. Trim and Yang-Im Lee. A security framework for protecting business, government and society from cyber attacks. In *System of Systems Engineering (SoSE), 2010 5th International Conference on*, pages 1–6, June 2010.

[32] Yang-Im Lee. Strategic transformational management in the context of inter-organizational and intra-organizational partnership development. In Peter R.J. rim and Jack Caravelli, editors, *Strategizing resilience and reducing vulnerability*. Nova Science Publishers, 2009.

[33] P.R.J. Trim and H.Y. Youm. Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership. *Report Submitted to*

the Korean Government and the UK Government - British Embassy Seoul: Republic of Korea, March 2014.

[34] Vlatko Cvrtila and Anita Perešin. New security models and public-private partnership. *Collegium Antropologicum*, 38(1):195–204, 2014.

[35] Kregg Aytes and Terry Connolly. Computer security and risky computing practices: A rational choice perspective. *Advanced Topics In End User Computing*, 4:257, 2005.

[36] Sheila Rosenblum, Karen Seashore Louis, and Nancy Brigham. *Stability and change: Innovation in an educational context.* Plenum Press New York, 1981.

[37] Eugene Schultz. Security training and awareness - fitting a square peg in a round hole. *Computers & Security*, 23(1):1 – 2, 2004.

[38] Ken Doughty. Implementing enterprise security: a case study. *Computers & Security*, 22(2):99–114, 2003.

[39] Effy Oz. Organizational commitment and ethical behavior: An empirical study of information system professionals. *Journal of Business Ethics*, 34(2):137–142, 2001.

[40] Edward Hartono, Albert L Lederer, Vijay Sethi, and Youlong Zhuang. Key predictors of the implementation of strategic information systems plans. *ACM SIGMIS Database*, 34(3):41–53, 2003.

[41] ClaraMaria Colombini, Antonio Colella, Marco Mattiucci, and Aniello Castiglione. Network Profiling: Content Analysis of Users Behavior in Digital Communication Channel. In Gerald Quirchmayr, Josef Basl, Ilsun You, Lida Xu, and Edgar Weippl, editors, *Multidisciplinary Research and Practice for Information Systems*, volume 7465 of *Lecture Notes in Computer Science*, pages 416–429. Springer Berlin Heidelberg, 2012.

[42] Antonio Colella, Aniello Castiglione, and Clara Maria Colombini. Industrial control system cyber threats indicators in smart grid technology. In *Network-Based Information Systems (NBiS), 2014 17th International Conference on*, pages 374–380. IEEE, 2014.

[43] Francesco Palmieri, Sergio Ricciardi, Ugo Fiore, Massimo Ficco, and Aniello Castiglione. Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures. *The Journal of Supercomputing*, pages 1–22, 2014.

[44] F. Palmieri, S. Ricciardi, and U. Fiore. Evaluating Network-Based DoS Attacks under the Energy Consumption Perspective: New Security Issues in the Coming Green ICT Area. In *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, pages 374–379, Oct 2011.

[45] Sergio Ricciardi, Davide Careglio, Ugo Fiore, Francesco Palmieri, German Santos-Boada, and Josep Sole-Pareta. Analyzing Local Strategies for Energy-Efficient Networking. In Vicente Casares-Giner, Pietro Manzoni, and Ana Pont, editors, *NETWORKING 2011 Workshops*, volume 6827 of *Lecture Notes in Computer Science*, pages 291–300. Springer Berlin Heidelberg, 2011.

[46] Aniello Castiglione, Roberto De Prisco, Alfredo De Santis, Ugo Fiore, and Francesco Palmieri. A botnet-based command and control approach relying on swarm intelligence. *Journal of Network and Computer Applications*, 38:22 – 33, 2014.

[47] Pedro HJ Nardelli, Nicolas Rubido, Chengwei Wang, Murilo S Baptista, Carlos Pomalaza-Raez, Paulo Cardieri, and Matti Latva-aho. Models for the modern power grid. *The European Physical Journal Special Topics*, pages 1–15, 2014.

[48] Raj Samani, Jim Reavis, and Brian Honan. *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*. Syngress, 2014.

[49] Ahmed AlKalbani, Hepu Deng, and Booi Kam. Investigating the role of socio-organizational factors in the information security compliance in organizations. *arXiv preprint arXiv:1606.00875*, 2016.

[50] Tejaswini Herath and H Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009.

[51] Mikko Siponen and Anthony Vance. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, pages 487–502, 2010.

[52] Princely Ifinedo. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *issues*, 36(42):45–52, 2013.

[53] Barry D Smith and Glen S Jamieson. Notes: Possible consequences of intensive fishing for males on the mating opportunities of dungeness crabs. *Transactions of the American Fisheries Society*, 120(5):650–653, 1991.

[54] Fayçal Bouraoui, Sihem Benabdallah, Amel Jrad, and G Bidoglio. Application of the swat model on the medjerda river basin (tunisia). *Physics and Chemistry of the Earth, Parts A/B/C*, 30(8):497–507, 2005.

[55] Dimitris Geneiatakis, Tasos Dagiuklas, Georgios Kambourakis, Costas Lambrinoudakis, Stefanos Gritzalis, Sven Ehlert, Dorgham Sisalem, et al. Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys and Tutorials*, 8(1-4):68–81, 2006.

[56] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3):523–548, 2010.

[57] Gurpreet Dhillon and James Backhouse. Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7):125–128, 2000.

[58] Li-tze Hu and Peter M Bentler. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal*, 6(1):1–55, 1999.

[59] SE NASA. Nasa systems engineering handbook. *National Aeronautics and Space Administration, NASA/SP-2007-6105 Rev1*, 2007.

[60] Gregory Conti and Edward Sobiesk. Malicious interfaces and personalization's uninviting future. *IEEE Security & Privacy*, 7(3), 2009.

[61] John Zager and Robert Zager. Improving cybersecurity through human systems integration. *Journal Article— Aug*, 22(3):41am, 2016.

[62] Benjamin Hadorn, Michèle Courant, and Béat Hirsbrunner. Towards human-centered cyber physical systems: A modeling approach. *Fribourg, Switzerland: University of Fribourg*, 2016.

[63] Ross Anderson. Why information security is hard-an economic perspective. In *Computer security applications conference, 2001. acsac 2001. proceedings 17th annual*, pages 358–365. IEEE, 2001.

[64] Meg Scofield. Benefiting from the nist cybersecurity framework. *Information Management*, 50(2):25, 2016.

[65] G Mani Bharat and M Seetarama Prasad. Fuzzy oriented risk assessment in enterprise information systems. *Journal of Theoretical and Applied Information Technology*, 89(1):236, 2016.

[66] D Henshel, MG Cains, B Hoffman, and T Kelley. Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, 3:1117–1124, 2015.

[67] Bang Nguyen, Jane Hemsley-Brown, and TC Melewar. Branding higher education. *The Routledge Companion to Contemporary Brand Management*, page 407, 2016.

[68] Cormac Herley. Unfalsifiability of security claims. *Proceedings of the National Academy of Sciences*, 113(23):6415–6420, 2016.

[69] Timothy Kelley, Timothy Kelley, Bennett I Bertenthal, and Bennett I Bertenthal. Attention and past behavior, not security knowledge, modulate users decisions to login to insecure websites. *Information & Computer Security*, 24(2):164–176, 2016.

[70] Alexandros Andre Chaaraoui, Francisco Florez-Revuelta, Marian Harbach, Alexander De Luca, Serge Egelman, Tao Dong, Elizabeth F Churchill, Jeffrey Nichols, Matthew Tischer, Zakir Durumeric, et al. Technologies and

applications for active and assisted living. current situation. *IEEE/ACM Transactions on Networking*, 24:2114–2127, 2016.

[71] Eliot R Smith and Diane M Mackie. Group-level emotions. *Current Opinion in Psychology*, 11:15–19, 2016.

[72] Susan Stevens-Adams, Armida Carbajal, Austin Silva, Kevin Nauer, Benjamin Anderson, Theodore Reed, and Chris Forsythe. Enhanced training for cyber situational awareness. In *International Conference on Augmented Cognition*, pages 90–99. Springer, 2013.

[73] Dylan D Schmorrow and Cali M Fidopiastis. *Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience: 10th International Conference, AC 2016, Held as Part of HCI International 2016, Toronto, ON, Canada, July 17-22, 2016, Proceedings*, volume 9744. Springer, 2016.

[74] Kai Jendrian. Der standard iso/iec 27001:2013. *Datenschutz und Datensicherheit - DuD*, 38(8):552–557, 2014.

[75] Cynthia Phillips and Laura Painton Swiler. A graph-based system for network-vulnerability analysis. In *Proceedings of the 1998 workshop on New security paradigms*, pages 71–79. ACM, 1998.

[76] Richard Paul Lippmann and Kyle William Ingols. An annotated review of past papers on attack graphs. Technical report, DTIC Document, 2005.

[77] Barbara Kordy, Ludovic Piètre-Cambacédès, and Patrick Schweitzer. Dag-based attack and defense modeling: Dont miss the forest for the attack trees. *Computer science review*, 13:1–38, 2014.

[78] Xinming Ou, Sudhakar Govindavajhala, and Andrew W Appel. Mulval: A logic-based network security analyzer. In *USENIX security*, 2005.

[79] Sushil Jajodia, Steven Noel, and Brian OBerry. Topological analysis of network attack vulnerability. In *Managing Cyber Threats*, pages 247–266. Springer, 2005.

[80] Michael Lyle Artz. *Netspa: A network security planning architecture.* PhD thesis, Massachusetts Institute of Technology, 2002.

[81] Judea Pearl. Fusion, propagation, and structuring in belief networks. *Artificial intelligence*, 29(3):241–288, 1986.

[82] Steffen L Lauritzen and David J Spiegelhalter. Local computations with probabilities on graphical structures and their application to expert systems. *Journal of the Royal Statistical Society. Series B (Methodological)*, pages 157–224, 1988.

[83] Judea Pearl. *Probabilistic reasoning in intelligent systems: networks of plausible inference.* Morgan Kaufmann, 2014.

[84] Yu Liu and Hong Man. Network vulnerability assessment using bayesian networks. In *Defense and Security*, pages 61–71. International Society for Optics and Photonics, 2005.

[85] Ke Tang, Ming-Tian Zhou, and Wen-Yong Wang. Insider cyber threat situational awareness framwork using dynamic bayesian networks. In *Computer Science & Education, 2009. ICCSE'09. 4th International Conference on*, pages 1146–1150. IEEE, 2009.

[86] Peng Xie, Jason H Li, Xinming Ou, Peng Liu, and Renato Levy. Using bayesian networks for cyber security analysis. In *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pages 211–220. IEEE, 2010.

[87] Robert Cole. *Multi-step attack detection via bayesian modeling under model parameter uncertainty.* PhD thesis, The Pennsylvania State University, 2013.

[88] François-Xavier Aguessy, Olivier Bettan, Gregory Blanc, Vania Conan, and Hervé Debar. Hybrid risk assessment model based on bayesian networks. In *International Workshop on Security*, pages 21–40. Springer, 2016.

[89] Nayot Poolsappasit, Rinku Dewri, and Indrajit Ray. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1):61–74, 2012.

[90] Nizar Kheir, Hervé Debar, Nora Cuppens-Boulahia, Frédéric Cuppens, and Jouni Viinikka. Cost evaluation for intrusion response using dependency graphs. In *Network and Service Security, 2009. N2S'09. International Conference on*, pages 1–6. IEEE, 2009.

[91] Marcel Frigault, Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Measuring network security using dynamic bayesian network. In *Proceedings of the 4th ACM workshop on Quality of protection*, pages 23–30. ACM, 2008.