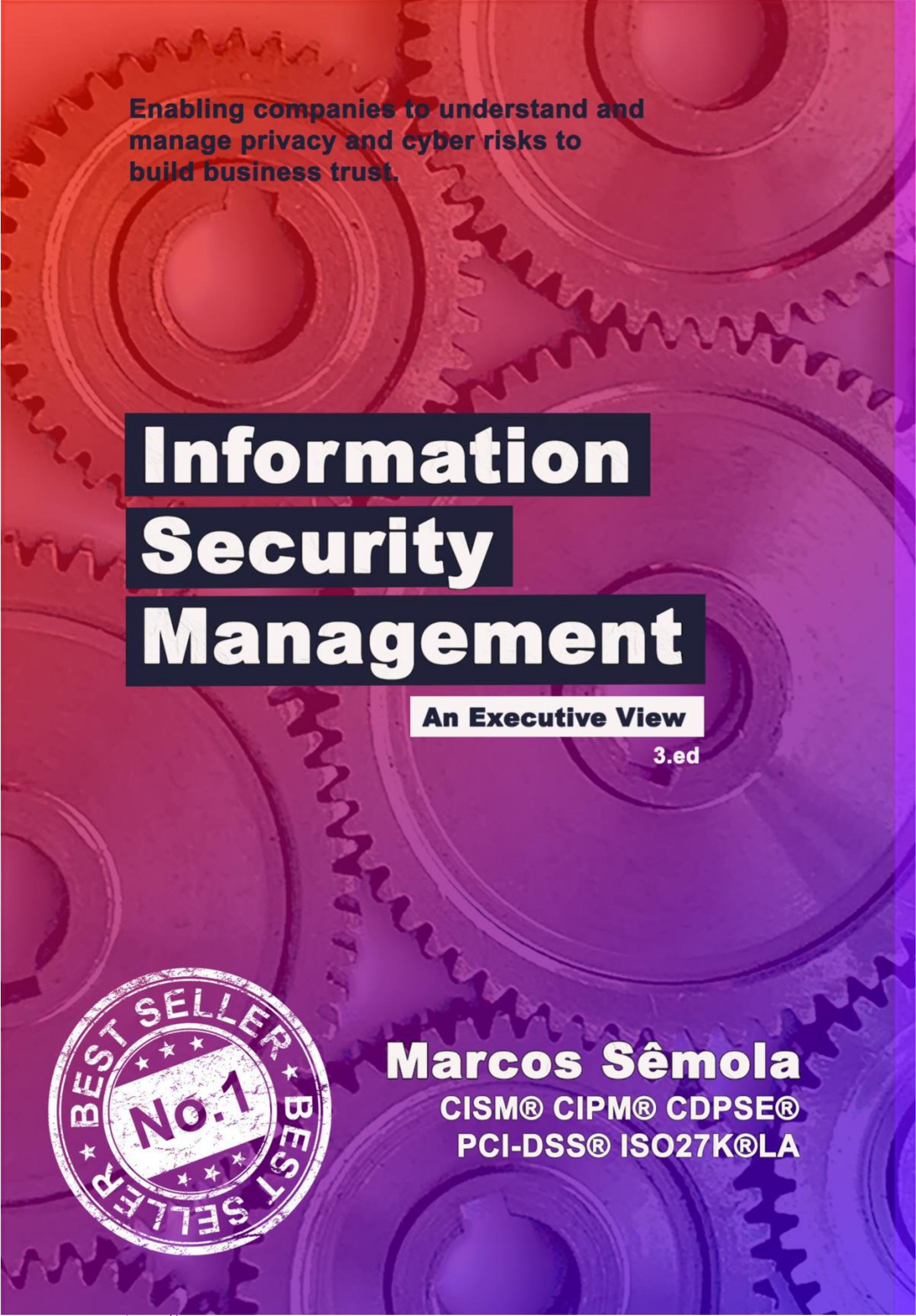


Enabling companies to understand and manage privacy and cyber risks to build business trust.

Information Security Management

An Executive View

3.ed

BEST SELLER No.1 BEST SELLER

Marcos Sêmola

CISM® CIPM® CDPSE®
PCI-DSS® ISO27K®LA

Information Security Management

An Executive View

Information Security Management
An Executive View
Marcos Sêmola

Translation from original version
by Ricardo Bruno Beckman Soares da Cruz

Cover Design by Andrea Hedler
Cover PhotoArt by Marcos Sêmola
Edition and Review by Marcos Sêmola
Author Rights Agent: sssolutions@semola.com.br

International Publication Cataloging Data (CIP)
Brazilian Book Chamber, SP, Brazil
3.ed (English edition). 222 pages. 23cm

Sêmola, Marcos, 1972
Information Security Management: an executive view / Marcos Sêmola; translation Ricardo Cruz.– Rio de Janeiro: Author Edition. 2022. Original title: Gestão de Segurança da Informação: uma visão executiva.

ISBN: 978-65-00-39842-7

1. Computer Science 2.Privacy Rights 3.Information Management 4.Data Protection 5.Information Security I. Cruz, Ricardo II.Title.

22-101483 CDD-658.4038

Acknowledgments

My gratitude for this version translated into English of the book that for years was a best seller in the Brazilian publishing market, goes to each professor, graduate student, master's student, doctoral student, and information risk management professional who welcomed me as an author and embraced the content of this book as a reference for their activities. Thank you for the reputation and authority on the subject that you have kindly been able to build up and endorse over the years.

Content

Preface

I recently had the unpleasant experience of being mugged at the end of a work day. The robber came in asking for my "laptop", in reference to my briefcase, which I thought was discreet and did not look like a traditional laptop briefcase. I argued that I did not have a "laptop" in my briefcase, relieved that I had left mine at home that day, and opened the folder, at his "request", showing the absence of the equipment. He wanted to take the case anyway, so I instinctively asked him to let me keep my notebook. He gave up, asked for my wallet, and then took off on his motorcycle.

Despite the fright and the trauma, I kept thinking about this episode with professional eyes. Of all the items I had with me at the time, perhaps my agenda was among the cheapests. However, because of all my notes and doodles, it was the only item I had risked myself for (insane!), in a tense argument to keep it with me.

Obviously, my life was the highest priority, followed by my personal documents that were in a second wallet and were not taken, but what this episode illustrated was an everyday situation where information was at risk, even though there was no technological device involved.

Extrapolating from this case, I wonder: what if a laptop was taken? Would the owner lose information? Would information contained in it be protected from the eyes of third parties? Could such a robbery be contracted by an unscrupulous competitor?

Of course, this is only one of the many risks to which, unfortunately, both you and I are subject to as long as we live in this imperfect and unfair world. However, let us look a way beyond: how many of us, as professionals, executives, and responsible business people that we are, can say that we manage the risks that our companies and businesses are subject to because they depend on information?

Let us think about our business in relation to information:

- How dependent are we? Can we stay a week without our computers and systems? Which computers and systems cannot stop?

- How sensitive are we? What information cannot fall into the hands of our competitors? What information cannot be made public?

- How well known and trusted are we? Will our reputation be affected if someone change our information, if third parties impersonate us, or if our services would be interrupted without warning?

- Where does the danger lie? In agents outside our business or among our own staff? In deliberate action or in the negligence or inability applied to our our daily routine?

Many people think that information security is all about buying expensive equipment and systems, such as firewalls, intrusion detection systems or antivirus. Others think that it includes the adoption of security policies and the establishment of functional responsibilities to the technological equipment is sufficient. But none of these approaches can prevent losses if they are adopted isolated and inconsequently.

Information security is not an exact science. If we were to classify it, it would be in the field of risk management. Moreover, to manage risks you have to conjugate several verbs: know, plan, act, audit, educate, monitor, learn, and manage are just some of them.

Marcos Sêmola's main contribution to this book is to translate into didactic language several common concepts and common approaches in the field of information security. More than that, the book allows for a global vision of the various aspects involved, introducing the subject to those starting out, and providing a concise and easy-to-understand orientation structure for the more experienced.

The book is intended for people who, like you, who have read this preface so far, are interested in the subject and aware of its importance, and also to those who have not yet awakened to it. As an aid to awareness, this text is a precious gift.

IVAN ALCOFORADO

Principal Director. Information Security Specialist

Production Engineer, Graduated from UFRJ, post-graduate from the Center of Reference in Intelligence (CRIE) of COPPE and consultant in the areas of Knowledge Management and Information Security.

Chapter 1

Knowledge-based Society

1.1 INFORMATION: AN INCREASINGLY VALUED ASSET

Companies have long been influenced by changes and novelties that arise in the market and provoke changes in the context. Discoveries, experiments, concepts, methods and models born from the movement of questioning scholars, researchers and executives who do not conform to the passiveness of life and seek innovation and the breaking of paradigms, revealing - almost frequently, as if we were in a cycle - a promising new trend.

If we go back in history, we will see several phases. From the industrial and electrical revolutions, the opening of the market and the increase in competitiveness provided by globalization, passing by the moments related to process' turn over, to outsourcing, to virtualization and, more recently, to the effects of information technology applied to business in an increasingly wide and deep way. In all these stages information has always been present and has played an important role for business management. Of course, for such analysis, we must consider cultural, market, and even macroeconomic variables of the time, in order to adjust the projection of impacts. Nevertheless, it is undeniable that all companies, regardless of its market segment, core business and size, in all these phases of existence, have always made use of information, aiming to reach higher productivity, cost reduction, gain in market share, increase in agility, competitiveness and more efficient support to the company's decision making processes.

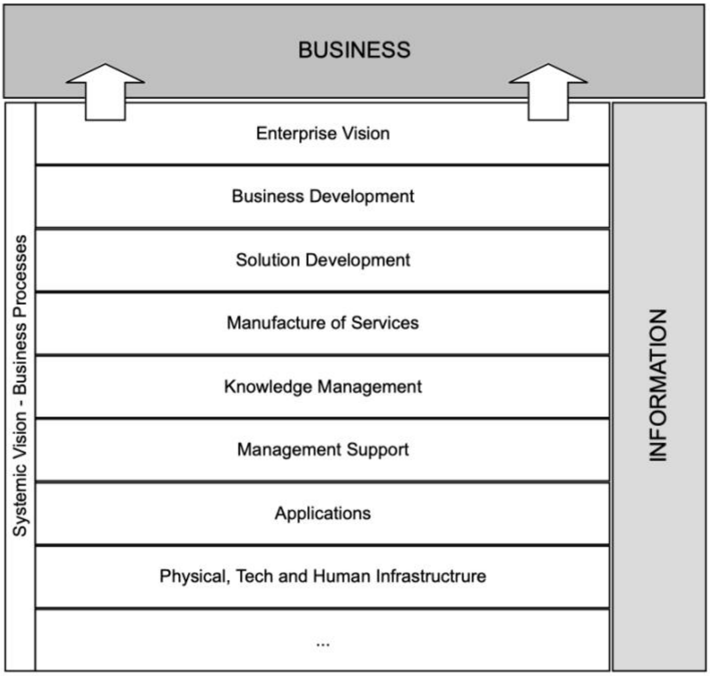


FIGURE 1.1

Omnipresence of information in the main processes of business.

Whether for a supermarket owner concerned with the management, or for a financial institution in search for the automation of its bank branches or for a food industry looking to optimize its production line, they all decide their actions and plans based on information. Business secrets, market and competition analysis, historical operational data, and research are fundamental information and reveal themselves as an important competitive differential linked to the growth and continuity of the business.

1.2 **DEPENDENCE GROWTH**

If we briefly compare the phases of corporate evolution, specifically the way companies used information and managed their business, we will notice clear changes in the tools over the years.

Decades ago, information was handled in a centralized and still not very automated way. Information technology was still crawling and appeared, at first, only as a new and promising new tool, especially considering the initial storage limitations and the prohibitive prices of the first large mainframe computers.

However, the high-tech industry's investments were being amortized and its payoffs were becoming more affordable. Although companies had a lot of information in handwritten documents, in the well-known iron archives, mainframes gradually inherited the function of central data processing and storage. Then we would see terminals spread throughout the company's settings - initially a single one per department - that started to enable consultations remotely.

Sharing information has come to be considered a modern management practice necessary for companies that sought higher speed in their actions. Therefore, the first computer networks emerged and, in parallel, information became more digitized and the processes more automated.

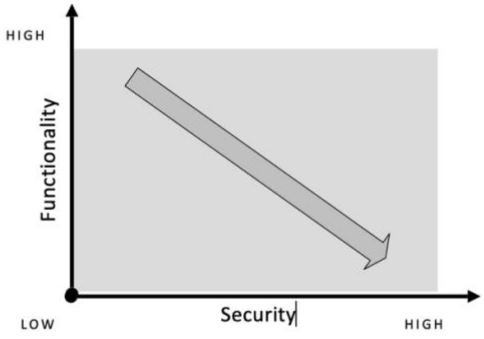


FIGURE 1.2

Direct association between increased operational functionality and the required security.

A few more years and companies were experimenting and applying information technology to business like never before, reaching high levels of connectivity and sharing. The old but surviving mainframes were no longer sole with the task of storing and processing information. Computers took over office environments, broke the paradigm of local access to information and reached anywhere in the world through the World Wide Web: the Internet.

Simultaneously with all this evolution, the corporate network was gaining performance and was also becoming more pulverized. It was to represent the main channel for distribution of internal and external information, and interconnection of environments and processes, culminating with the integration of partners in the production chain.

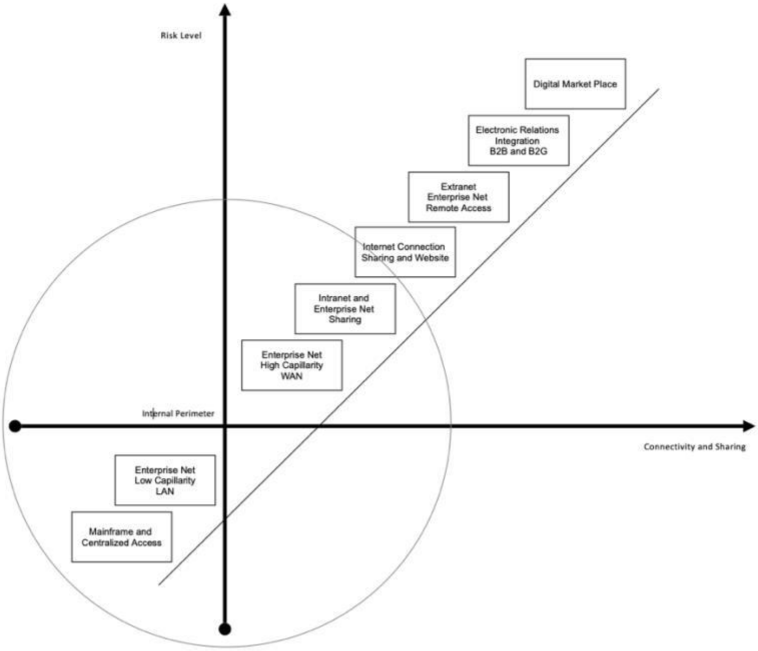

Risk Level
Digital Market Place
Electronic Relations Integration B2B and B2G
Extranet Enterprise Net Remote Access
Internet Connection Sharing and Website
Intranet and Enterprise Net Sharing
Enterprise Net High Capillarity WAN
Internal Perimeter
Connectivity and Sharing
Enterprise Net Low Capillarity LAN
Mainframe and Centralized Access

FIGURE 1.3

Evolution of connectivity and sharing.

The first decade of the 21st century became prodigious in expressions and business applications that have come to make use of modern network and computing infrastructure such as business-to-business, business-to-consumer, business-to-government, e-commerce, e-procurement, and integrated ERP systems (Enterprise Resource Planning). Which promised better organization of business processes, and came to represent one of the main pillars of for the company to reach the dreamed and promising digital marketplace, through which elements of the productive chain, such as suppliers, partners, customers and government, would interact electronically, integrating and sharing their knowledge bases.

Nowadays, Internet access links are becoming increasingly available, and computing power is no problem: "farms" of servers of extremely high performance and capacity are accessible to companies of any size.

Personal computers have evolved to become extremely powerful machines, aided also by the increasingly portable and no less powerful laptops and their similar devices (netbooks, ultra-books), tablets, cell phones and smartphones. We have reached the era of big data, in which massive volumes of information are generated, stored, manipulated, and shared all the time, among all the entities we can imagine. Cloud computing and the convenience of companies paying for storage and processing services for information and systems somewhere they do not quite know where it is, has also become a reality with more and more supporters.

From this, it is possible to assess that if the perception of the high degree of dependence of companies on information - digitized, shared and distributed - and the elements of the infrastructure that maintains it, already attracted attention a few years ago, today, the scene is much more complex and reinforces the need for an even more attentive outlook at the theme.

1.3 HOLISTIC APPROACH TO RISK

Performing an analysis analogous to the human body, it is possible to extract a valuable learning experience in order to ratify the current scenario companies are facing an exponential increase in dependence on information.

Think of the human being as a complex machine, dynamic, unpredictable and subject to physical and emotional changes at any moment, many of them motivated by external factors. Now think about the similarities with your company, subject to the influences of market, macroeconomic, political, sectorial, physical, and technological variables.

Think about the strategic characteristics, challenges, mission, vision, products, and services. As much as other companies may look similar to yours, just like the human body, they all have their differences that make them unique, each with its own personalized characteristics and certainly with different sensibilities.

What would happen to two individuals - apparently alike, if we consider the anatomical similarities of limbs, organs, etc. - consuming too much sugar, one of them diabetic? Would they have equal sensitivities, provoking the same effects?

Now think about your company again. Apparently similar to a competitor because it operates in the same segment, with the same products, and even having similar business processes. Imagine, then, either being contaminated by a computer virus or having the Internet connection shortly lost. Would they have suffered the same effects? Would they have identical financial impacts? I am sure they would not, because each institution has physical, technological and human differences, in addition to the external factors that influence directly and indirectly, interfere in the variations of sensitivity and, consequently, in the resulting impacts.

Finally, think about our limbs. Each one with its function and importance for the maintenance and functioning of our body.

With a similar role, there are the business processes for the company, each one with distinct objectives that, integrated, enable its growth and operation. However, in order for us to have life and to be able to keep the organism alive, we need a vital element: blood. It carries and shares oxygen to every cell scattered throughout the body mass. It carries nourishment to every limb and circulates ceaselessly from head to toe.

Now, the company, due to the high levels of computerization and information sharing, has allowed us to make this comparison...

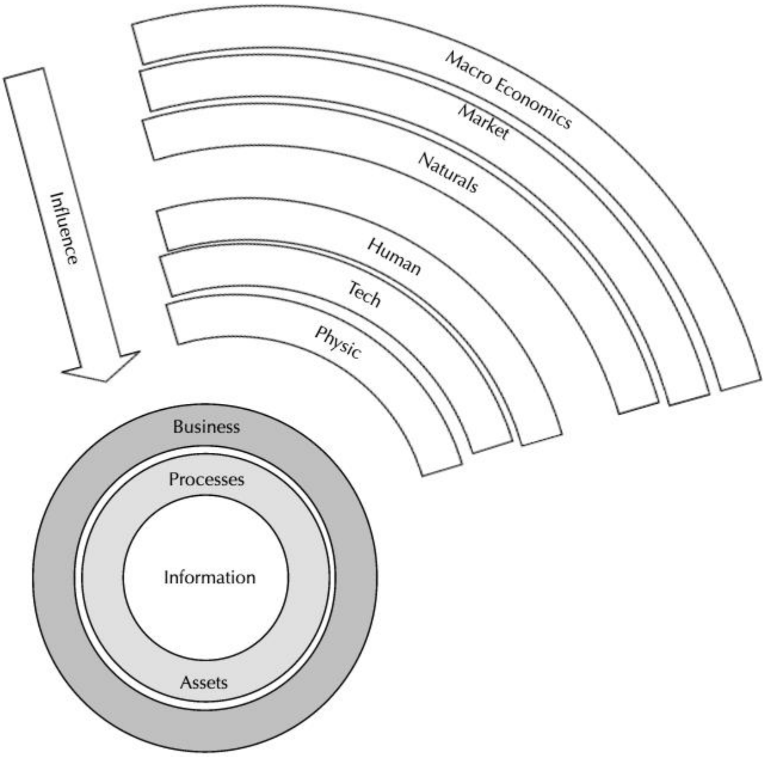


FIGURE 1.4

Influence of internal and external variables that personalize the information security problem.

The company's blood is information. Distributed throughout all business processes, feeding them and circulating through assets (everything that directly or indirectly manipulates information, including information itself), environments and technologies, information fulfills the important role of providing tools for business management. Despite having a large volume temporarily stored and processed centralized in large computers and servers - similar to the heart in the human body - all the information is accessible from the most distant points through the Internet, Intranet, Extranet, VPNs, culminating with wireless access technologies such as Wi-Fi, 3G, 4G and now 5G.

It is easy to realize how the risk level has grown based on this analysis, as the following example suggests.

As an account holder in a banking institution, not so long ago you had to go to a bank branch in order to use your account, because the information was partially shared and only accessible through ATMs or cash machines. This situation simultaneously added greater control and security to the information because it was more centralized. Today, using the same scenario, we are no longer obliged to physically displace ourselves to access our account. Many of the services provided on site are now available over the telephone by simply entering some information - including a password - or via Internet Banking from any Web browser in the world, or still, by cell phone or smartphone.

Notably, these new and modern conditions raise the risk of companies to levels never before experienced, making them realize the need for integrated corporate actions in search of control mechanisms that allow them to reduce the risk and make it manageable and viable.

In the corporate environment, many other risk treatment processes are mature, such as legal risk, credit risk, financial risk, personnel risk, etc. However, there is still much to be done in the field of information risk.

1.4 **AN EXPLOSIVE MIXTURE**

To try to understand and build up a single view of the scenario, we can use a didactic exercise that looks at the security situation experienced by companies as if everything were a food recipe. As if we mixed several ingredients and the result could represent, even if symbolically, a photograph or a diagnosis.
Start by gathering:

- Systematic growth of information digitalization.
- Exponential growth of company connectivity.
- Growth of electronic business-to-business relationships.
- Exponential growth of information sharing.
- Cheapening of computers and other information access devices, facilitating their acquisition.
- Use of personal electronic devices with high interconnection and storage capacity in the workplace and beyond.
- Easy and free broadband Internet access.
- Low level of user identification in access to the Internet.
- High sharing of attack and intrusion techniques.
- Availability of a great diversity of attack and intrusion tools.
- Ease of use of attack and intrusion tools.
- Widespread, confusing, subjective, and unaware of the legal mechanisms of accountability in a virtual environment and the laws that typify computer crimes in the country.
- Mass communication exalting the young invader for the merit of the invasion.
- Creation of the stereotype of the hacker as a genius and hero who succeeded in invasion.
- Misleading association between competitive intelligence and electronic espionage.
- Diversification of threat profiles: competitor, saboteur, profiteer, hacker, dissatisfied employee, etc.

- Growing valorization of information as the main asset of company management.

Mixing the ingredients, safeguarding the due proportions inherent to the peculiar cuisine proposed, we will have as the final product a bitter cake, difficult to digest, and that presents a scenario of great risk, if there is no adequate preparation to manage it in order to make the business operation viable.

1.5 **INFORMATION LIFE CYCLE**

Now we know how valuable information is to the business, however we must go deep to analyse all the aspects connected to security, the properties that must be preserved and protected so that the information would be effectively under control, and especially the moments that are part of its life cycle.

All information is influenced by three main properties: confidentiality, integrity and availability, besides the aspects of authenticity and legality, which complement this influence.[1]

The life cycle, in turn, is composed of and identified by the moments experienced by information that put it at risk. The moments are experienced precisely when physical, technological and human activities make use of information, underpinning processes that, in turn, maintain the operation of the company.

[1] Concepts and aspects will be discussed in due course in a later chapter.

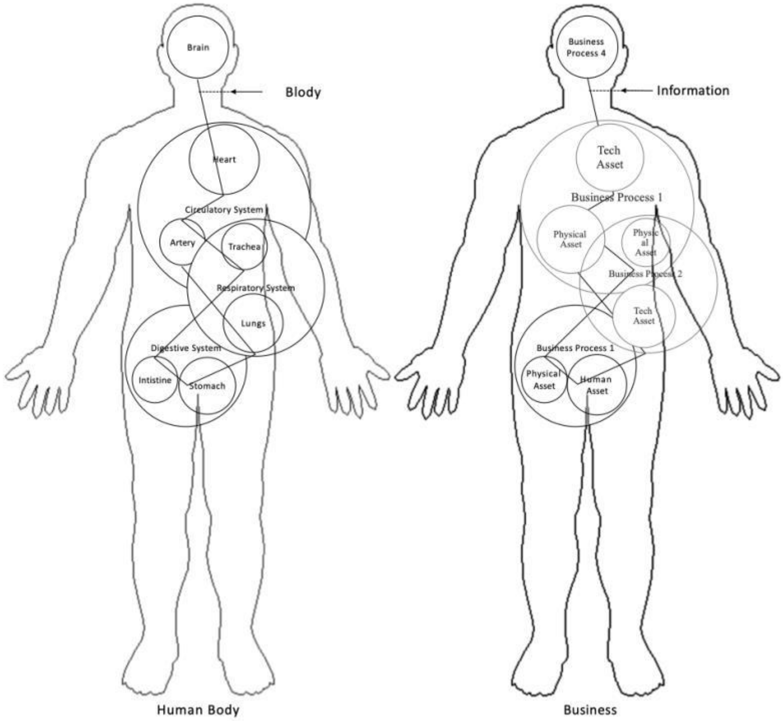


FIGURE 1.5

Analogy with the functioning of the human body.

Again, it is like the functioning of our body, in that organs (analogously, assets: physical, technological, and human) use blood (analogously, information) to run the digestive and respiratory systems, etc. (analogously, business processes) to consequently maintain the individual's consciousness and life (analogously, business continuity).

Corresponding to situations in which information is exposed to threats that put its properties at risk, affecting its security, the diagram reveals all four moments of the life cycle that are worthy of attention.

Regardless of how information is represented - be it atoms or bits - all moments apply.

Handling

The moment in which information is created and manipulated, by flipping through a stack of papers, typing newly generated information into an Internet application, or when using a password for authentication, for example.

Storage

The moment when information is stored, either in a shared database or in a paper annotation that is later posted to an iron file, or even to a CD-ROM, DVD-ROM, or flash drive deposited in a desk drawer, for example.

Transport

The moment when information is transported, either by forwarding information by electronic mail (e-mail), or by posting it on an Internet system, or when talking on the phone about confidential information, for example.

Disposal

The moment when information is discarded, either when depositing in the company's trashcan a printed material, or when eliminating an electronic file from your computer or, yet, discarding a used CD-ROM that failed to read.

Now think about security as a whole, where the target is information. What good would it do to secure three of the four concepts?

Imagine... You generate, in a meeting, a new definition: confidential strategic information. It is written down on paper and stored later in an appropriate safe. At the moment immediately afterwards, you task the secretary with to type this information and send it by e-mail to those involved. Consider now that, after completing the task, the secretary has not adopted the appropriate disposal and, consequently, has thrown, without any criterion or treatment, the original paper material in the nearest rubbish bin. At this very moment, a vulnerability or security hole has been installed! Now imagine that there is effectively a potential threat ready to exploit this vulnerability. For example: another employee on the physical perimeter of the desk is interested, but who has not attended the meeting and has obscure objectives.

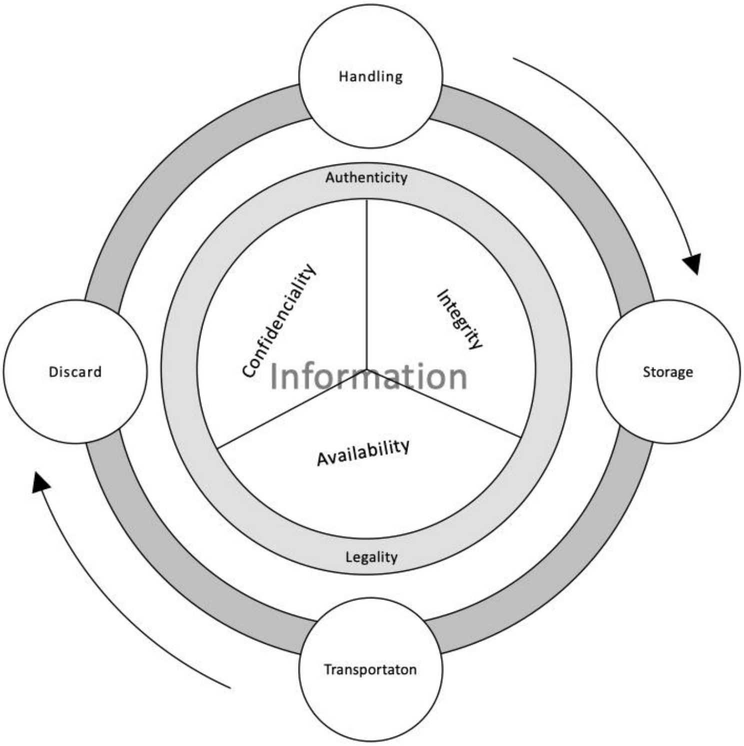


FIGURE 1.6

Four moments of the information life cycle, considering the basic concepts of security and complementary aspects.

That's it! No matter how much you have adopted a controlled behavior aligned with the security policy in the moments of handling, storage and transport, the information, target and reason for all the work, was exposed at the moment of disposal, compromising all the others and also putting the entire security of the business security at risk (see Figure 1.6).

Chapter 2

Challenges

2.1 ANATOMY OF THE PROBLEM

In any solution initiative, it is necessary to first identify the problem in fine detail and to segment it in such a way as to allow for a deeper analysis of its characteristics. When the matter is information security, this challenge grows exponentially, because there are many factors associated with the theme.

We have to understand that the target is information and that it is no longer confined to specific physical environments or to isolated processes. Information now circulates throughout the company and even outside the company, considering the virtual, which today far exceeds the physical ones, feeds all business processes and is subject to various threats, security holes or vulnerabilities, and is sensitive to specific impacts.

The company has become one big web of integrated communication, dependent on the flow of information that is distributed and shared through it. This same information, now subject to vulnerabilities that transcend technological aspects, are also targets of interference caused by physical and human aspects.

Today, many companies and their executives are surprised by this statement, because they still maintain a deficiency of perception of the problem that I usually call "iceberg view". I sympathize with this label because it looks a lot like the problem. The portion of ice that we see outside the waterline is commonly only about 1/7th of the entire block of ice that remains submerged and therefore hidden from our eyes. This is precisely the similarity.

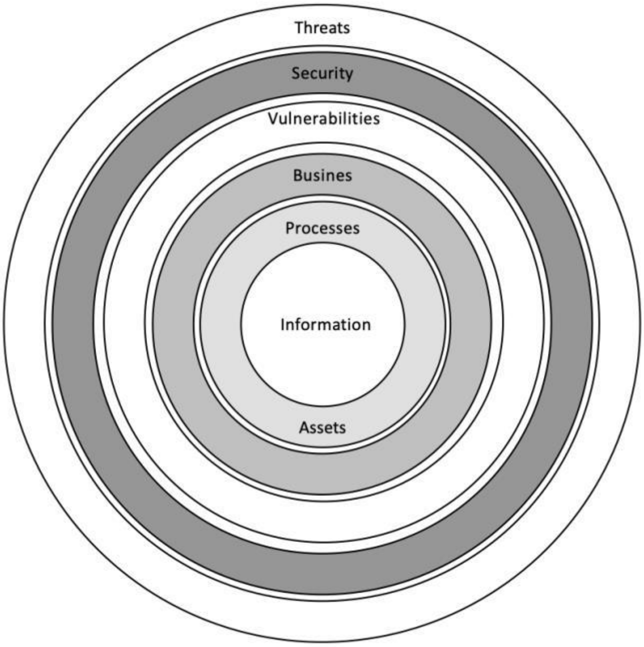


FIGURE 2.1

Perimeters. The target is information.

Commonly, a big part of the market and its executives have this "myopia", perceiving only a small fraction of the security problem: the technological aspects. They usually associate the risks only with networks, computers, viruses, hackers and the Internet, whereas there are still many others, just as important and relevant to business security.

It is a critical success factor for the anatomy of the problem that identifying the internal and external elements that interfere with information security risks. It is the moment to map the physical, technological and human characteristics of the company, the market where it operates, competitors, in addition to considering the plans and strategic business definitions.

Once again using the analogy with the human body, we can compare the doctor's role in consulting the patient before prescribing treatment to the challenge of defining and modeling an information security solution for the enterprise.

The professional needs to perform a series of examinations of the patient's current situation, although the patient may have symptoms similar to other patients, the origin may be different. All of this with the objective of equating the problem and recommending appropriate treatment and medication that will specifically treat the illness. Also in this dimension, we have to consider the possibility of a mistaken treatment or medication. A high dose could generate side effects, and a lower dose might not cure the patient.

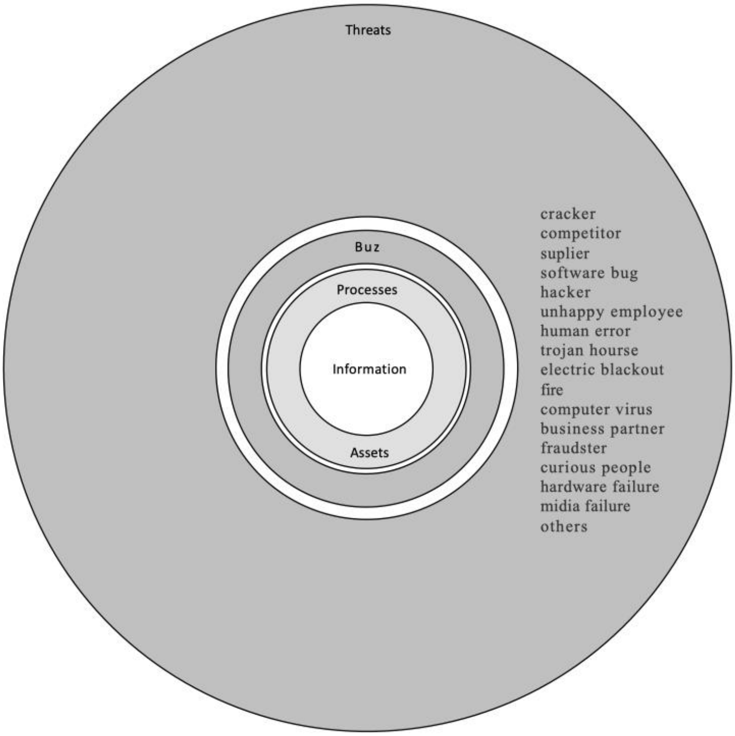


FIGURE 2.2

Diversity overview of the threats that put the business at risk.

In the company, the situation is similar. The challenge is to carry out actions that map and identify the company's current situation, its threats, vulnerabilities, risks, sensitivities, and impacts, in order to allow the adequate dimensioning and modeling of the solution. What happens to the medicine happens to the company. Each company has particular characteristics that will lead to the application of a customized solution capable of bringing to a security level that is also customized.

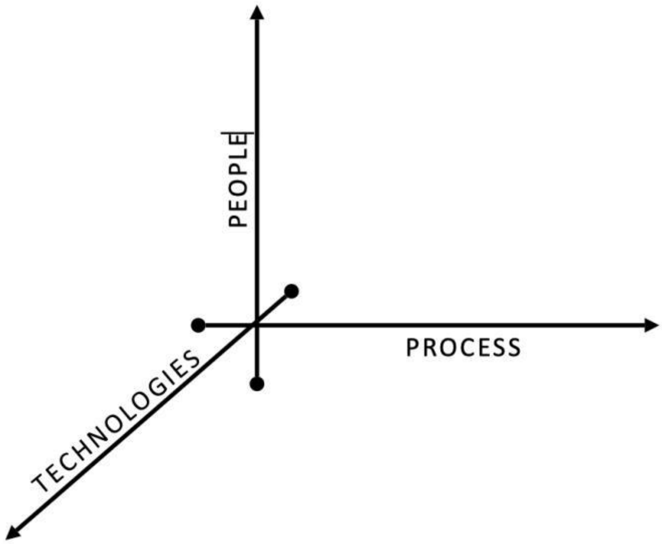


FIGURE 2.3

Macro aspects considered in the analysis of the security context.

Differently to what many people think, there is no such thing as total security, and, based on the example, each company will need a distinct level of it. If the level is too high, it can generate side effects such as loss of speed due to bureaucratization of processes, loss of time-to-market, dissatisfaction of customers and partners, and even the disinterest of potential investors.

Therefore, the myth that it is possible to operate with zero risk falls apart. There will always be risk, and it must be adjusted to the nature of the business, considering all the internal and external variables previously mentioned in order to make the company's operation feasible.

2.2 **CORPORATE VISION**

Why do I need security? Have you ever asked yourself this question? Have you ever stopped for at least ten minutes to evaluate and verify why you need security?

Let's take a short and common example from our daily life to better understand what we are talking about and also how we end up replicating personal errors in our professional activities, taking them to the company.

Think about your residence, a house or apartment that, in most cases, has only two entrance doors, usually called the social door and the service door. They play an important role. Have you ever stopped to think about this? Do you know what it is?

Assuming that your behavior regarding this question follows the great majority of people, you have never really stopped for even a few minutes to evaluate the importance and the role that doors play. For they are devices installed to provide physical access to your apartment. They are control mechanisms that can be opened and closed according to the owner's will, allowing or preventing access to the interior of your residence.

Generally speaking, doors offer resistance to those who insist on physically accessing your environment and, consequently, protect all the other assets that are inside. Do not think only of burglary attempts; after all, who has never found itself in the situation of having forgotten the key to one's own home?

The essence of this comparison lies in the inconsistency of these controls, commonly found in most homes. Follow the reasoning.

You have documents, computer equipment, furniture, appliances, clothes, jewelry, and even cash. Besides material goods, you still keep inside the people you love: your family.

The curious thing is that, despite being the mechanisms that protect and offer resistance and, consequently, security to your main assets, the doors of the residences do not have the same physical access mechanisms, the same locks and alarms, or are not even made of the same material. This reveals that social and service doors end up offering different levels of security and that, therefore, the investments have not been distributed adequately, resulting in a lower return than normally expected.

What is the point of having two locks on the social door if the other, which allows access to the same environment, has only one?

What we see here are two points with common objectives, but fulfilling them in a different and unbalanced way. It is like going on vacation, calibrating three tires of the car and forgetting the fourth one empty or flat.

If we make simple and impactful mistakes like these at home, we would not be replicating them when practicing information security within our companies?

Wouldn't your security team be focused only on the technological aspects of security and, consequently forgetting the physical and human aspects?

Are the investments made in security aligned with the strategic objectives of the company in order to the best return on investment?

Are your actions guided by a security master plan or do they continue to occur according to reactive demands?

Is your company operating on high-risk ground, encouraged by control mechanisms that give you a false feeling of security, despite continuing to have the "doors locked" but the "windows still open"?

The level of security of a company is directly associated with the security offered by the weakest "door". Therefore, it is necessary to have a corporate vision capable of enabling a consistent and comprehensive action, leading the company to achieve the appropriate level of security for the nature of the business.

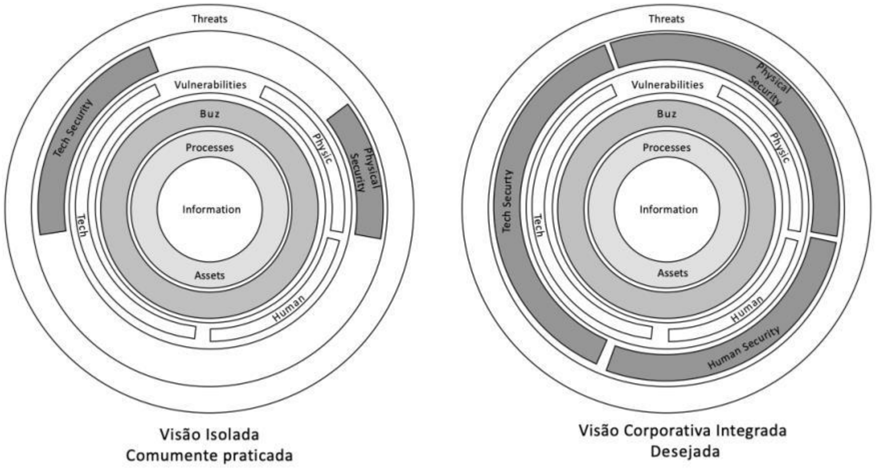


FIGURE 2.4

Current versus desired scenario: coverage of the solution security considering all three aspects.

Vulnerabilities × Threats

All the time, businesses, their processes, physical, technological, and human assets are subject to onslaughts by threats of all kinds, which seek to identify a compatible weak point, a vulnerability capable of potentiating their action. When this possibility appears, the security breach is consummated.

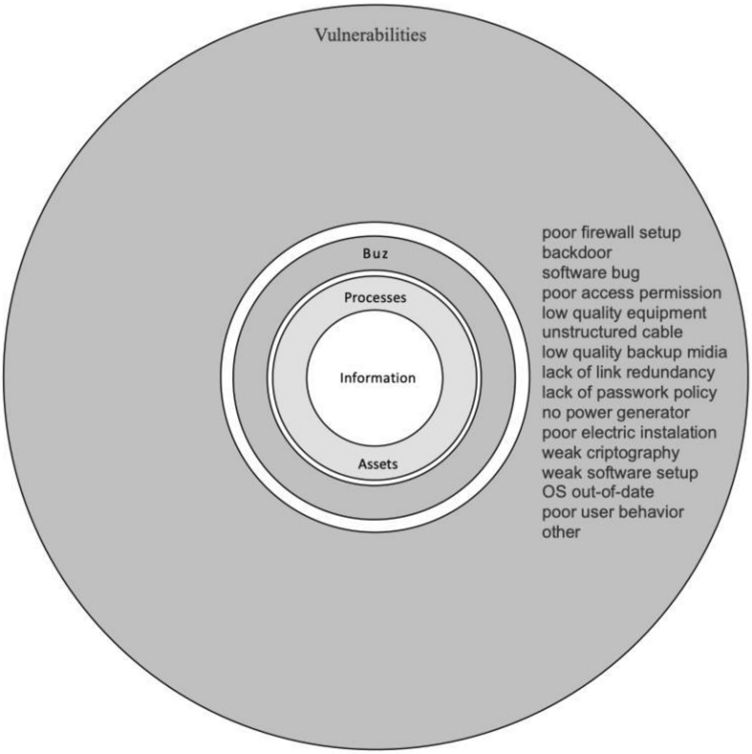


FIGURE 2.5

Diversity overview of vulnerabilities that expose the business to associated threats.

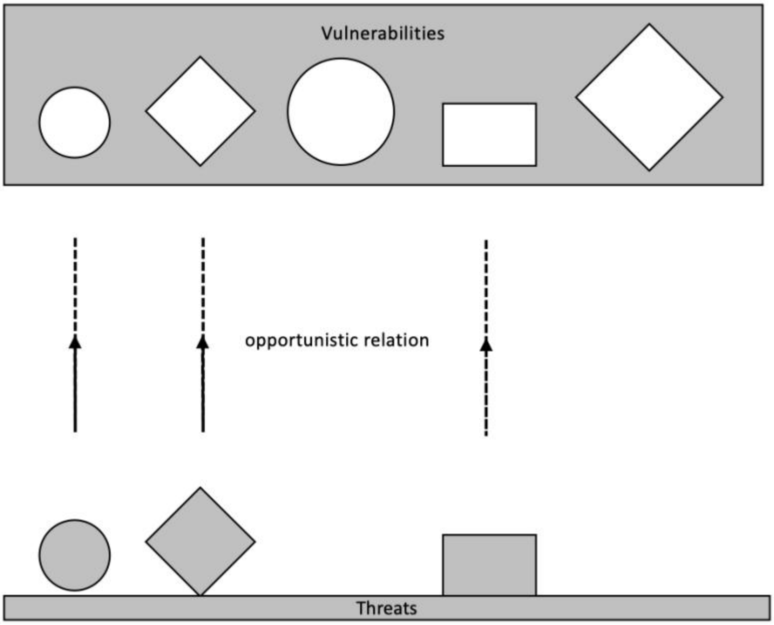


FIGURE 2.6

Like pieces that fit together, specific threats exploit compatible vulnerabilities.

2.3 **SINS COMMITTED**

There are many mistakes commonly made when thinking about information security, caused by the myopic view of the problem and the distorted perception of the issue. It is easy to understand this mistake when we compare it to an iceberg; that is right, that big block of ice that floats loose in the ocean. Well, you should know that what is seen out of the water corresponds only to a small top of the whole block, about 15%; therefore, there is much more ice underwater that cannot be seen. This is exactly the way many people perceive the security aspects, considering and seeing only the problems associated with technology, more precisely Internet, networks, computers, e-mail, viruses, and hackers. Because of this partial understanding many sins are committed that reflect negatively on the business.

- Assigning exclusively to the technological area the responsibility over information security.
- Hierarchically position this team below the IT executive board and think that this is the definitive position.
- Defining investments that are underestimated and limited to the scope of this board.
- Elaborate action plans oriented to reactivity.
- Not realizing the direct interference of security with the business.
- Treating activities as expenses and not as investment.
- Adopting specific tools as a palliative measure.
- To be satisfied with the feeling of security provoked by isolated actions.
- Not to corporately cultivate the culture of risk management.
- To treat security as a project and not as a process.

2.4 **RAISING EXECUTIVE BODY AWARENESS**

Due to the fact that it is a widespread and corporate problem involving the physical, technological and human aspects that underpins the operation of the business, it becomes a sine qua non condition that work begins in the top down format, that is, mobilizing the executives of the company's board for only later reach the others in the hierarchy. This condition is fundamental, because there will be no possibility of simultaneously and equally reaching the vulnerabilities of all the company's distributed environments and processes if there is no coordinated action, and above all, supported by the top.

Support is not only the awareness and adequate perception of risks and associated problems, but also the consequent prioritization of actions and budgetary definition to an adequate level.

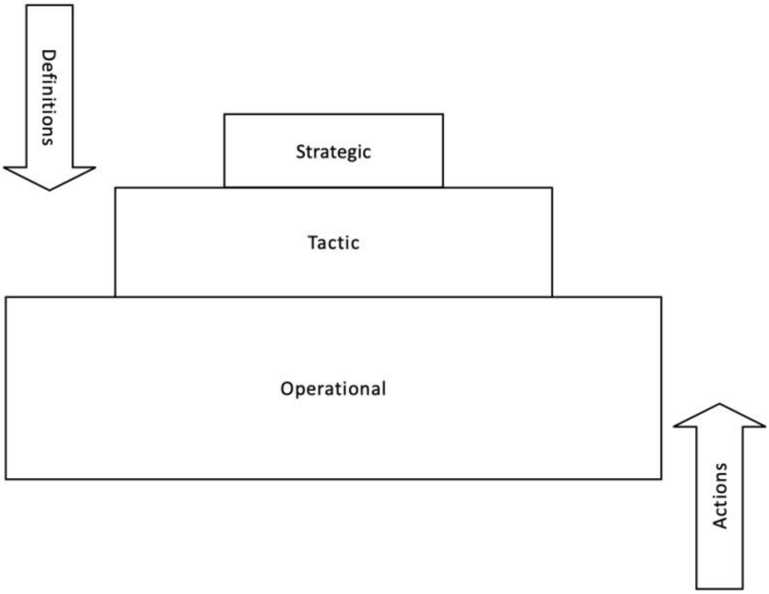


FIGURE 2.7

Action coordinated by strategic definitions resulting in operational actions.

It is not an easy task to find an adequate language and elements capable of translating in an executive way the investment needs and, above all, the benefits directly related to security. After all, there is a high degree of subjectivity in the actions, besides it is an investment that usually does not materialize easily and only shows a return when there is some event that puts the control mechanisms to the test.

Despite this, some successful experiences, previously lived by executives, today corroborate the challenge of security due to their similarity and convergence. At the time of the challenge to reduce the risks posed by the year 2000 bug, the entire high echelon was involved and made aware of the risks and the need to invest in order to overcome the threat. Analysis was performed and important characteristics were extracted that also apply to information security. The same occurred when they sought to organize their corporate management system in an integrated manner, through ERP (Enterprise Resource Planning) systems, when it came to the quality standards provided by ISO 9001 certification.

The Year 2000 Bug

- Widespread problem
- Corporate Action
- Compliance

ERP

- Strategic vision
- Process change
- Centralized control

ISO 9001

- Senior management awareness
- Creation of standards and procedures
- Implementation, certification and administration

In time to solve the systems problem for the turn of the year 2000, they concluded that it was a widespread needed corporate action, and that they needed to be complacent about the bug. When it came time to optimize their management model with ERP solutions, they concluded with the analysis that, to be successful, they needed to have a strategic vision, change and adapt processes, and still maintain centralized control. In the ISO quality certification initiative, they realized the dependence of senior management awareness, the creation of standards and procedures, certification, implementation, and constant management.

These nine points, identified as critical success factors in different actions, are equally important in overcoming the security challenge and configure mental models already experienced and absorbed by the executives that face the challenge of information security.

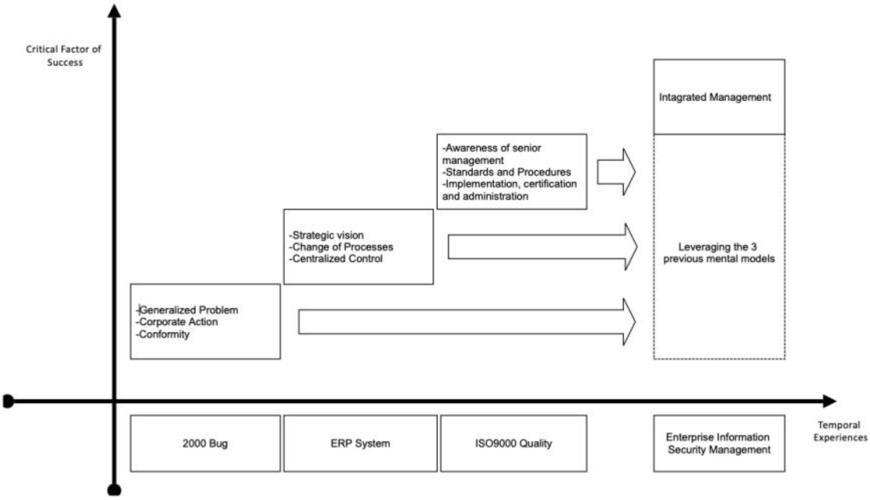

Critical Factor of Success
Intagrated Management
-Awareness of senior management
-Standards and Procedures
-Implementation, certification and administration
-Strategic vision
-Change of Processes
-Centralized Control
Leveraging the 3 previous mental models
-Generalized Problem
-Corporate Action
-Conformity
2000 Bug
ERP System
ISO9000 Quality
Enterprise Information Security Management
Temporal Experiences

FIGURE 2.8

Absorbing mental models.

Moreover, in order to achieve the appropriate level of awareness among the executive body, you cannot give up the ROI (return on investment) exercise. It is the language most closely linked to the executive profile of cost profitability, revenue, profit, dividends, gain in market share and share of mind, and stock price appreciation.

2.5 **RETURN ON INVESTMENT**

ROI (return on investment) is an ancient tool, old known to entrepreneurs, investors, and executives attentive to the market and opportunities. It is built by cross-referencing real data related to direct, indirect and intangible costs, with the projection of investments, it becomes a great instrument to guide the actions of these executives.

It seems, at first, an essential instrument to support decision-making, and it really is. By analyzing it, one can often justify high investments, changes in direction and strategy; after all, it becomes possible to project the return on investment.

There is not a unique ROI model, nor is there a right or wrong model. What exists are different approaches and views of the same object. The depth of the analysis directly interferes in this model, adding an even greater number of variables and refinements. However, they all seek a magic answer to the question: should I make this investment?

It may sound strange to many, but the same question also applies to investments in the technological area, did you know? It became in the past when investments of this kind were seen as a "necessary evil". It was a time when large acquisitions - state-of-the-art technology - were made and were not concerned with measuring results, projecting the time to reap the laurels of the investment. It was the time when these expenses (as investments were seen) would be passed on through the product or service to the final consumer, or diluted in adventures in the financial circuits.

Now the time has come to plan, design, measure, and charge the results of the integration between technology and business. However, it is also time to exercise ROI more in subcategories, with more detail. It is not enough to model a macro technological ROI; we must address more specific technologies and problems, such as information security.

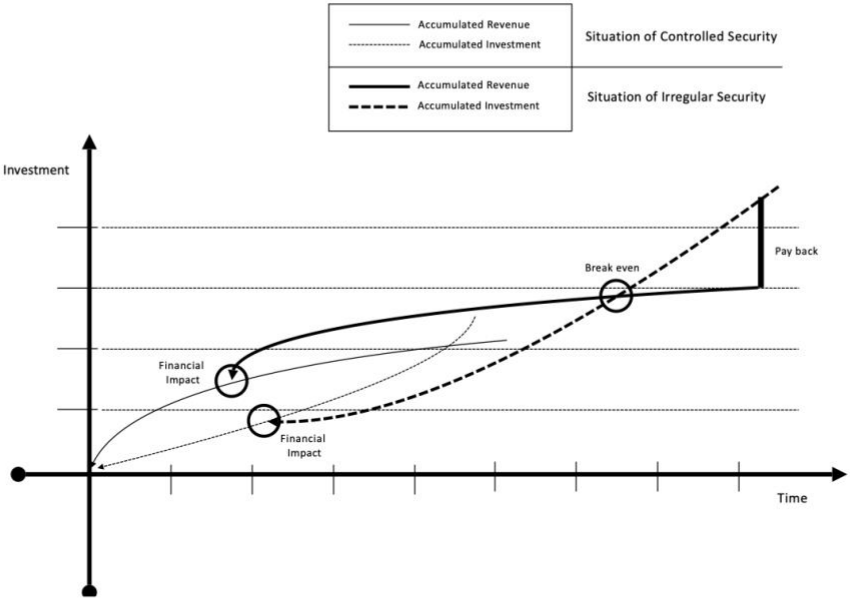


FIGURE 2.9

Analysis of the consequences of delayed payback on ROI, arising from the absence of a security process.

The bottleneck of this work is notoriously understanding, knowing and mapping the corporate problems because, without this information, it would not be possible to develop a tool to be coherent, reliable, and ready to support prioritization of actions and decision-making.

Security ROI especially has many enlightening answers that help us reverse the old image of expense, converting it into investment.

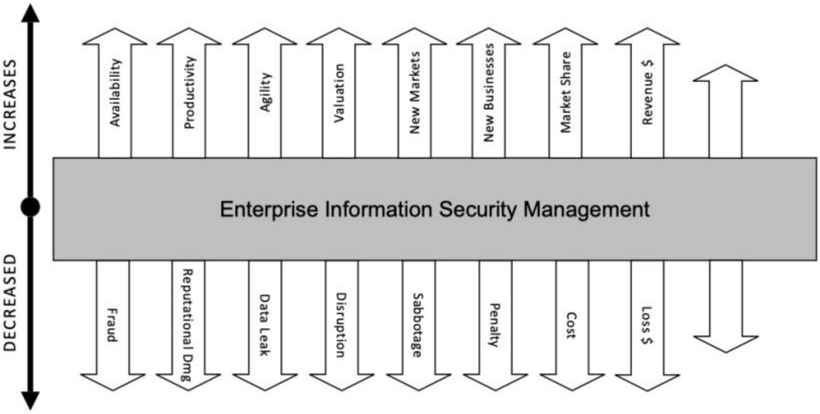


FIGURE 2.10

Security ROI insights.

Let's exercise by dealing with direct costs first. If we cross-reference the number of computer virus contaminations in a year, the percentage of employees affected, the time lost with the downtime and the cost worker/hour, we will perceive the direct impact on the business.

When we analyze the work time consumed by employees with free access to the Internet, accessing information that is not associated with the professional activity, and again worker/hour cost, we will be able to project the impact on the productivity of human resources.

If, during a disaster, a service is unavailable - for example, Internet Banking - multiply the number of account holders who access it per hour, the savings that the company has by the fact that its account holders avoid the branches and migrate to the Internet, and then you have the direct impact.

Speaking now of indirect impacts, using the same situations, we can highlight the costs related to the mobilization of teams to remove the viruses that have infected the computers on the network, the time it takes to remove the viruses, the time required to reconstruct files and information that was lost due to the contamination, and also possible restorations of backup copies (if any). Following the previous examples, the indiscriminate and uncontrolled access to the Internet can cause an overload of the network bandwidth, anticipating investments and causing unavailability. In addition, it can allow virus contamination of the entire network by running programs copied from the Internet, and worse: expose the company to legal sanctions related to software piracy, pedophilia and cybercrime.

The problems do not end there: The unavailability of service can deeply affect you and your customer. First you, because the customer has not been able to perform a financial transaction, an investment, a credit card application, etc. Now the customer, who will have to be repaired through a telemarketing call, direct marketing campaigns, etc.

Now comes the worst. Intangible and incalculable costs that truly jeopardize the continuity of the business. The impact of an invasion, whether internal or external, causing information theft, is not easy to calculate. Many times, it is not known what has happened to the information, and even less how it will be explored. Will it be in the hands of a competitor? Or in the hands of the press, ready for a scoop?

This is a problem without a defined dimension. The impact to image is a serious and costly thing to be reversed. Much more resources are spent trying to rebuild a solid image, secure, efficient and committed to the client than what was spent to build it.

We still have to think about the new business that will come and that will depend on security for their viability. After all, what company would not want to be the enterprise that makes it happen instead of just watching it happen?

The ROI study is definitely part of the day-to-day life of technology, executives, and information security in particular is already a meeting agenda and more than enough reason to be considered an investment. It remains, first of all, to generate and implement control mechanisms that, preliminarily, gather information that signals the events in which there is a security breach and record the effects over time. With these numbers, added to projections and simulations, it will be possible to generate a ROI study capable of translating into executive language what really needs to be understood: security is an important, necessary, measurable, and justifiable investment.

It is very important to emphasize, at this point, that every investment has its inflection point, that is, a point on the curve where the return is no longer proportional to the effort employed. This situation is undesirable and must be the target of attention to avoid its occurrence. It would be the same as investing in security an amount greater than the value of the protected asset itself, considering and weighing, of course, all the aspects associated with the operation of the business.

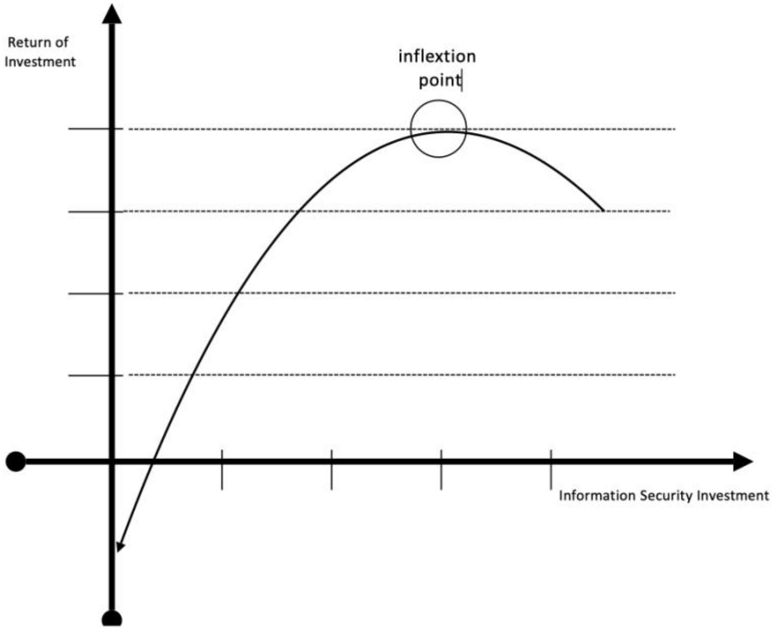


FIGURE 2.11

Analysis of the inflection point of security investments × ROI.

2.6 HIERARCHICAL POSITIONING

Given the scope of the challenges associated with information security, it is essential to reorganize the hierarchical structure of the company in order to meet the new demands. It is common to have immediate confusion when associating the activities and responsibility of security management to the technological area. Many companies insist on relating, and many times encapsulate, the security budget and actions to the IT master plan or IT strategic plan.

If we consider the diversity of vulnerabilities, threats and impacts that affect all the environments and processes of the company, we will realize that this model does not fulfill the role. This way, the company would have a security coordination focused on the technological aspect, certainly important, but not the only one to require attention, because the other physical and human aspects would be forgotten and allow the risks.

The actions need to be closely aligned with the strategic guidelines of the company and, for this, it is necessary to have a corporate, global, and broad vision, capable of creating synergy among the activities and, especially, a greater return on investment. The latter is achieved mainly by eliminating redundant, and many times conflicting, actions that depreciate the corporate information security plan.

Inheriting the importance and participation already practiced by the executive board, a corporate information security committee must be created. Positioned at the second level, next to the executive board, that brings together the CIO, CEO, and counselors, this unit should be multi-departmental, coordinated and mediated by the Security Officer, but with strong representativeness of the company's directorships.

Considering the size and the organizational model of the company the creation of interdepartmental security committees may be necessary, which will report to the corporate committee, these driven by representatives with a managerial profile - in tune with the Security Officer - that will be segmenting the actions from tactical operational activities. Simultaneously, will act as consolidators of partial and final results, performing functions of coordination, control, planning/evaluation, and execution, making them available to the corporate committee, in order to feed back the management process.

2.7 **MANAGING CHANGES**

Change is the only certainty. This sentence is already more than worn out, but it is still valid when applied to the challenge of companies in the face of information security.

There are many variables that directly and indirectly interfere on operational risks of the business: market changes, new marketplaces, technological innovations, physical expansion and growth of human resources are examples that end up in the risk equation, making it oscillate and move out of its equilibrium point (see Figure 2.13).

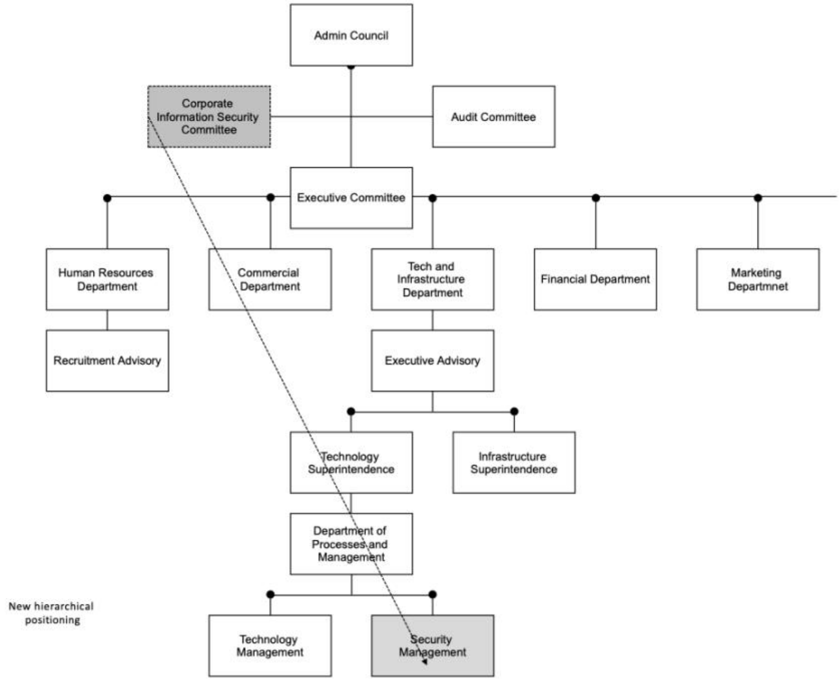

Admin Council
Corporate Information Security Committee
Audit Committee
Executive Committee
Human Resources Department
Commercial Department
Tech and Infrastructure Department
Financial Department
Marketing Departmnet
Recruitment Advisory
Executive Advisory
Technology Superintendence
Infrastructure Superintendence
Department of Processes and Management
New hierarchical positioning
Technology Management
Security Management

FIGURE 2.12

Hierarchical positioning appropriate to the challenges with corporate breadth.

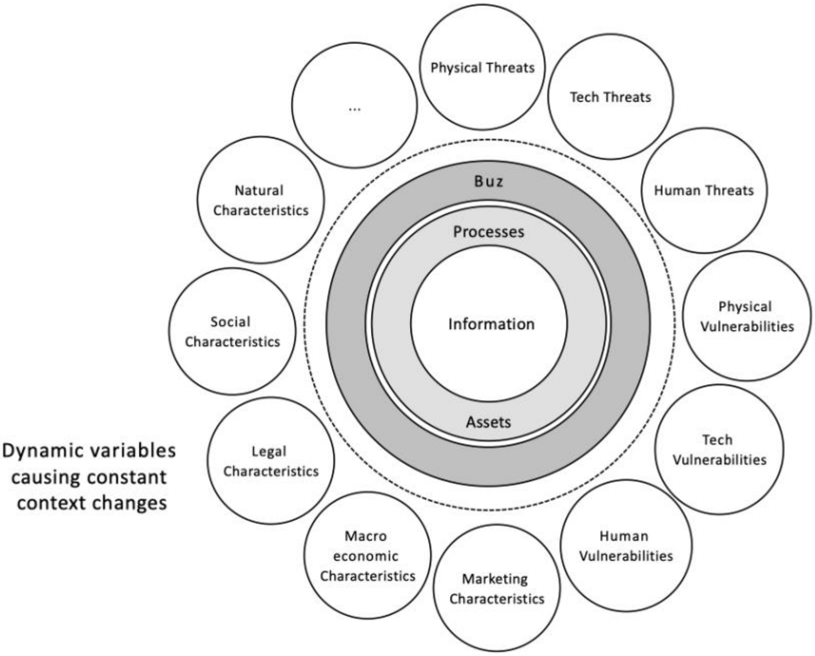


FIGURE 2.13

Perception of the dynamism of the context in which the company is inserted.

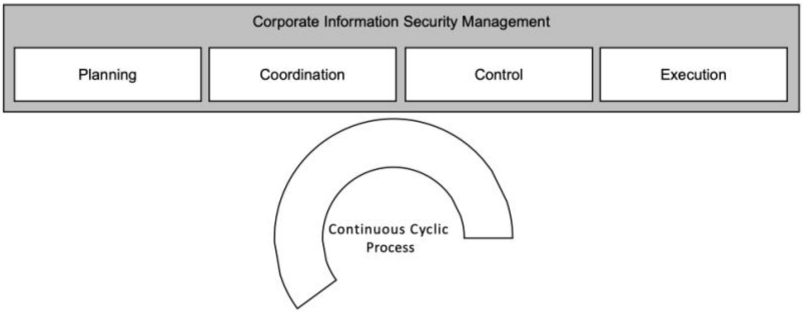

Corporate Information Security Management
Planning
Coordination
Control
Execution
Continuous Cyclic Process

FIGURE 2.14

Macro view of the management process.

Faced with the dynamism of these variables, many of which are unpredictable and uncontrollable, companies would not let themselves be trapped for being backed by a security solution that represents a project with beginning, middle, and end. They will all need something equally dynamic, a process that can keep pace with the changing environment at speed and adjust controls to maintain the appropriate level of risk.

The security they all must strive for must be maintained by a true information security management process, supported by feedback-loaded subprocesses that interact all the time with the variables and are constantly being adjusted to the strategic guidelines of the business.

Think about your company. Couldn't it be happening now with a new hire of human resources, the upgrade or update of a server and its operating system? The implementation of a new management system, application, Internet connection, or even the occupation of a new commercial room or building? Couldn't you be suffering the effects of upcoming dangerous storms or the appearance of a new, voracious competitor? These facts would represent changes that would interfere with your operational risks, generating the need for a thorough analysis of the reflexes that would later serve to support the definition of the next actions. You need a corporate information security management model!

2.8 **CORPORATE SECURITY MANAGEMENT MODEL**

It is not just to create a new department or administrative unit and call it a corporate information security committee. It is necessary to have a clear vision of all the steps that make up the corporate security challenge and formalize the processes that will give life and dynamism to management.

We are talking about a corporate information security management model that is cyclic and chained, formed by stages:

- Corporate Information Security Committee
- Security Mapping
- Security Strategy
- Security Planning
- Security Implementation
- Security Management
- Supply Chain Security

Each of these stages plays an important role in the cycle and generates final results that should be properly formatted and ready to feed the subsequent stage. This way it will be possible to quickly react to the changes that will inevitably occur in the business operation, making the risk oscillate.

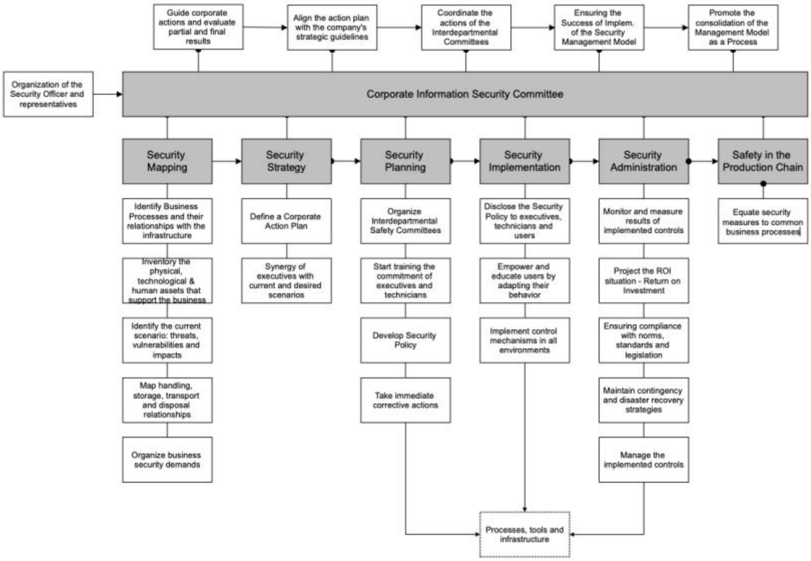

Guide corporate actions and evaluate partial and final results
Align the action plan with the company's strategic guidelines
Coordinate the actions of the Interdepartmental Committees
Ensuring the Success of Implem. of the Security Management Model
Promote the consolidation of the Management Model as a Process
Organization of the Security Officer and representatives
Corporate Information Security Committee
Security Mapping
Security Strategy
Security Planning
Security Implementation
Security Administration
Safety in the Production Chain
Identify Business Processes and their relationships with the infrastructure
Inventory the physical, technological & human assets that support the business
Identify the current scenario: threats, vulnerabilities and impacts
Map handling, storage, transport and disposal relationships
Organize business security demands
Define a Corporate Action Plan
Synergy of executives with current and desired scenarios
Organize Interdepartmental Safety Committees
Start training the commitment of executives and technicians
Develop Security Policy
Take immediate corrective actions
Disclose the Security Policy to executives, technicians and users
Empower and educate users by adapting their behavior
Implement control mechanisms in all environments
Monitor and measure results of implemented controls
Project the ROI situation - Return on Investment
Ensuring compliance with norms, standards and legislation
Maintain contingency and disaster recovery strategies
Manage the implemented controls
Equate security measures to common business processes
Processes, tools and infrastructure

FIGURE 2.15

Diagram of the corporate information security management model.

Corporate Information Security Committee

- To guide the corporate security actions and all the stages of the model, in addition to measuring partial and final results in order to repair focus deviations.
- Align the action plan with the strategic guidelines of the business, seeking to add value and make feasible the best return on return on investment.
- Coordinate the security agents in their interdepartmental committees, in order to attune them to possible adjustments in the action plan.
- Ensure the successful implementation of the corporate information security management model, which will prepare and give autonomy to the company to manage its current and future associated challenges.
- Promote the consolidation of the corporate information security management model as a dynamic, self-managed process.

Security Mapping

- Inventorying the physical, technological, human and environmental assets that support the company's operation also considering the other internal and external variables that interfere in the company's risks, such as niche, competition, expansion, etc.
- To identify the degree of relevance and the direct and and indirect relations between the various business processes, perimeters, infrastructures, and assets.
- Identify the present scenario - threats, vulnerabilities and impacts - and speculate the projection of the desired security scenario capable of sustaining and making the company's current and new businesses.

- Map the company's needs and relations associated with the handling, storage, transportation and disposal of information
- Organize the security demands of the business.

Security Strategy

- Define an action plan, usually multi-year, considering all the strategic, tactical, and operational particularities of the operational particularities of the business mapped out in the previous step, besides the physical, technological, and human risk aspects.
- Create synergy between the current and desired scenarios, in addition to align expectations among executives, in order to gain commitment and explicit support for the measures foreseen in the action plan.

Security Planning

- Organize the interdepartmental committees, specifying responsibilities, positioning, and scope of action, formalizing its role in the face of local actions in line with global actions coordinated by the corporate committee of information security.
- Initiate preliminary actions to train executives and technicians, in order to better guide them regarding the challenges, involving them in the results and sharing with them the responsibility for the success of the management model.
- Elaborate a solid information security policy, considering with extreme particularization and detailing the characteristics of each business process, perimeter and infrastructure, materializing

it through guidelines, norms, procedures and instructions that will formalize the company's positioning around the theme and, furthermore, point out the best practices for handling, storage, transportation and disposal of information in the risk range indicated as ideal.

- Carry out emergency corrective actions as a function of the imminent risk perceived in the mapping stages and currently, in the elaboration of the criteria defined in the security policy.

Security Implementation

- Disseminate corporately the security policy, in order to make it the official instrument, known by all, which will guide executives, technicians, and users about the best practices in the interaction with information.
- Capacitate by making users aware of the behavior in handling, storage, transport and disposal of information, including knowledge of the criteria, prohibitions and responsibilities inherent to the subject.
- Implement physical, technological and human control mechanisms that will allow the elimination of vulnerabilities or their viable management, in order to lead the risk level to a desired standard of operation.

Security Management

- Monitor the various controls implemented, measuring their efficiency and signaling changes in the variables that interfere directly and indirectly in the level of business risk.

- Project the ROI situation based on the measurements made, allowing the identification of achieved results and, also, to enable new needs that arise due to business demands.
- To ensure the adequacy and conformity of the business with associated norms, internal rules, market segment rules, standards, and incident legislation.
- Maintain strategic plans for contingency and disaster recovery, aiming to ensure the adequate level of availability and the consequent operational continuity of the business.
- To manage the implemented controls, adjusting their operating rules to the criteria defined in the security policy or preparing them to meet the new needs caused by changes in context or internal and external variables.

Supply Chain Security

- Equalize the security measures adopted by the company to the common business processes, maintained with stakeholders in the productive chain (suppliers, clients, government, etc.), in order to level the risk factor without one of the parties exposes shared information and poses a threat to the operation of both businesses.

As you can see, what we call information security should be shaped in a set of integrated processes that have specific local objectives but are closely aligned with a single corporate objective: to dynamically manage comprehensive control mechanisms - considering processes technologies, people, and environments - that add value to the business, allowing its operation with controlled risk.

2.9 **ADDING VALUE TO YOUR BUSINESS**

The return on investment analysis should have already hinted at the measurable results associated with the corporate security management model, but it is worth highlight also the benefits of integrated management from the perspective of the executive and his/her business:

- Enhances the value of the company's actions
- Facilitates new business
- Facilitates exploration into new markets
- Facilitates new sources of revenue
- Increases market share
- Increases share of mind
- Consolidates the image of modernity
- Consolidates the image of administrative health
- Consolidates the competitive differential provided by technology applied
- Increases customer satisfaction
- Increases user productivity
- Increases the revenue
- Increases profitability
- Increases agility in adapting to change
- Increases operational availability levels
- Reduces costs caused by threats that exploit security gaps
- Reduces costs caused by misuse of technological resources
- Reduces operational risks

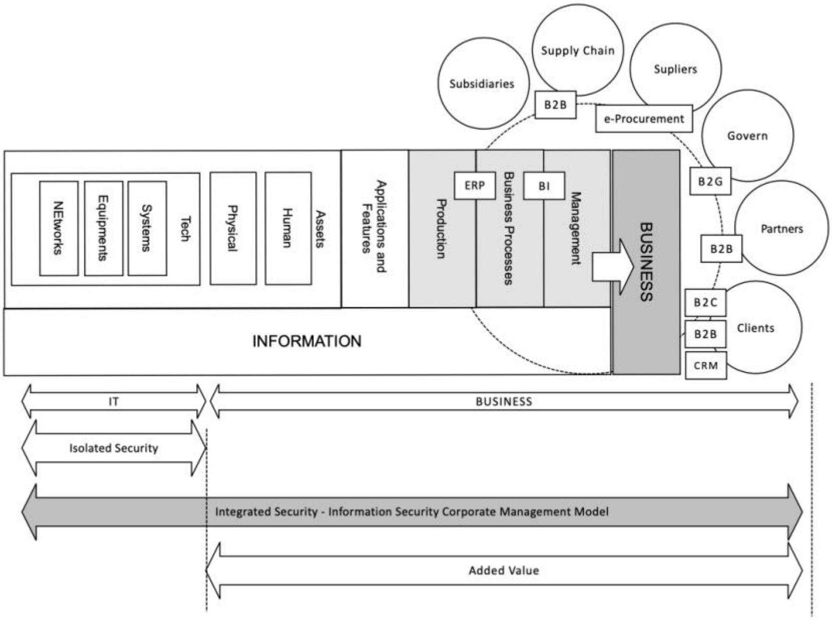


FIGURE 2.16

Perception of the added value promoted by the integrated management model

- Prepares the company for today's challenges
- Prepares the company to react to future challenges
- Preserves the company's image
- Integrates security into the business

Integrated management is one of the most relevant tangible benefits provided by the model, because it is responsible for avoiding redundant investments, mismatched actions, contrary or conflicting activities and, mainly, for providing the concentration of efforts toward a common objective: the company's business.

Chapter 3

Knowledge

Checkpoint 1

This knowledge checkpoint is a brief and objective consolidation of the concepts covered in each section of the book with the objective of reinforcing the process of absorbing the relevant content.

Information: an increasingly valued asset

CONCEPT: Information represents the competitive intelligence and is recognized as a critical asset for the operational continuity and health of the company.

Dependence growth

CONCEPT: The risks are inherent and proportional to the degree of dependence that the company has on information and the complexity of the structure that supports the automation processes, computing and information sharing processes.

Holistic approach to risk

CONCEPT: Considering the plans and identifying the challenges and specific business characteristics are the first steps to model an adequate security solution.

An explosive mixture

CONCEPT: Looking around and designing new situations should be a practice for companies concerned with building a solid, but adequately flexible solution to adjust to the changes that will inevitably occur in the environment.

Information life cycle

CONCEPT: The corporate view of information security should be compared to a chain, where the weakest bond determines its degree of resistance and protection. Invasion occurs where security fails!

Challenges

Anatomy of the problem

CONCEPT: Security is about implementing controls that reduce risk to adequate, manageable, and feasible levels.

Corporate vision

CONCEPT: Companies are different and will need to map their risk by weighing threats, physical, technological and human vulnerabilities, and impacts, in search of the ideal solution.

Sins committed

CONCEPT: Learning from the experiences and mistakes made by others is part of the growth process, but learning from your own must be part of your survival process.

Raising executive body awareness

CONCEPT: Only with executive support, will security actions gain autonomy and reach capable of affecting corporately the security holes.

Return on investment

CONCEPT: Projecting the ROI of integrated actions and aligned with the company's strategic guidelines will represent an effective and sensitization tool for the executive, in order to gain their commitment.

Hierarchical positioning

CONCEPT: Autonomy and strategic positioning are conditions for sustaining a dynamic process of effective security management.

Managing changes

CONCEPT: Security should be treated as a corporate process capable of considering the inevitable physical, technological, human and contextual changes, and react dynamically.

Corporate security management model

CONCEPT: The fact that there is now a management model that serves as a compass does not guarantee its successful implementation. It is necessary to have a multi-specialist human structure, dedicated and conceptually grounded, always in search of updating.

Adding value to your business

CONCEPT: Differently from what was thought, every information security initiative must have as its main target the business and, consequently, its actions must be totally convergent, aligned and focused on the challenges of the business.

Chapter 4

Information Security

4.1 **SECURITY CONCEPTS**

We have already covered the challenges associated with security in an executive superficiality, but no expectations will be met if actions are not consistently underpinned by solid and widely recognized concepts.

Avoiding reinventing the wheel and giving a new interpretation that I have borrowed the knowledge base called the module Security Body of Knowledge, owned by the Brazilian company leader in corporate information security solutions, *Módulo Security Solutions*, and added to it the definitions of the NBR ISO/IEC 27002:2013 (Code of practice for information security management) and the other standards that make up the ISO 27000 (Information technology - security techniques) families, especially NBR ISO/IEC 27005:2011 (Information security risk management) and ISO 31000 (Risk management).

Information Security

We can define information security as an area dedicated to the protection of information assets against unauthorized access, improper alteration or unavailability. Broadly, we can also consider it as the practice of risk management of incidents implying the compromise of the three main concepts of confidentiality, integrity and availability of information. In this way, we would be talking about the definition of rules that would apply to all moments of the information life cycle: handling, storage, transport and disposal, making it possible to identify and control threats and vulnerabilities.

The corporate information security management model lends a wider meaning to the expression, considering in the foreground the challenges of the business as a whole. In light of this comprehensive orientation, two other concepts gain autonomy: authenticity and conformity (previously referred to as legality).

Authenticity is a concept originally drawn from the precursors of confidentiality and integrity, due to its importance in the context in which we have been living for at least the last 30 years, in which it plays the role of signaling the commitment of aspects associated with the authenticity of information and of the parties involved in its exchange.

Compliance, on the other hand, is one of the components of the GRC model (governance, risk and compliance management), which has the role of ensuring the fulfillment of organizational obligations, ranging from commitments to stakeholders (investors, employees, creditors, regulatory agencies, etc.) to legal and regulatory aspects related to the company management. Compliance has expanded the boundaries of legality, commonly referred to as one of the most important aspects associated with information security. In this context, the term "information security" is itself ambiguous and can take on a double interpretation:

1. Security as a practice adopted to make an environment safe (activity, action, preservation of principles), of interdisciplinary character, composed of a set of methodologies and applications that aim to establish security controls (e.g., of authentication, authorization and auditing) of the constitutive elements of a communication network and/or those that manipulate information; and procedures to ensure business continuity in the event of incidents.
2. Result of the practice adopted, the goal to be achieved. It is the characteristic that information acquires when it is the target of a security practice (secure - adjective, objective of the practice).

Therefore, when using this name, one must be aware of this ambiguity, in order to identify the most appropriate concept to be addressed. For example:

Security as a "means" - Information security aims to ensure the confidentiality, integrity and availability of information, the impossibility of agents participating in transactions or communication to repudiate the authorship of their messages, compliance with organizational obligations, legislation and regulatory requirements, and business continuity.
Security as an "end" - Information security is achieved through practices and policies aimed at an adequate operational and managerial standardization of the assets and processes that store, manipulate, transmit, receive and dispose of information.

Basic concepts of information security

Information security has as its objective the preservation of three basic principles that guide the implementation of this practice.

Confidentiality

All information must be protected according to the degree of secrecy of its content, aiming at limiting its access and use only to the people to whom it is intended.

Integrity

All information must be kept in the same condition in which it was made available by its owner, aiming to protect it against undue alterations, whether intentional or accidental.

Availability

All information generated or acquired by an individual or institution must be available to its users at the time they need it for any purpose.

Information

Set of data used for the transfer of a message between individuals and/or machines in communicative (based on the exchange of messages) or transactional processes (processes in which operations involve, for example, the transfer of monetary values).

Information can be present in numerous elements of this process, called assets, which are the target of information security protection, or be manipulated by them.

Asset

It is every element that makes up the processes that manipulate and process information, including the information itself, the media in which it is stored, and the equipment in which it is handled, transported and discarded.

The asset has this denomination, coming from the financial area, because it is considered an element of value to an individual or an organization and, for this reason, requires adequate protection. The standard ISO/IEC 27000:2009 (reference for Information Security vocabulary and terms) only defines it as "anything that has value to the organization".

There are many ways of dividing and grouping the assets to facilitate their treatment, but one model in particular has my sympathy: equipment, applications, applications, users, environments, information and processes. In this way, it becomes possible to better identify the boundaries of each group, treating them with specificity and qualitatively enhance security activities.

Aspects of information security

Some elements are considered essential in the practice of information security, depending on the objective that is to be achieved:

Authentication

Process of identification and formal recognition of the identity of the elements that communicate or are part of an electronic transaction that enables access to information and its assets through identification controls of these elements.

Compliance

The process of ensuring compliance with business obligations to stakeholders (investors, employees, creditors, etc.) and with legal and regulatory aspects related to the administration of business, within ethical principles and conduct established with their top management. It is part of the tripod of GRC - governance, risk, and compliance management model.

Associated Aspects

Authorization

Granting permission for access information and application functionality to participants in an information exchange process (user or machine), after their correct identification and authentication.

Audit

The process of gathering evidence of the use of existing resources in order to identify the entities involved in an information exchange process, that is, origin, destination, and means of traffic of an information.

Authenticity

Ensuring that entities (information, machines, users) identified in a communication process as senders or authors are exactly what they say they are and that the message or information has not been altered after it was sent or validated. Usually the term authenticity is used in the context of digital certification, where cryptography and hashing are used to assign an identification label to messages or files sent between members of a public key infrastructure in order to guarantee the principles/aspects of irretrievability, identity, authenticity, authorship, originality, integrity and confidentiality.

Severity

Severity of the damage that a given asset may suffer due to the exploitation of a vulnerability by any applicable threat.

Asset Relevance

The degree to which an asset is important to the operationalization of a business process.

Business Process Relevance

Degree of importance of a business process to the achievement of the objectives and survival of an organization.

Criticality

Severity relative to the impact to the business caused by the absence of an asset, due to the loss or reduction of its functionality in a business process, or by its improper and unauthorized use.

Irreversibility

Characteristic of information that has the identification of its issuer, which authenticates as the author of information sent and received by him/her. Synonym of non-repudiation.

Threats

Are agents or conditions that cause incidents that compromise information and its assets through the exploitation of vulnerabilities, causing losses of confidentiality, integrity and availability, and, consequently, causing impacts to the businesses of an organization.

Classifying the threats according to their intentionality, they can be divided into the following groups:

Natural

Threats arising from phenomena of nature, such as natural fires, floods, earthquakes, electromagnetic storms, tsunamis, warming, pollution, etc.

Involuntary

Unconscious threats, almost always caused by ignorance. They can be caused by accidents, errors, lack of energy, etc.

Voluntary

Purposeful threats caused by human agents such as hackers, invaders, spies, thieves, creators and disseminators of computer viruses, arsonists.

Vulnerabilities

These are weaknesses present or associated with assets that manipulate and/or process information that, when exploited by threats, allow the occurrence of a security incident, negatively affecting one or more information security principles: confidentiality, integrity and availability.

Vulnerabilities by themselves do not cause incidents, as they are passive elements, requiring a causative agent or factor, which are the threats.

Examples of vulnerabilities

Physical

Building installations that do not comply with good practices or the current rules and regulations; lack of fire extinguishers, smoke detectors and other resources for firefighting in environments with strategic assets or information; poor access control in places containing confidential or sensitive information, etc.

Natural

Environments with electronic equipment next to places susceptible to natural disasters, such as fires, floods, earthquakes, storms and others, such as power outages, dust accumulation, humidity and temperature, etc.

Hardware

Computers are susceptible to dust, humidity, dirt, and improper access to inadequately protected resources, and may also suffer from poorly configured or misconfigured components, with failures or fluctuations in the power supply or excessive increases in ambient temperature.

Software

Errors in coding, installation or configuration of systems and applications can lead to improper access, information leakage, loss of data and audit trails, or unavailability of the asset when needed.

Media

Disks, files, reports, and printouts can be lost or damaged; power failures can cause equipment glitches, potentially damaging logical data tracks; hard disks usually have a lifespan; electromagnetic radiation can affect many types of magnetic media.

Communication

Telephone communication is vulnerable to eavesdropping (improper access) or problems in the physical or logical infrastructure that prevents it from being established.

Human

Lack of training or awareness of people, lack of adequate psychological evaluation or background check that identifies hidden objectives or previous problems, or even an employee's bad faith or discontent, among others, can lead to the improper sharing of confidential information, failure to perform security routines, or to errors, omissions, etc. that put the information at risk.

Security measures

These are the practices, procedures, and mechanisms used for protection of information and its assets, which can prevent threats from exploiting vulnerabilities, reduce vulnerabilities, limit the probability or impact of their exploitation, minimizing or even avoiding risks.

Specifically when it comes to risk, it is worth noting that avoiding it or reducing it to an acceptable level is not always the best strategy to be adopted. There are cases in which the cost of implementation of security measures to avoid or reduce a given risk is greater than the value of the information to be protected, making this action inadvisable. In these cases, the possibility of the company retaining the risk must be evaluated, living with it, sharing it or outsourcing it, for example, contracting insurance (ISO/IEC 13335-1:2004).

The security measures are also referred to as controls and can have the following characteristics:

Preventive

Security measures that aim to prevent incidents from occurring. They aim to ensure security through mechanisms that establish the conduct and ethics in the institution. As examples we can mention safety policies, work instructions and procedures, user awareness campaigns and lectures, security specifications, access control equipment, tools for the implementation of the security policy (firewall, antivirus, appropriate router and operating system configurations, etc.).

Detectives

Security measures that aim to identify conditions or individuals causing threats, in order to prevent them from exploiting vulnerabilities. Some examples are risk analysis, intrusion detection systems, security alerts, surveillance cameras, alarms, etc.

Corrective

Actions aimed at correcting a technological and human structure to adapt it to the security conditions established by the institution or aimed at reducing impacts: emergency teams, backup restoration, operational continuity plan, disaster recovery plan.

Note that many of the security measures may have more than one characteristic, which means that a business continuity plan is both a preventive action (when it is created) as well as a corrective action (when it is applied). Therefore, this categorization only serves to identify the focus of the security work proposed when it is being carried out.

Risks

Probability of threats exploiting vulnerabilities, causing loss of confidentiality, integrity and availability, possibly causing business impacts.

Impact

Extent of damage caused by a security incident on one or more business processes.

Incident

Fact (event) resulting from the action of a threat, which exploits one or more vulnerabilities, leading to the loss of information security principles: confidentiality, integrity and availability.

An incident generates impacts on the company's business processes, it is the element to be avoided in a management chain of processes and people.

The severity of an incident can be analyzed in qualitative and quantitative terms, and is measured by its impact (see Figure 4.1).

From the condensed view diagram in Figure 4.1, you can get a real sense of the magnitude of the corporate challenge of information security.

4.2 **PERIMETER THEORY**

There is nothing new for the security field, especially property security, to talk about perimeters. This structure of segmentation of physical environments is considered a military defense strategy and also applies to the current scenario in companies, even if we have to go beyond the physical aspects and apply them to segment logical environments. Certainly, the big secret to obtaining the best return on the mechanisms that guarantee the levels of protection of information is in the intelligent segmentation of assets. This way, it becomes possible to apply the appropriate controls, each one offering a previously metered level of protection without exceeding the limits nor falling short of the needs.

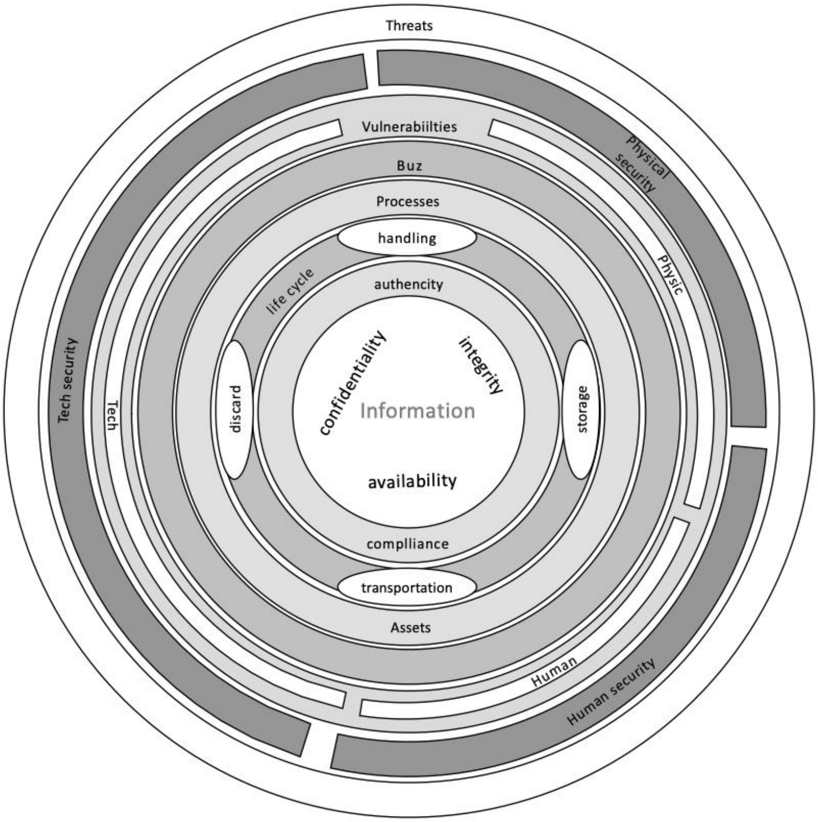


FIGURE 4.1

Condensed view of challenges.

Think, for example, of the resources of restrictive auditing of Internet access. If employees are not logically segmented in the network access systems, mixing departments and people who are authorized by necessity imposed by the nature of the activity and other employees whose access is controlled or prohibited altogether, the ability of applying the appropriate controls to each of the profiles gets lost. Thus, the chances of exceeding the level of control for some or offering them a level that falls short of their needs, thereby exposing information unnecessarily is more likely to happen (see Figure 4.2).

Not only is the perimeter associated with the compartmentalization of physical and logical spaces, but also plays an important role of an alert and resistance mechanism distributed over areas, in order to allow attempts of improper access and intrusion to generate alert signals and meet resistance that will provide time for contingency measures to be taken before the action moves further toward the target.

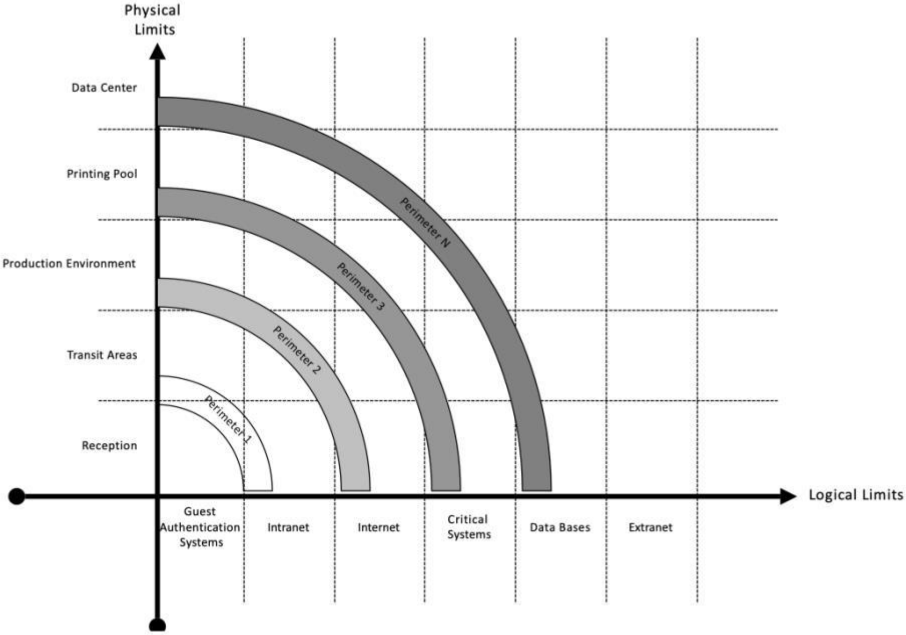


FIGURE 4.2 ____I llustration depicting physical and logical perimeters.

4.3 **SECURITY BARRIERS**

Conceptually, given the breadth and complexity of the role of security, it is common to study the challenges in layers or phases, partitioning all the work to make the understanding of each one clearer. We call this division the barriers - the six security barriers.

Each of these has an important role to play in the larger objective of reducing risks and, for this reason, must be adequately sized to provide the most perfect interaction and integration, as if they were pieces of a single puzzle. Note that this conceptual model implements the perimeter theory, segmenting physical or logical perimeters and offering complementary and biased levels of resistance and protection.

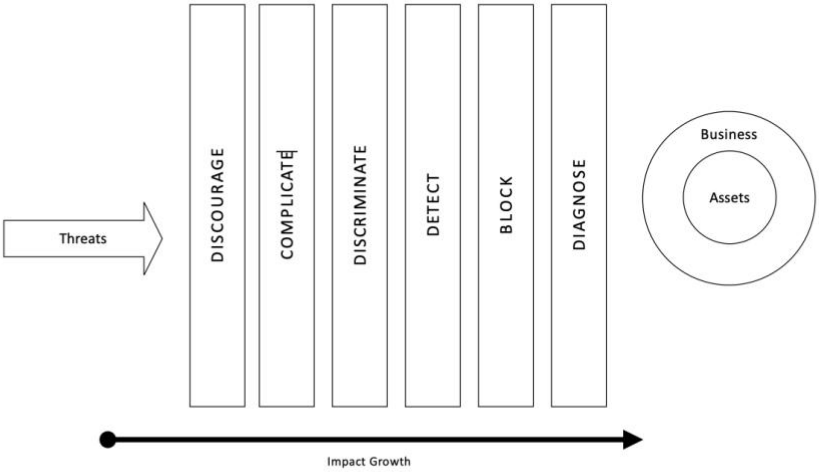


FIGURE 4.3

Representative diagram of the security barriers.

Barrier 1: discouragement

This is the first of the five security barriers, and fulfills the important role of discouraging threats. Threats, in turn, can be demotivated or lose interest and stimulus by the attempted breach of security by physical, technological or human mechanisms. The mere presence of a video camera, even a false one, of a warning of the existence of alarms, campaigns to divulge the security policy, or training of employees informing them of auditing practices and monitoring access to the systems are already effective in this phase.

Barrier 2: hinder

The role of this barrier is to complement the previous one by effective adoption of controls that will hinder undue access. As an example we can cite the physical access control devices, such as turnstiles, metal detectors, and alarms, or logical such as magnetic card readers, biometric, password, smartcards and digital certificates, besides the firewall, etc.

Barrier 3: discriminate

Here the important thing is to surround yourself with resources that allow you to identify and manage access, defining profiles and authorizing permissions. Systems are widely used to monitor and set limits on access to telephony services, physical perimeters, physical perimeters, computer applications, and databases. The processes for evaluating and managing the volume of resource use, such as e-mail, printer, or even the flow of physical access to environments, are good examples of this barrier's activities.

Barrier 4: detect

Acting in a complementary way to its predecessors, this barrier must provide the security solution with devices that alert and instrument security managers to detect risk situations, whether in the detection of risk situations, whether in an invasion attempt, or in a possible contamination by a virus, non-compliance with the company's security policy or the copying and sending of sensitive information in an inadequate manner.

This is where monitoring and auditing systems come in to help the identification of exposure attitudes, such as the antivirus and the intrusion detection system, which have reduced incident response time.

Barrier 5: detain

This fifth barrier represents the goal of preventing the threat from reaching the assets that support the business. The triggering of this barrier, activating its control mechanisms, is a sign that the previous ones were not enough to contain the threat's action. At this point, detention measures, such as administrative and punitive actions, and blocking physical and logical access respectively to environments and systems, are good examples.

Barrier 6: diagnose

Although it represents the last barrier in the diagram, this phase has the special meaning of representing the continuity of the information security management process. It may seem like the end, but it is the link to the first barrier, creating a cyclical and continuous movement. Because of these factors, this is the most important barrier. It must be driven by risk analysis activities that consider technological as well as physical and human aspects, always oriented to the specific characteristics and needs of the company's business processes.

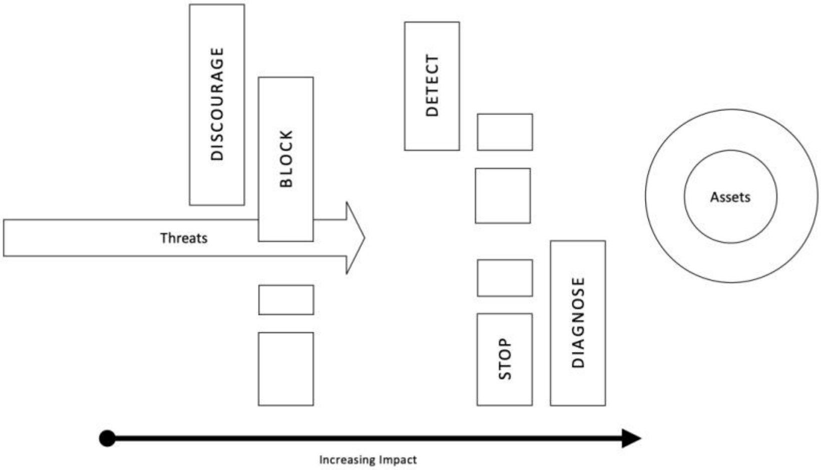


FIGURE 4.4

Symbolic illustration of a security action guided by an inadequate diagnosis.

It is important to note that a preliminary diagnostic work conducted poorly or executed without methodology and instruments that provide more accuracy to the risk analysis process may distort the understanding of the current security situation and, simultaneously, the desired situation. This increases the likelihood of inappropriately sizing barriers, distributing investments disproportionately, often redundantly, and ineffectively. The return on investment will not live up to expectations, and the company will not achieve the level of security appropriate to the nature of its activities.

4.4 **GRC**

It emerged in the first decade of this century and is an acronym for the concepts of governance, risk, and compliance. In fact, GRC refers specifically to the management of each of these items by corporations and is closely linked to information security, the aspects of controlling and ensuring that the organization is not adversely affected by inadequate management. It has been common practice to identify GRC as an evolution of information security, taking it to a more comprehensive and therefore more extensive and critical.

Governance refers to the set of people, processes, and policies that guide how the organization should be run. According to the CVM (*Comissão de Valores Mobiliários*, a Brazilian Securities and Exchange Commission linked to the Ministry of Finance), governance encompasses the practices that aim to optimize a company's performance and protect all stakeholders, such as investors, employees and creditors, facilitating access to capital. The IBGC (Brazilian Institute of Corporate Governance) includes in this definition the purpose of increasing the value and contributing to the perpetuity of the company.

However, of the three aspects of GRC, governance is perhaps the most distant from information security management, despite its procedural, policy-setting, and protection, because it is centered on a upper level than that of organizational management, involving board of directors, shareholders, and, at the board of directors level, usually the CEO, who is usually part of the board of directors and sometimes the CFO, who also has strong responsibility for operational control.

In the literature, it is suggested that the Security Officer may be in charge of governance, but, given the natural dissension between the technology and information security areas, many times this occupation will not be possible. The tension between "I.T." and "I.S." is historical and can be explained by the difference in focus, since the IT area is primarily concerned with making feasible the initiatives that depend on it, even if the security aspects are not fully guaranteed, something unreasonable in the vision of the IS area. The approach of the IS area with auditing areas, commonly associated with coercive and unpopular initiatives, to perform risk analysis and compliance activities, does not favor the relationship too. Obviously, both IT and IS managers of the 21st century have a much broader sense of their obligations and the need to focus on what is important to the business, which tends to minimize any past raids.

In the opposite direction, risk management is a natural extension of the responsibility of information security management in organizations. In fact, we have suggested that one should not think of information security by itself, but in the context of adding value to the business, applying risk management concepts, from the definition of the relevance of the information assets to the decision-making regarding the implementation of controls or countermeasures to the vulnerabilities identified in these assets.

In the context of risk management, two reference standards emerge: NBR ISO 31000:2009 and NBR ISO/IEC 27005:2011.

ISO 31000 (Risk management, principles and guidelines), published in 2009, is a comprehensive standard that deals with risk management to suit any organizational segment and serves as a reference or "framework" for the creation of specific norms to address the particularities of business areas or interests that demand them.

This is exactly the case with ISO 27005 (Information technology, security techniques, information security risk management) published in 2011, and one of the components of the 27000 family of norms, aimed at information security management. This standard, as its title defines, details the ISO 31000 risk management model a bit more, focused on the management of information security risks, also becoming one of the Security Officer's bibles.

The subject of risk is dealt with in more detail in Section 4.5.

Compliance, as we have seen earlier in this chapter, works to guarantee the fulfillment of organizational obligations, ranging from commitments with stakeholders (investors, employees, creditors, regulatory agencies, etc.) to legal and regulatory aspects related to the company management.

Legality was already one of the aspects of concern in information security since its fundamentals have been established. However, compliance, because of its wide focus, expands the boundaries of legality to the point of deserving to take its place as an essential aspect of information security management.

If we look back to the late 20th century and the last decade, it is easy to justify the growth of compliance (and GRC as a whole) as an essential management aspect of organizations, as a result of a growing concern, especially in the United States, to avoid new financial scandals such as those that motivated the creation of the FCPA (Foreign Corrupt Practices Act) and SOx (Sarbanes-Oxley Act), among others, but that still occur today, such as the American subprime scandal at the end of the first decade of the 21st century.

In today's information technology market, one of the fastest growing sectors is that of tools and applications to support and automate the management of governance, risk, and compliance, and there are only benefits for the information security manager from this movement.

4.5 **RISK EQUATION**

Detailing the risk management aspect a bit further, it is reasonable to sustain that every business, regardless of its market segment and its core business, has dozens, perhaps hundreds of variables that relate directly and indirectly to the definition of its level of risk. Being aware, that, according to the ISO 31000 definition, risk is the effect of uncertainty on the objectives, and this effect can be positive or negative, identifying these variables becomes the first step in the challenge of implementing an effective risk management process.[2]

Interpretation of the equation

Risk is the probability that agents, which are the **threats**, exploit **vulnerabilities**, exposing **assets** to losses of confidentiality, integrity and availability, and causing **impacts** on the business.

[2] In the context of information security, hardly ever is the positive bias of risks evaluated.

These impacts are limited by **security measures** that protect the assets, preventing threats from exploit vulnerabilities, thus reducing the risk.

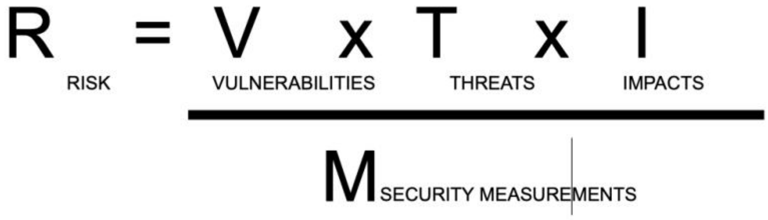


FIGURE 4.5

Diagram of the information security risk equation.

No matter how well assets are protected, new technologies, organizational changes and new business processes can create vulnerabilities or identify and draw attention to existing ones. In addition, new threats can emerge and significantly increase the possibility of business impacts. Therefore, corrective security measures need to be considered, because there will always be the possibility of an incident occurring, even if we have taken all appropriate preventive measures.

Zero-risk bias

It is crucial that we all stay aware that there is no such thing as total security and, therefore, we must be well structured to withstand changes in the variables of the equation, reacting quickly and adjusting the risk back to the standards specified as ideal for the business.

Given this, we conclude that there is no R (risk) outcome equal for all. It will always be necessary to assess the level of security appropriate to each moment in the company's history, as if we had to weigh ourselves at regular periods to define the best dose of caloric intake (safety dose) in the period, in order to get closer to the ideal weight (risk level) for the moment.

4.6 **CORPORATE INFORMATION SECURITY COMMITTEE**

Representing the concentrating core of the work, the corporate information security committee must be, besides being adequately positioned in the hierarchy of the organization, formatted based on the clear definition of its objective, structure, functions, responsibilities, profile of the executors, besides the formal and and official identification of its members, who will give representation to the most critical and relevant departments of the company.

Bringing together managers with visions of the same object, but from distinct points, is fundamental to obtain a clear picture of the problems, challenges, and impacts. Thus, involving representatives from the technological, communication, commercial, business, legal, patrimonial, financial, auditing areas, etc, will enhance the management process, in such a way as to avoid conflicts, wastes, redundancies, and the main thing: to foment the synergy of the company, which closely aligns its strategic guidelines for the short, medium and long term.

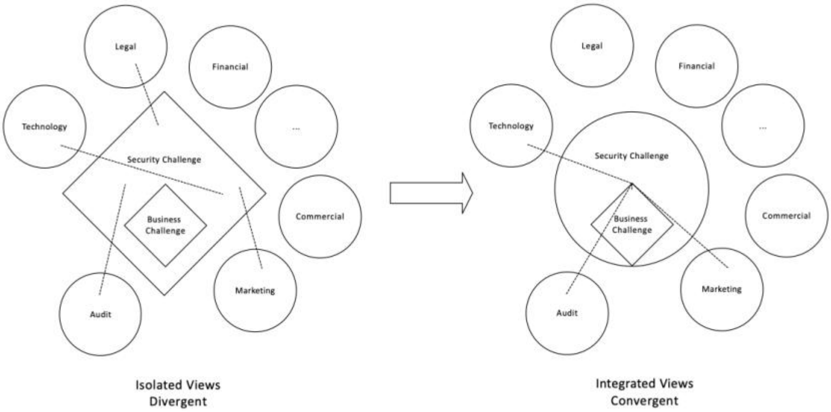


FIGURE 4.6

The integration scenarios of different views of the same object (view of the lighthouse).

Objectives

- Foster the corporate information security management model, through distributed but integrated actions, with physical, technological and human scope, and interfere in all business processes that maintain the company's operation.
- To analyze, through a multidisciplinary and multi departmental team with representation on the committee, the partial and final results of the actions, in order to measure the effects, compare them to the defined goals and make adjustments to the safety master plan, adapting it to the new reality generated by the change in internal and external variables.
- Interact constantly with the executive committee and the audit committee, seeking synergy of the macro-objectives of the company, in addition to exchanging information linked to the safety index and indicators as a way to demonstrate the corporate results of the safety committee.
- Align and define actions for the interdepartmental committees that must act locally in a distributed way, collecting in greater detail the facts related to the physical, technological and human aspects inherent to their sphere and scope.

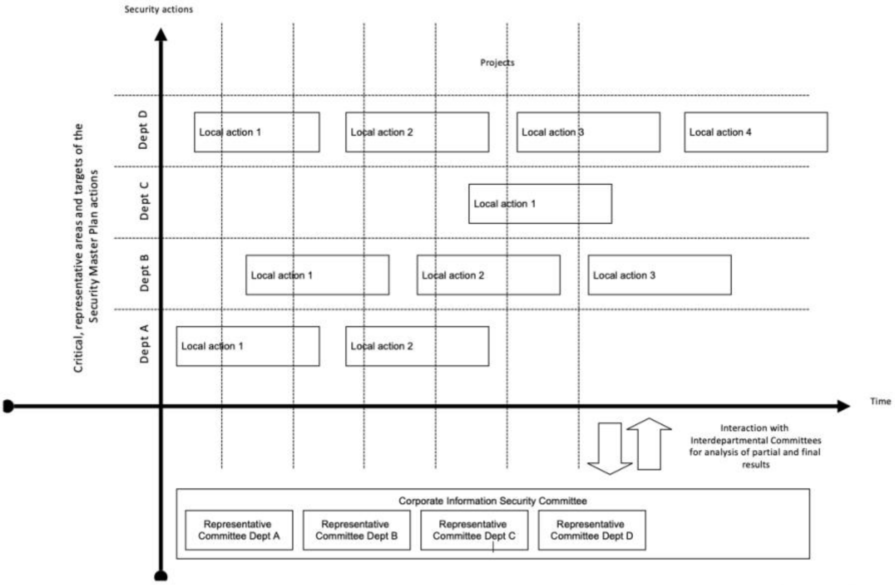

Security actions
Projects
Critical, representative areas and targets of the Security Master Plan actions
Dept D
Local action 1
Local action 2
Local action 3
Local action 4
Dept C
Local action 1
Dept B
Local action 1
Local action 2
Local action 3
Dept A
Local action 1
Local action 2
Time
Interaction with Interdepartmental Committees for analysis of partial and final results
Corporate Information Security Committee
Representative Committee Dept A
Representative Committee Dept B
Representative Committee Dept C
Representative Committee Dept D

FIGURE 4.7

Interaction of the committee with corporate actions and interdepartmental committees.

Coordinator of the Corporate Information Security Committee

Security Officer

Basic structure of the committee

- General security coordination
- Security coordination
- Control
- Planning and evaluation
- Execution

Due to the breadth of the corporate committee's action, large companies that have a distributed and well dispersed management model start to need security "cells" spread throughout the company and located in more representative and critical departments or units. These cells are called interdepartmental information security committees and maintain in their structure the same four functions and responsibilities that apply to the corporate security committee. What distinguishes them in this dimension are the scope and sphere of action that correspond, respectively, to tactical-operational management and strategic management.

In this way, they come to have a relationship of dependence and synergy, in which the interdepartmental committees report to the corporate committee, which, in turn, keeps them aligned to the strategic definitions of safety and of the company as a whole.

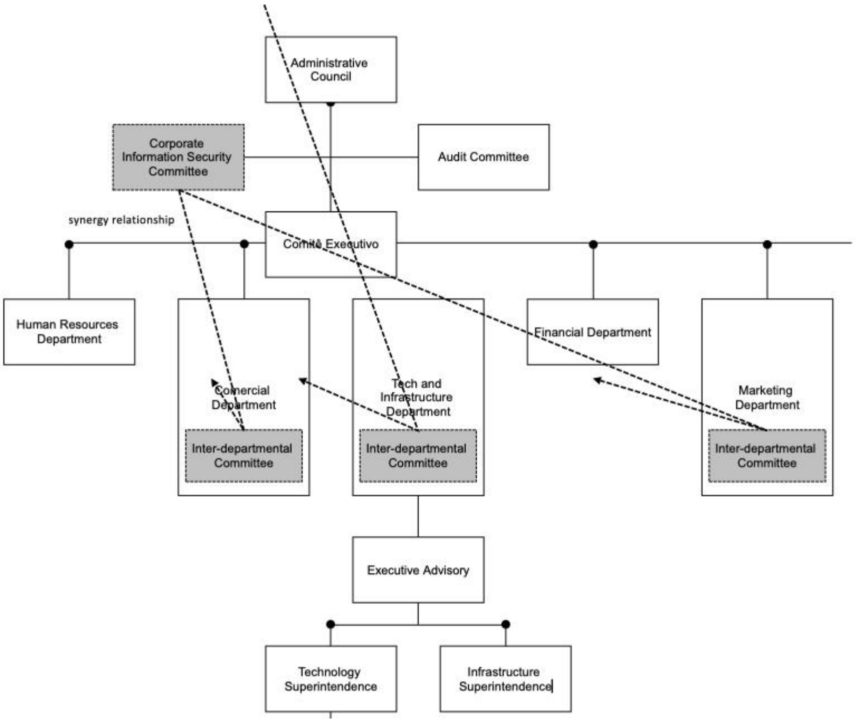

Administrative Council
Corporate Information Security Committee
Audit Committee
synergy relationship
Comitê Executivo
Human Resources Department
Comercial Department
Tech and Infrastructure Department
Financial Department
Marketing Department
Inter-departmental Committee
Inter-departmental Committee
Inter-departmental Committee
Executive Advisory
Technology Superintendence
Infrastructure Superintendence

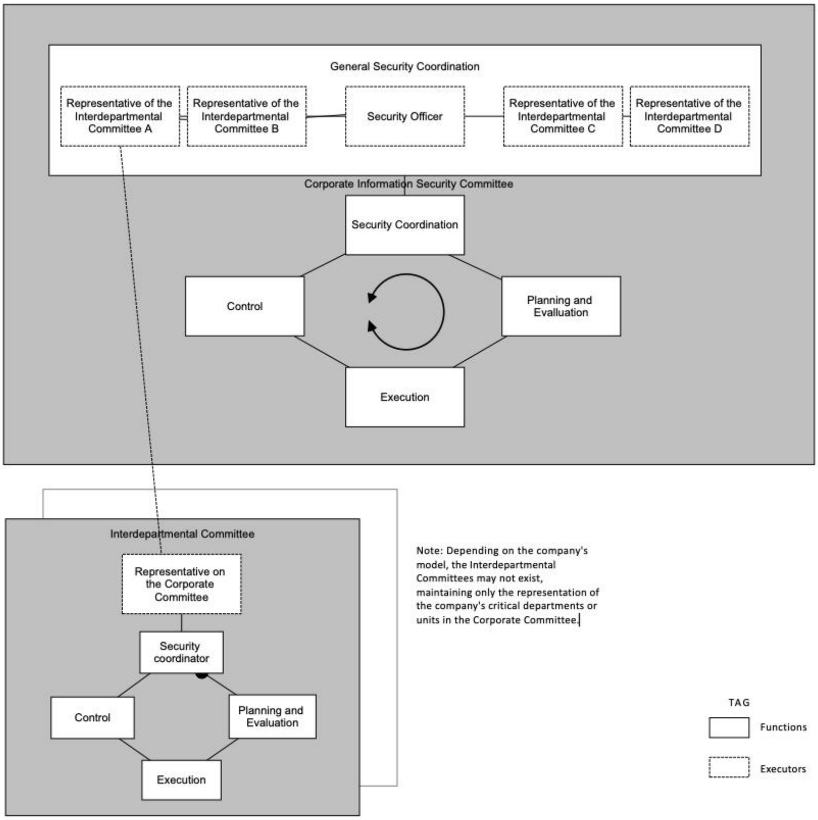
FIGURE 4.8

List of committees contextualized to large companies and distributed management model.

Structure, roles and responsibilities

- General security coordination
    - Mobilize the associated areas corporately
    - Deliberate corporate measures and countermeasures
    - Define indexes, indicators and strategic goals
- Security coordination
    - Coordinate the sub-functions of the general security coordinator
    - Evaluate the results achieved
    - Propose changes
    - Propose measures and countermeasures
    - Mobilize the associated critical managers
- Planning and evaluation
    - Prepare management reports on the results achieved
    - Elaborate proposals for specific security projects
    - Promote lectures to raise awareness and maintain of knowledge
    - Provide advisory support to the general coordinator
- Control
    - Conduct auditing and monitoring actions
    - Analyze metrics of indexes and indicators
    - Perform risk analysis
    - Train the execution function in the handling of indexes and indicators
- Execution
    - Comply and enforce the security policy in the associated environments
    - Inform the control function of the results of the indexes and indicators
    - Respond to audit queries
    - Register occurrences of security breaches reporting them to the control function

- Execute security measures and countermeasures


General Security Coordination
Representative of the Interdepartmental Committee A
Representative of the Interdepartmental Committee B
Security Officer
Representative of the Interdepartmental Committee C
Representative of the Interdepartmental Committee D
Corporate Information Security Committee
Security Coordination
Control
Planning and Evalluation
Execution
Interdepartmental Committee
Representative on the Corporate Committee
Security coordinator
Control
Planning and Evaluation
Execution
TAG
Functions
Executors

Note: Depending on the company's model, the Interdepartmental Committees may not exist, maintaining only the representation of the company's critical departments or units in the Corporate Committee.

FIGURE 4.9

Structure macro diagram.

Performers' profile

- General security coordination
  - Security Officer with support from directors and their representatives
- Security coordination

  - Security Manager
- Planning and evaluation
  - Security consultant
  - Contingency consultant
  - Security Analyst
  - Security Assistant
- Control
  - Security Auditor
  - Risk Manager
  - Safety Monitor
- Execution
  - Network Administrator
  - Development Manager
  - Production Manager
  - Application Manager
  - Physical Security Manager
  - Technology Support

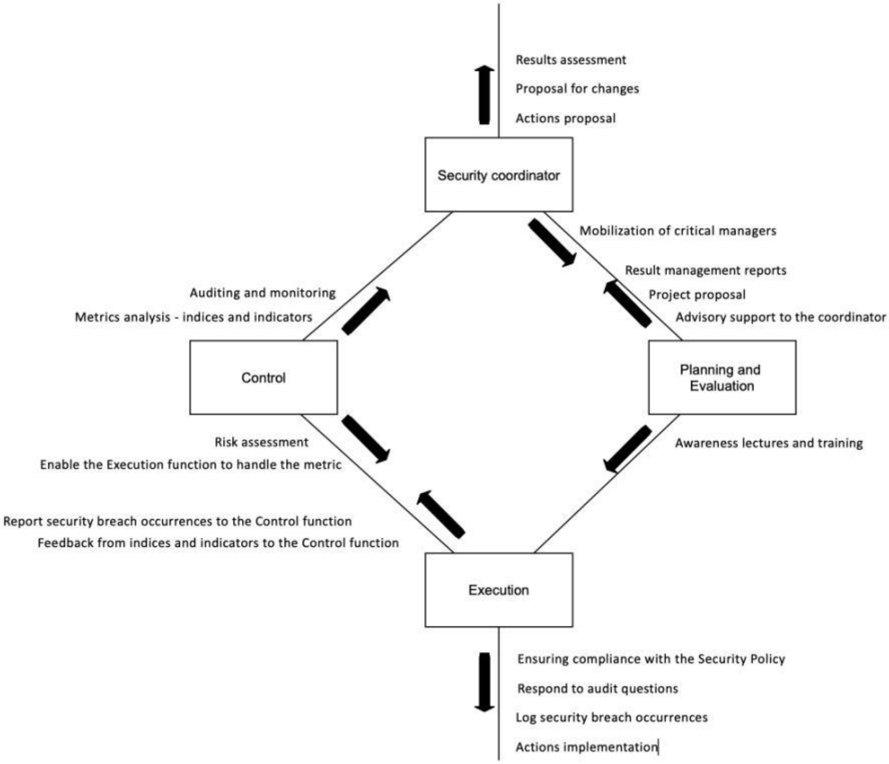

Results assessment
Proposal for changes
Actions proposal
Security coordinator
Mobilization of critical managers
Result management reports
Project proposal
Advisory support to the coordinator
Auditing and monitoring
Metrics analysis - indices and indicators
Control
Planning and Evaluation
Risk assessment
Enable the Execution function to handle the metric
Awareness lectures and training
Report security breach occurrences to the Control function
Feedback from indices and indicators to the Control function
Execution
Ensuring compliance with the Security Policy
Respond to audit questions
Log security breach occurrences
Actions implementation

FIGURE 4.10

Functional macro diagram.

4.7 **ROLE OF THE SECURITY OFFICER**

The Security Officer, acting as the central axis in the general coordination of the corporate information security committee, has a substantial role in the success of the model. He/She is the one who receives all the pressure from the company in face of the results and who is required to adjust the level of control and, therefore, the level of security to meet the demands of the business.

Due to the magnitude of his/her challenge, the professional who occupies this position has to be strictly vertical to the associated functions, without sharing focus and, for such, it is not enough to have an extreme technological profile. This executive must be multi-specialist, have a complete and horizontal vision of information security based on solid concepts, comprehensive knowledge of the GRC disciplines, besides having a rich knowledge on project management, team coordination, and leadership. Must be truly executive, in the full amplitude of the term, wisely nurturing interpersonal relationships, always seeking to achieve commitment.

His/her critical success factor is to keep the alignment and focus on the characteristics and needs of the business, knowing it deeply and constantly adjusting its action plan to the premises and strategic definitions of the company.

Like every executive, must be results-oriented, which can be understood in this dimension as fostering the obtaining of the best return on investments in security, leading the company to operate under controlled risk, as well as preparing it to dynamically manage security, preparing it for current and future challenges.

Important factors for the proper performance of the Security Officer's activity

- Knowing the company's business.
- Knowing the market segment.
- Knowing the company's Business Plan.
- Knowing the expectations of the executive body in relation to his/her activity.

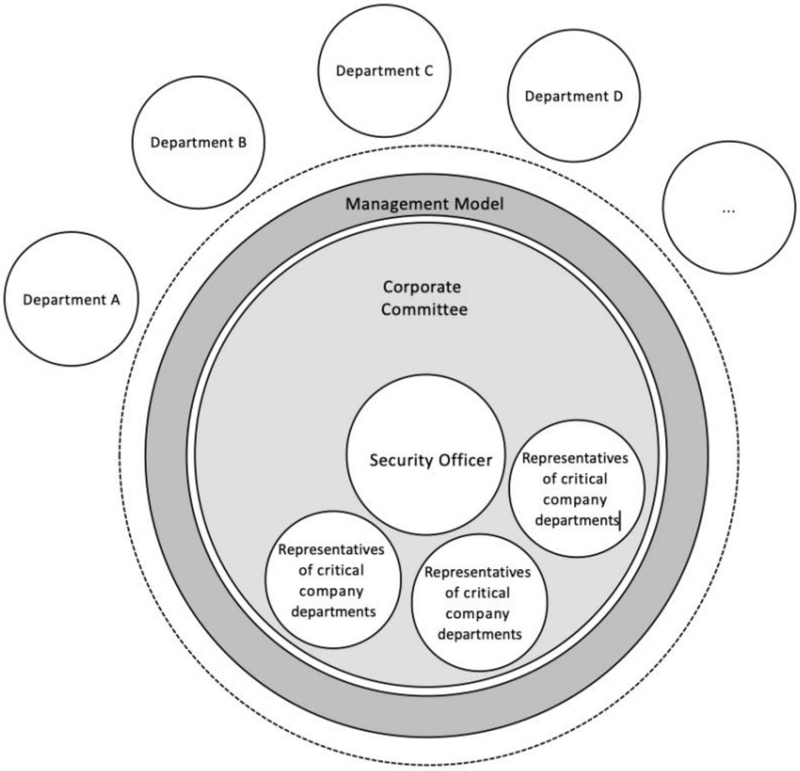

Department A
Department B
Department C
Department D
...
Management Model
Corporate Committee
Security Officer
Representatives of critical company departments
Representatives of critical company departments
Representatives of critical company departments

FIGURE 4.11

Security Officer as the axis of the corporate committee and, consequently, of the security management model.

Security Officer Macro-challenges

- Understand the boundaries of authority.
- Matching the action plan to the security budget.
- Accompany the cultural changes in the company.
- Identifying prepared professionals in the market.
- Organize the security demands of the business.
- Managing physical, technological and human changes.

4.8 **HOW TO CONDUCT INTERNALLY THE NEGOTIATION**

Before thinking about the form, it will be necessary to define the issues that effectively sensitize the executive, making him/her not only understand the challenges related to security, but also its importance to the development of the business, as well as involving the executive in such a way that he/she feels co-responsible for overcoming the challenge and achieving the success of the initiative.

Once the objectives are aligned, it is necessary to touch on the points that sensitize them, in the subjects that converge and are in tune with their expectations and their greatest interests. It is as if adapting the language - technical or managerial - to a different one, contextualized, that makes the short, medium, and long term results of the security solution tangible. I am talking about numbers. Nothing better than the language of numbers and graphs to make oneself understood in the restricted time window the executive will grant us.

Use the slide projection to conduct your explanation, but moderately, without overloading in quantity and avoiding polluting them with unnecessary information. Try to pass clear and consistent messages. Compare the current scenario with the projected scenario resulting from the proposed security solution. Organize your biggest challenges and associate them with the direct and indirect benefits of security. Design an ROI analysis, even if it is limited in scope to specific environments, but do not fail for inconsistency. Gather real and representative information that demonstrates the value added by the initiative. Identify - as proposed in the following list - the reasons why the executive would act voluntarily, and lead him/her to the desired attitude (last on the list).

Main reasons that would lead executives to act voluntarily:

- Fad (occasional action motivated by public opinion).

- Normative (occasional action motivated by external rules and regulations).
- Competitive threat (occasional action motivated by industrial espionage, etc).
- Fear (occasional action motivated by opaque and partial perception of risks).
- Disaster (occasional reactive action motivated by consummated facts).
- Broad vision of the challenges and perception of the benefit to the business (integrated action motivated by understanding the benefits of the corporate solution).

It is important to consider that we will not be dealing with people with standardized, predictable behaviors and profiles. The human being is a complete, non-binary machine and, for this reason, the more information about his/her personality, his/her line of action in the company and their values, the more efficient the approach will be. However, regardless of his/her profile, practically all executives who are on the board of the company have these issues on their agenda of priorities and objectives:

- Adding value to the company's shares.
- Facilitate new businesses.
- Facilitate the exploration of new markets.
- Bonuses and stock options.
- Generate new products and services.
- To be pioneering.
- Fight the competition.
- Increase revenue.
- Increase profitability.
- Increase productivity.
- Reduce time-to-market.
- Reduce direct and indirect costs.
- Reduce risk.
- Manage investor relations.
- Give visibility to results.

- Strengthen the company's image and positioning in the market.

If I had the task of synthesizing in one line, merging all the topics mentioned above as important, I would have no hesitation that the executive's big target is the Annual Net Income (NI). So, always associate your security actions to the positive reflexes that you can cause in the last line of the balance sheet, because it has redoubled weight in decision making.

However, in spite of so many topics and control points, it is common that the executive does not get much time to address the subject; therefore, keep in mind the critical success factors: acting objectively, clearly define the impacts of the lack of security by revealing the current scenario, clearly define the benefits of the security proposal revealing the projected scenario, and define the associated investment amounts.

This may seem like an easy task after all, but the main bottleneck remains the gathering of real information that measures costs and projects risk situations that compromise the operation and generate substantial impacts to the business. As a result, has been constant the execution of a superficial mapping of the security with a restricted scope through an invasion test, capable of capturing a "photograph" of the environment at a given period. In possession of these results - which are usually positive due to the fact that the invasion took place -, you gain power of persuasion and convincing, increasing the efficiency of the approach and the chances of attracting the attention and commitment of the top executive.

Now it is time to take the initiative and prepare for D-day.

4.9 **KNOWING HOW TO IDENTIFY THE OUTSIDE PARTNER**

Considering the dynamism and complexity of the environments, the heterogeneity of technologies, and the diversity of threats, vulnerabilities, and risks, it makes sense to rethink the cost × benefit of taking alone the responsibility for security management.

The first aspect to be analyzed is associated with the investment necessary to technically equip, train, and constantly keep trained a large team of multi-specialists capable of supplying all the current and future new security challenges as they arise. Moreover, we cannot ignore the fact that these investments are not directly linked to the company's core business, thus consuming disassociated physical, human and financial resources, which makes it uninteresting and, many times, unjustifiable.

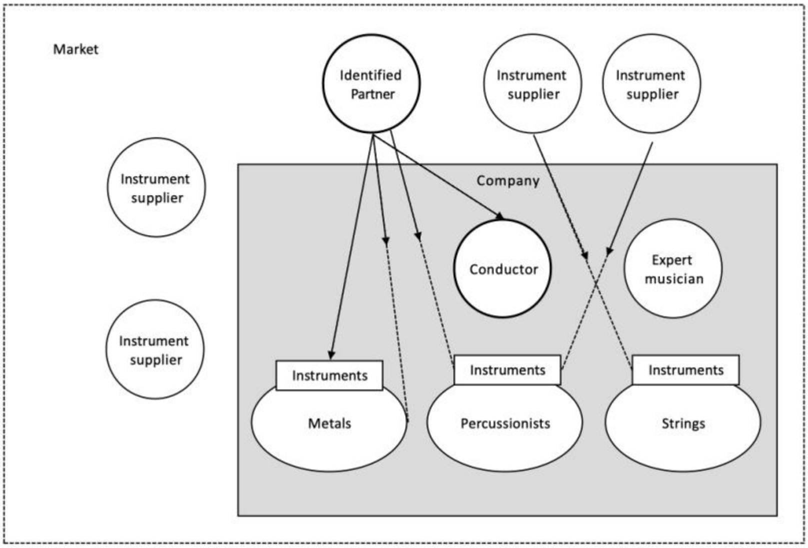
In light of this, a new and difficult challenge arises for the Security Officer linked to the search for companies able to offer complementary external, acting as a true and omnipresent security back office.

Desired characteristics in external consulting:

- Positioning and profile of a consulting and tool integrator.
- Notorious expertise in information security.
- Specificity in information security.
- Multi-specialist technical team.
- Local action with a global mindset.
- Structure of execution of projects capable of making viable simultaneous actions in parallel.
- Methodology for sizing the solution that considers the characteristics and challenges of the business.
- Specific methodology for the execution of information security projects.
- Methodologies in accordance with the international ISO 27002, ISO 27005, and ISO 31000.
- Geographic presence proportional or capable of meeting the characteristics of the company.

- Point of presence abroad, enabling the absorption of experiences, innovations and trends, and facilitating partnerships and technical contacts.
- Proven experience in complex corporate projects.

So many virtues together make the identification of a partner an difficult task, mainly because there are few options in the market capable of supporting large projects and, furthermore, that have in their curriculum the competence to guide their actions to the understanding of the market segment and the strategic guidelines of the of the business in an integrated manner, through consulting behavior. The target of the selection must be a partner with experience and in conditions to act as a conductor of an orchestra, in which the brass - made up of senior specialists in each type of wind instrument - belong to the conductor's own team, where the percussionists - also from the conductor's team - use with harmony the best instruments available in the market provided by various manufacturers and, finally, the strings, performed by the company's own musicians, guided by an expert musician who receives advice from the conductor.



Conductor............................. = Security company partner in advisory support through the Corporate Committee
Expert Musician
Expert musician...................... = Security Officer and team
Metals and Percussionists........ = Multi-specialist managerial and technical resources in various instruments
Strings.................................... = Management and technical resources of the company itself (team of the Interdepartmental Committees)
Instruments............................ = Services or software and hardware products (tools)
Instrument supplier.................. = Security company specializing in specific instruments (tools)
---------------►--------------- = Origin of human or technological resources (tools)

FIGURE 4.12

Relationship of partnership and security back-up.

It is natural and coherent, at a certain moment, to evaluate the new risks inherent to the outsourcing of part or all of the security information actions, considering the accessibility of physical and technological assets, critical information for the company, and the consequent increase in exposure. However, going a little deeper into the analysis, we will soon conclude that it is a rewarding and controlled risk - if the selection of the partner was appropriately meticulous - capable of positively interfering in the result of the cost × benefit ratio.

4.10 **COMPLIANCE WITH SPECIFIC STANDARD**

As it can be observed, there are many variables involved with the security challenge, and they tend to grow as new technologies, new business models and innovations in the commercial relationship emerge.

Motivated by this, in 1995, the British community, led by England, through the BSI (British Standard Institute), created the BS 7799 standard, composed of two parts, where the first part brought together the best practices for information security management, and the second one, published in 1999, a model for the establishment of information security management systems (ISMS), subject to certification of compliance. As the reflections of the lack of security in the world began to be reported and gain visibility, countries in the British Commonwealth, such as Australia, South Africa and New Zealand adopted BS 7799.

Considered the most complete standard at the time, this British standard gained worldwide visibility. As usual, despite the first homologation attempt, the ISO (International Organization for Standardization) followed in its footsteps and, without "reinventing the wheel", tried to analyze the first part of BS 7799, in order to build its version of the standard to address the subject, called ISO/IEC 17799:2000.

The process did not take long, and soon ABNT (Brazilian Association of Technical Standards), operating in tune with ISO, took the ISO 17799 as a reference and made the Brazilian version of the project available for Brazilian version for public consultation. During that time, some committees were created in the country, with important representatives of the public and private sectors, who were able to comment and suggest adaptations to the needs of the Brazilian market.

In 2005, ISO and ABNT renamed ISO 17799 to ISO 27002, thus creating the family of standards associated with information security management. In the same year ISO/IEC 27001:2005 was released, which was the ISO version of the second part of BS 7799, which defined the ISMS and the possibility of certification of companies by the establishment of this type of system.

Recently, in September 2013, ISO released revisions to ISO 27001 and 27002 standards, updating and reorganizing their contents and, above all, seeking a more flexible and simplified approach, in order to ensure a more effective risk management.

ISO 27002 (or its ancestor BS 7799-1) does not have the same characteristics of certification, but suggests, through a less formal model, the concern with important aspects and the use of controls that guide companies to reduce their operational risks, which potentially would cause impacts on business. It brings together, as in a code of conduct, already defined in its title - Code of Practice for Information Security - the topics that must be analyzed, the best practices and, didactically speaking, points out "WHAT" to do, without worrying about the details associated with the "HOW" to do it.

The main objective of the norm is to guide and, based on this, to create synergy between the companies that face the challenge of information security management. In this way, it was possible to seek a "common base" for the development of standards that would strengthen them and make them compatible under the aspect, adding value to the market process by reducing the risks of all the elements of the supply chain, providing confidence in the relationships between organizations.

All versions of the standard, including the Brazilian one, which amendments, deal with wide-ranging aspects, but always revolving the main concepts of security: confidentiality, integrity and availability.

Despite the superficiality of its recommendations, the standard is wide and represents an important instrument to point out the direction for companies concerned with the operation of their business and the protection of the information that sustains it.

"This Standard may be considered as the starting point for the development of specific recommendations for the organization. Not all the recommendations and controls in this Standard can or should be fully applied. Moreover, additional controls not included in this Standard may be necessary and complementary. Whether that be the case it may be useful to maintain a cross-reference to facilitate verification of compliance by auditors and business partners."

According to the transcribed text of the standard, one can note the concern in disassociating the standard from the figurative role of a TRACK, attributing to it the purpose of a TRAIL capable of pointing the direction without, however, generating compulsory and inflexible standardization, which certainly would not be compatible with the dynamism of the companies, their environments, the changes in their physical, technological and human assets.

The ISO 27002 standard, already considering the 2013 version, has 18 sections, the first four of which are considered introductory and the other 14 sections (or domains) organized into 35 objectives of controls that expand into a total of 114 suggested controls. The standard serves as support and detailing of the aspects necessary for implementation of the ISMS as described in ISO 27001.

Reminder

BS 7799-1:1995 generated NBR ISO/IEC 17799:2000, subsequently NBR ISO/IEC 27002:2005 and, subsequently NBR ISO/IEC 27002:2013.

BS 7799-2:1999 generated NBR ISO/IEC 27001:2006 and, subsequently, NBR ISO/IEC 27001:2013.

Trend

Just as happened with the ISO9000 quality standard, which gradually gained the confidence and credibility of companies in all segments and fields of activity, we have identified in recent years a new movement in the corporate environment in search of harmony, conformity and, consequently, certification based on the information security standard.

As the first and important players in the market started the movement, we soon saw several others shaken by the positive fever for adequacy and compliance. The concern with information security already transcends the technological aspect and the physical and logical limits of the company, seeking - and, later on, demanding - the same harmony and conformity with the other partners of the supply chain.

Regarding this scenario, it is not appropriate that your company is the last to move. If you were not the pioneer, do not be late and extract from it - which is already one of the main restructuring of companies in this century - the benefits linked to this still important and powerful competitive differential for your business, but which may soon turn from a differential into an obligation.

4.11 **NORM VERSUS METHODOLOGY**

The fact that there are already national and international standards code of conduct for information security management does not completely solve the challenge that companies face. This happens because the norm has the clear role of only pointing out the aspects that deserve attention, indicating WHAT to do for the adequate management without, however, indicating with methodological precision HOW the activities should be carried out.

It is the same as being instructed to perform an annual check-up of our health status, considering the respiratory, circulatory, digestive systems, etc., without knowing exactly how to do it, but to seek a specialist. This specialist, in turn, having the specificity, will apply all his/her knowledge base, following, with the richness of detail and precision inherent to the activity, a methodology of his/her own, a great "manual" that will allow to consider all the important points for analysis and will point out the most appropriate tools for each type of examination.

It is, in fact, an unfolding with procedures based on a larger standard, such as ISO, that will point out how examinations, or rather activities, should take place, how the instruments are to be handled, and also how the results are to be interpreted for a consistent diagnosis of the state of health and subsequent suggestion of treatment and medicine.

Therefore, it is useless to be aware of the controls and aspects ruled by safety norms if you do not have a consistent methodology, capable of guiding the activities, transforming them into real results connected to the reduction of risks.

In the time when the companies had a low degree of exposure (due to low computerization, connectivity and sharing) and the perception of security did not transcend the physical aspects, the need for a methodology was little perceived. However, as the risks, threats and impacts became more present and representative, and there was a more refined and correct perception that security is not limited to technology, but also considers physical and human aspects, the volume of problems and vulnerabilities have grown exponentially. The surveys and implementations became, then, deeper, more accurate and, consequently, the proportional increase of the critical mass made the analysis and management process even more complex. Therefore, the adoption of a methodology became a critical success factor to support the increasingly complex action plan, or better, the security master plan.

Examples of methodological tools:

- Vulnerability Mapping Form
- Form for mapping critical business processes
- Form for guiding the conduction of interviews
- Worksheet for the identification of physical, technological and human assets
- Worksheet to study sensitivities to security breaches
- Instrument for topological mapping
- Criticality matrix for prioritizing actions
- Downtime tolerance matrix

Unlike the norm that aims to guide everyone in the sense of building a common basis of conduct, there will not be a single recommended methodology. Many of them will emerge simultaneously at the hands of many companies in many different countries, but all must be aligned with the guidelines of the standard, while being adapted and contextualized to each market, considering the local culture and the internal and external variables that interfere in the company.

In fact, today we have several systems and applications in the market that help automate this process, whether in the universe of security, focused on the implementation of information technology controls, or in the comprehensive universe of GRC.

Finally, it is already possible to notice that, after being successively applied and constantly adapted over time, some of these tools eventually gained greater visibility and prominence, becoming international references, adopted by several companies. For reference, we suggest consulting, for example, the documents of the Gartner Institute and Forrester Research documents on the GRC market.

Chapter 5

Knowledge

Checkpoint 2

This knowledge checkpoint is a brief and objective consolidation of the concepts covered in each section of the book with the objective of reinforcing the process of absorbing the relevant content.

Security Concepts

CONCEPT: Solid concepts and their clear understanding are the raw material that will imply the quality and outcome of the work.

Perimeter Theory

CONCEPT: Knowing how to segment physical, technological, and human assets according to the similarity of their criticality and importance (value to the business) is the basis for the specification and application of the right controls that will offer the level of protection adequate to each profile and need.

Security Barriers

CONCEPT: Knowing the barriers to protection and seeking synergy between them is not sufficient without a diagnosis capable of associating assets and business processes, transcending the mapping of technological failures and identifying the company's risks by analyzing the trinomial people, technology, and processes.

GRC

CONCEPT: GRC is an acronym that describes an integrated organizational approach to governance, assurance and management of performance, risk and compliance (OCEG), in order to ensure the achievement of objectives without losing focus on existing uncertainties and always acting with integrity. Risk and compliance management is very closely aligned to information security management, mainly in what concerns the establishment of controls, while governance ensures the balance and the association with business objectives.

Risk Equation

CONCEPT: Each company will have its own personalized risk equation. A true dashboard that will signal situations of controlled risk, situations of fluctuating risk, and situations of intolerant risk.

Corporate Information Security Committee

CONCEPT: Backbone, the corporate committee must be consistent, dynamic and flexible, officially representing the company's interests in the face of business challenges.

Role of the Security Officer

CONCEPT: Explicitly define the Security Officer's responsibilities towards the result, but provide him/her with the adequate instruments to enable his/her activity.

How to conduct internally the negotiation

CONCEPT: To conquer the commitment of the company's executive body is a sine qua non condition to obtain the appropriate dimensioning of the financial resources that will subsidize the structure of the corporate information security management model. Therefore, be convincingly consistent make it perceive security as an investment, and not as an expense.

Knowing how to identify the outside partner

CONCEPT: The choice of the partner that will fulfill the role of security backstop will define the success or failure of the initiative, so gather particular information about the candidate that ratify its notorious specialization, experience, and above all, commitment to deliver final corporate results and aligned to the strategic guidelines of the business. After all, no one looks for just any doctor when have to operate the heart.

Compliance with specific standard

CONCEPT: By structuring itself to manage information security from a dynamic and flexible model, it is fundamental to follow the movements of the local market, its partners in the supply chain, and also the international movements. Try to be in synergy with the concepts and initiatives of national and international standardization in order to provide the best return on investment and still allow you to enjoy a unique position of prominence.

Norm × methodology

CONCEPT: Guided by the safety standard, do not start activities without basing them on a consistent methodology even though - in hypothesis - you may have to develop it, or you may have to identify a successful one in the market, or have to check if your outside partner has a consistent methodology with a positive track record.

Chapter 6

Orientation to the Security Officer

After we have covered, in the previous chapters, the most relevant aspects to guide companies, helping them to achieve success and overcome the challenges of managing information security, the time has come to explore some more practical issues, orienting the executive responsible for the entire coordination of the process: the Security Officer.

6.1 **CORPORATE SOLUTION ON INFORMATION SECURITY**

Perhaps there are still doubts about the expression - and no wonder, after all, many pieces of the puzzle have been identified by this stage of the book, but we have not yet put them together to form a single picture. The time has come to do so.

We should call a corporate information security solution the result of creating a corporate structure properly positioned in the organization chart, called the corporate information security committee, based on a dynamic management model, with autonomy and scope, coordinated by an executive in focused action, entitled Security Officer. This executive, supported by its own team or outsourced in the tactical-operational sphere and by representatives of departments or managers of critical processes in the executive sphere, all guided by a security master plan custom developed and aligned to the strategic guidelines of the business, will organize the activities in search of the adoption of controls that the risks to the operational level defined as ideal. In this way, you will be enabling the best return on investment, reflecting, consequently, in greater benefit for the business, where it reads: higher net profit for the year.

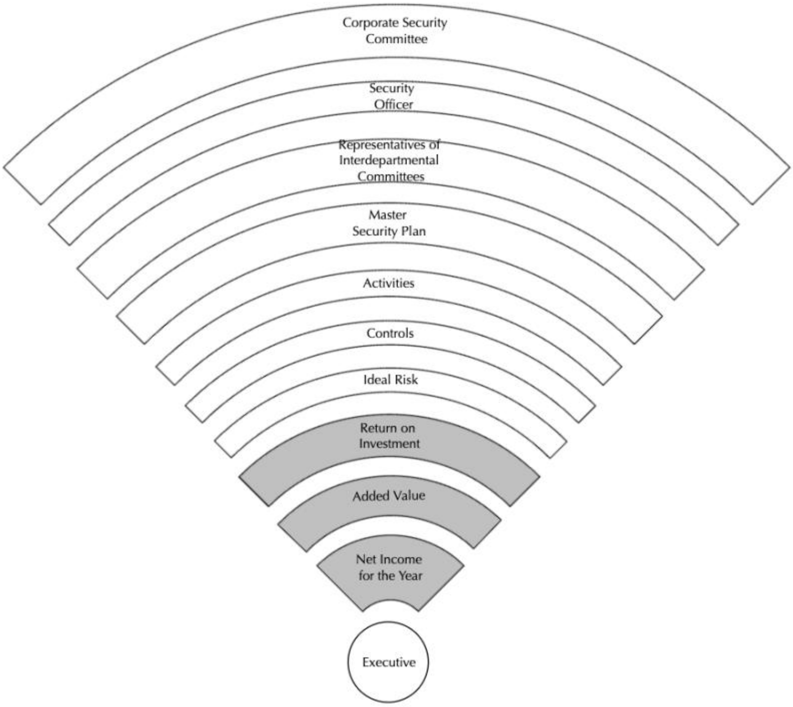


FIGURE 6.1

Cascading view of the corporate information security solution and its tangible results.

Perhaps a few words can help us understand such complexity, and if I had to choose one to represent the macro-challenge of the security solution - capable of signaling all associated aspects - it would be: CONTROL.

That's it. Control is all that is needed - from the perspective of the application - effectively to manage vulnerabilities and reduce risks. It is with control that you will be able to, for example, authorize or block people who try to enter restricted physical environments; register the attempts to access the Internet website; measure the damage caused by security breaches; inhibit attempts to attack the router; avoid the disposal of critical printed material without adequate care; to signal the drop in productivity of employees; point out the best practices to transport information in magnetic media; prevent sabotage and fraud attempts; perform and measure the efficiency of awareness and training of technicians and users of the corporate network; and react with speed and efficiency in crisis situations and security breaches that are predictable and often unavoidable, etc.

Many would have mistakenly chosen the word BLOCK or PROHIBITION, but, in fact, the main objective of a corporate security solution lies in the specification and application of control mechanisms that lead the risks to the level predefined as ideal for the company (and this varies from company to company), in order to avoid and minimize impacts in the business in time of handling, storage, transport, and disposal of information.

Another word that can help us and is equally important for security is SEGMENTATION. Considering the particularities that differentiate one company from another and, furthermore considering that a single company has information with distinct importance and distinct values, flowing through various environments and sustaining business processes, we come to the conclusion that the physical, technological and human perimeters of this company will need different levels of security, always seeking to identify and apply the ideal "dose". In this way, knowing how to intelligently segment the company and bring together the pieces, that is, the activities that will compose the solution, we will be enabling the effective reduction of risks and the real increase in business security, without depreciating its commercial and productive processes, etc., with excessive bureaucracy, loss of agility and competitiveness (see Figure 6.2).

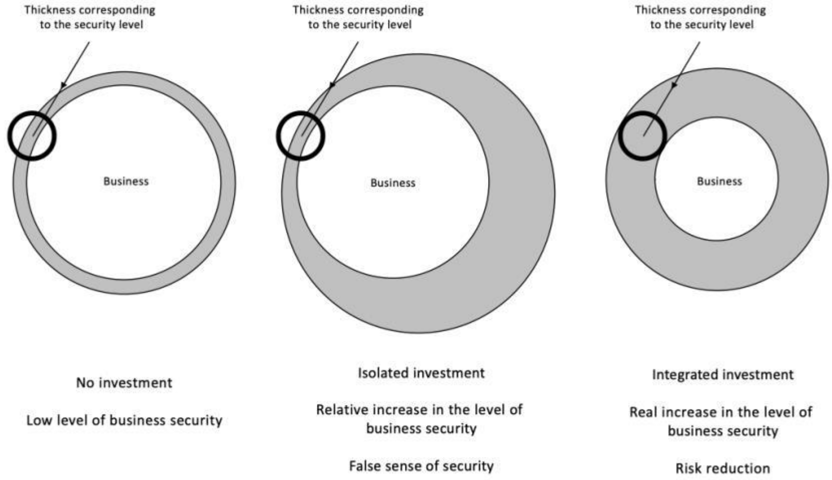

Thickness corresponding to the security level
Business
No investment
Low level of business security
Thickness corresponding to the security level
Business
Isolated investment
Relative increase in the level of business security
False sense of security
Thickness corresponding to the security level
Business
Integrated investment
Real increase in the level of business security
Risk reduction

FIGURE 6.2

Figurative overview of the stages and main objective of the information security solution.

Objective

The solution can be very well perceived - from an application point of view - as a large set of building blocks that fit together smoothly, if well shaped and guided by the customized "template" of the security master plan. Put together, they will form a mosaic, a solid but flexible and dynamic structure that will support the company in building a contextualized management model in order to overcome the current and react adequately to future challenges associated with the control of information security risk.

The pieces are activities or projects with the most diverse purposes and of distinct natures. Following the organization model proposed by ISO 27002, originally inspired in the PDCA model adopted in ISO 9001 and which has synergy with the conceptual studies of security, we have the following phases:

- PLAN (planning)
- DO (implementation)

- CHECK (analysis)
- ACT (monitoring)

It is important to note that these four phases are applicable to the organization of all activities that are part of the security solution, and should also guide the sub-activities (see Figure 6.3).

As an exercise, we can say that it is necessary to plan the executive actions (security master plan) to make adequate investments and organize the Security Office. In the same way, it is necessary to analyze the risk factors of the business that will point out the characteristics and gather information to support the dimensioning of the actions. Implementing the physical, technological and human controls is the next step, followed by the monitoring phase, which will be linked to the first, providing it with information of new failures, threats, and risks (see Figure 6.4).

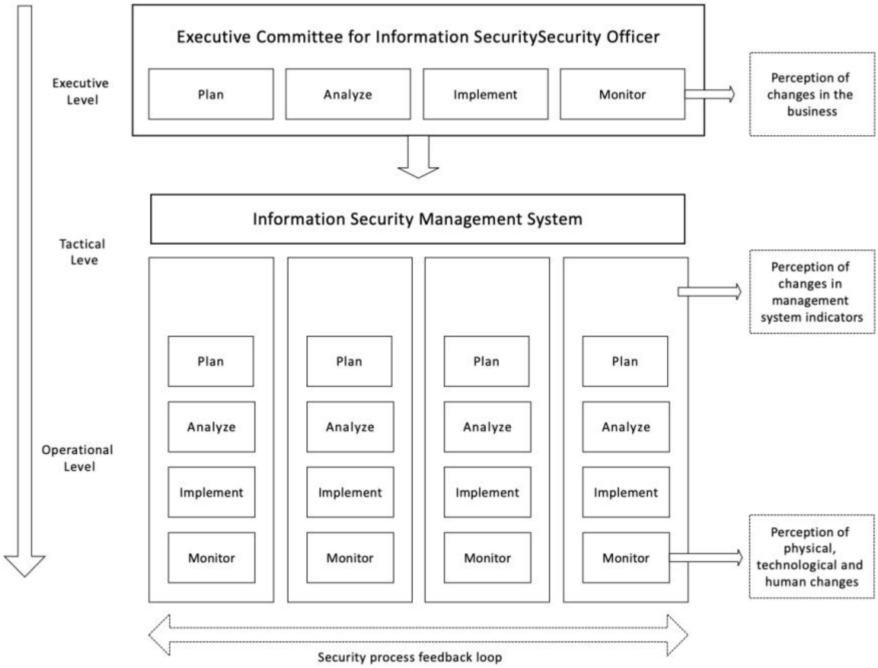

Executive Committee for Information SecuritySecurity Officer
Executive Level
Plan
Analyze
Implement
Monitor
Perception of changes in the business
Information Security Management System
Tactical Leve
Perception of changes in management system indicators
Operational Level
Plan
Analyze
Implement
Monitor
Perception of physical, technological and human changes
Security process feedback loop

FIGURE 6.3

Overview of the applicability of the PDCA model at the multiple levels.

Going down one more level, that of the activities that make up each of the four phases, we will see, once again, the applicability of the same model. Resorting again to the exercise, we can plan the scope and the sub-activities performed in a risk analysis, analyze the results obtained during the interviews (physical analyses and technical analyses), implement the emergency measures, and finally, monitor the indexes and indicators that may alter the level of risk of the scope of the analysis.

Phases

Plan

Includes activities that aim to define architectures, actions, activities, continuity alternatives, and criteria, encompassing the entire information life cycle: handling, storage, transport and disposal, applicable from the operational to the most strategic levels, which will serve as a guide.

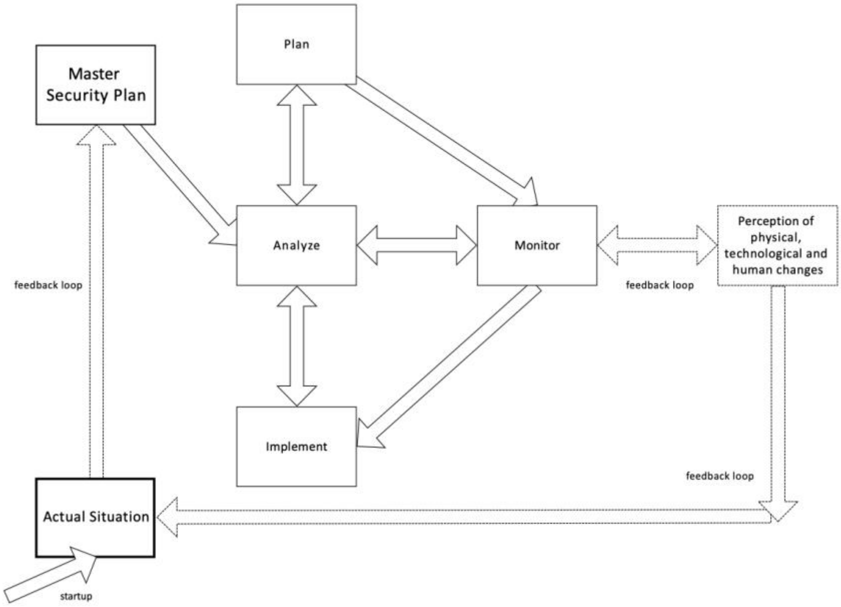


FIGURE 6.4

Macro-flow of activities.

- Security Master Plan
- Business continuity plan
- Information security policy

Check

Comprises activities that seek to generate a security diagnosis, through mapping and identification of physical, technological and human particularities of the company as a whole or of smaller perimeters, vulnerabilities, threats, risks, and potential impacts that may reflect on the business.

- Risk Analysis
- Penetration test

Implement (Do)

Comprises activities that apply control mechanisms to physical, technological and human assets with vulnerabilities, seeking to eliminate - when possible and feasible - or manage them, in order to increase the level of security of the business. It is the phase that materializes the actions considered necessary in the diagnosis and organized by the planning.

- Implementation of security controls
- Security training and awareness

Monitor (Act)

Comprises activities that aim to manage the security level, through devices that monitor indexes and indicators, channeling new perceptions of physical, technological and human changes that cause oscillation in the degree of level of risk, in order to adjust the security actions to the context. It is the phase that represents the link with the others, forming a continuous cycle, giving life to the true dynamic management process.

- Incident Response Team
- Security management and monitoring

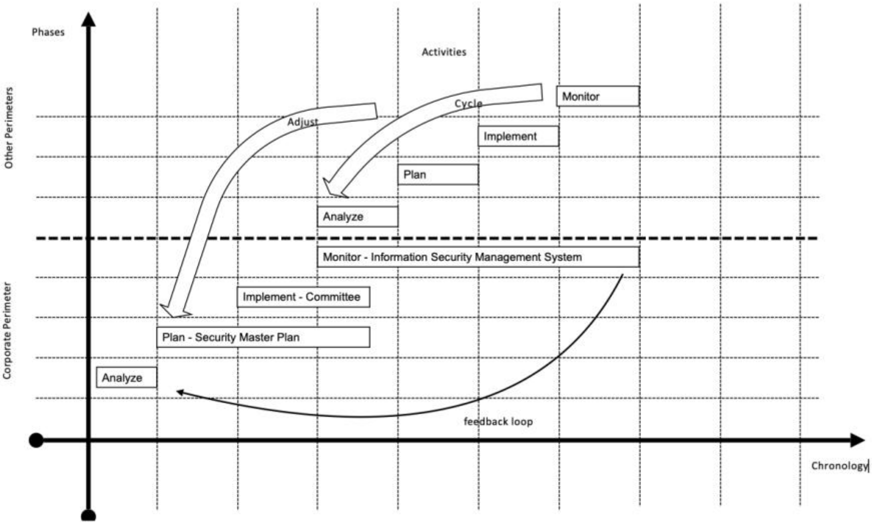


FIGURE 6.5

Example of activity chaining.

Because of the very nature of the activities, there is a natural sequence of execution, making their final products connect to each other, feeding into the next activity, and linking the last step to the first, in a way that establishes a continuous cycle of risk maintenance. We can see in the diagram in the example the moment when the needs and corporate characteristics were analyzed, generating a security master plan, which, in turn, was supported by the implementation of a security committee/Security Office. Next, a set of criteria, indexes, indicators and metrics for monitoring that fostered the creation of the information security management system.

Because of the fundamental role played by the security master plan, we will explore it, in detail, in the next chapter.

It is important to note that the executive or corporate-wide activities will serve as a guide for all the activities that will occur in the other perimeters of the company. This synergy allows the integration of the work, avoids redundancies, disproportionalities of investment and, mainly, that the concept of building blocks is implemented. That way, the company will be able to break down security actions into integrated parts that, little by little, will build a corporate-wide management model.

This movement is closely linked to the proposed management system and in tune with it by the ISO 27001 standard: ISMS (Information Security Management System).

6.2 **SECURITY MASTER PLAN**

Planning is the critical success factor for the initiative to managing information security, and the security master plan is precisely the specific element to this goal. More than a budget line for technological investments as the already traditional IT master plan suggests, the PDS has to be dynamic and flexible to support the new security needs that arise due to the speed in which the corporate context changes.

Didactically speaking, the security master plan represents the compass that will point the way and the steps (activities) that will form the mosaic of the solution and meet the security needs of the business, leading it to operate under controlled risk. It is important to realize that this compass must be specified tailored to each company. There is no one model plan that is capable of serving every type of company, no matter whether they are companies of the same size and in the same market segment. There are intrinsic particularities, such as threats, risks, sensitivities, impacts, and physical, technological, and human vulnerabilities that make the problem unique. Therefore, following the analogy with medicine, this patient will have to be treated by a unique, personalized medicine prescription, able to cure and stop the disease that is also unique. So, we are facing the first step, the first challenge of the Security Officer: how to dimension a security master plan?

Methodology

The beginning of PDS modeling is directly associated with actions of gathering business information , similar to a medical appointment, in which, besides the initial anamnesis, exams and tests are performed to diagnose the patient's symptoms, abnormalities and potential risks of the patient, that is, to identify threats, vulnerabilities, risks, and potential impacts to the business.

It is crucial to understand the challenges of the business, to know the short, medium and long term plans, and the demands that are to come as a result of the Business Plan. As much as the security actions do not directly impact the business processes, all business processes, all of them will have to be guided by them; therefore, the objective is, in this preliminary phase of the survey build a relationship map and dependency among business processes, applications, and physical, technological, and human infrastructure (see Figure 6.6).

This is a task of a complex nature, especially when it comes to a large company, because it is difficult to find an accessible, small, and cohesive group that is capable of having a broad and complete corporate vision. In addition, the complexity of environments, the heterogeneity of technologies, multiple hybrid accesses, geographic decentralization, and the predictable distribution of security responsibilities across departments become complicating factors, so take them into account.

Accordingly, the methodology comprises six distinct steps that complement each other, fostering a consolidated vision of the business that will support the modeling of a customized security master plan.

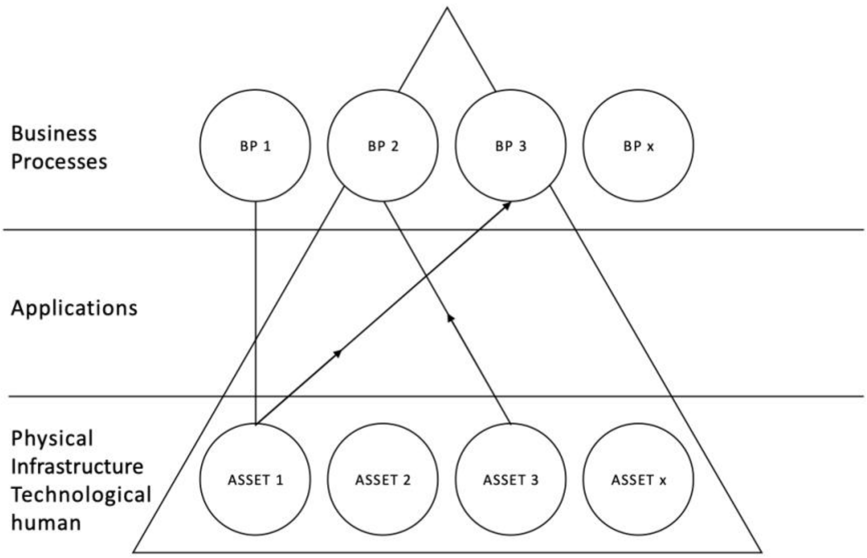


FIGURE 6.6

Relationship map between business processes and infrastructure.

1. Identifying the business processes

Gathering the main managers with representation in the company, previously identified commonly in the executive-managerial level, the work begins with the objective to identify - through interviews and brainstorming - the critical business processes that will be the target of the activities that will compose the solution. Starting from the premise that security actions must focus on the business and on the information that sustain it, it is essential to list the most sensitive processes. It is as if we were to ask the patient what pains he/she is feeling and their location. In addition, we seek to identify the physical, technological, human, and connectivity needs of these processes for the functioning of the entire business.

Once again, over using analogies for didactic purposes, I use the comparison of the company with an automobile engine. Think of different engines, representing different companies. In this way, this preliminary stage of the initial objective of identifying the most critical and representative parts to ensure the performance and the functioning of the engine, that is, the business.

Remember that during this step it is customary to guide the identification of critical processes based on their resulting financial and strategic results; therefore, it is important to involve company representatives who can share information about that transcends the operational aspects.

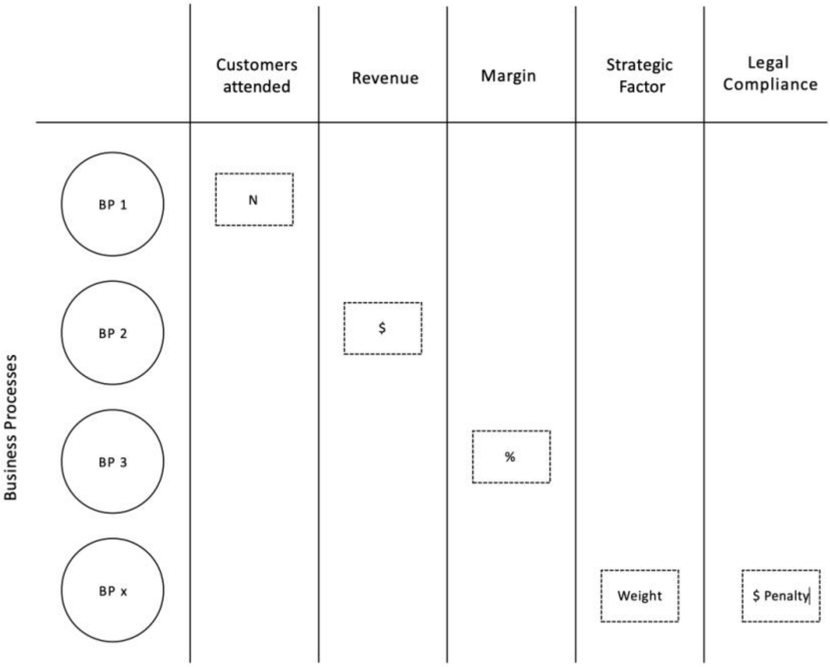


FIGURE 6.7

Examples of units of measurement considered for identifying critical business processes.

2. Mapping Relevance

Knowing better how the business works, after having coherently broken it down after identifying the critical processes, the time has come to map the relevance of each of them, in order to avoid discrepancies in the prioritization of the activities that will compose the solution.

Returning to the didactic analogy of the human body, this step is similar to the need to score the organic functions, signaling those that deserve more attention, importance, and priority. After all, in a life-threatening illness, would you, as a physician, give priority to the treatment of a bladder or a heart injury? Would you treat the circulatory or the digestive system in this case?

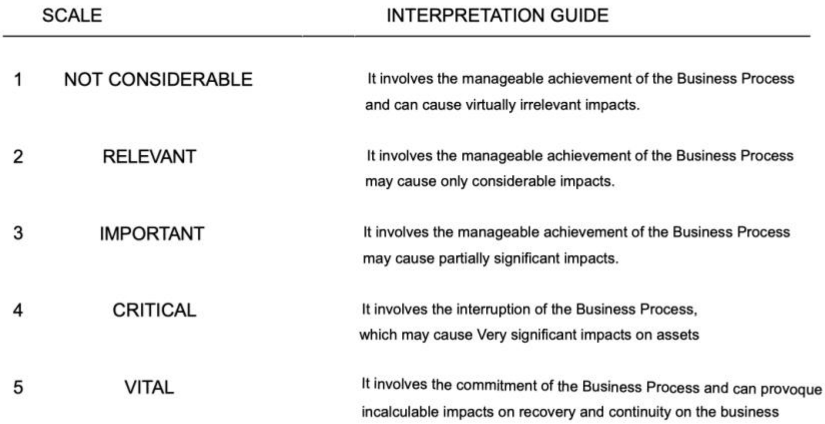
To properly map the relevance of each critical business process (relation of consideration between them associated to the importance to the business), it is necessary to involve one or more managers who share a corporate perspective - knowing the global operation of the business - without being directly and exclusively involved with one or more specific processes, or that has impartiality when it comes to weighing the importance that will guide the prioritization of actions in subsequent steps.

Criteria

The methodology applies values within the range 1 to 5 to indicate the degree of relevance, and this number is directly proportional, increasing in relevance as the score approaches 5. In addition, the association of the scales with words and expressions makes the mapping process more elucidative, making it easier for those involved in measuring the relevance between the processes. However, it must be careful not to generate a misinterpretation of the expressions adopted in the scales. They should be seen only as a way of weighing and measuring the importance of each business process and should not be interpreted in isolation. This would provoke the inevitable question: "If process XPTO has already been pre-selected, how can it now be classified as NOT CONSIDERABLE?"

Thus, the best way to conduct the analysis, qualifying it, is always to induce managers to reflect on the importance of the target process for the operation of the business, adjusting (re-assessing), throughout the interview, the relations between all the business processes.

By applying, in a holistic way, these criteria to the business processes, we will subsidize the other steps with weighting parameters that will help in the interpretation of the studies that will be conducted on each of the processes separately, relying on the segmented vision of each one of its managers.



SCALE		INTERPRETATION GUIDE
1	NOT CONSIDERABLE	It involves the manageable achievement of the Business Process and can cause virtually irrelevant impacts.
2	RELEVANT	It involves the manageable achievement of the Business Process may cause only considerable impacts.
3	IMPORTANT	It involves the manageable achievement of the Business Process may cause partially significant impacts.
4	CRITICAL	It involves the interruption of the Business Process, which may cause Very significant impacts on assets
5	VITAL	It involves the commitment of the Business Process and can provoque incalculable impacts on recovery and continuity on the business

FIGURE 6.8

Scale table for rating the relevance of business processes.

Expected result of this step:

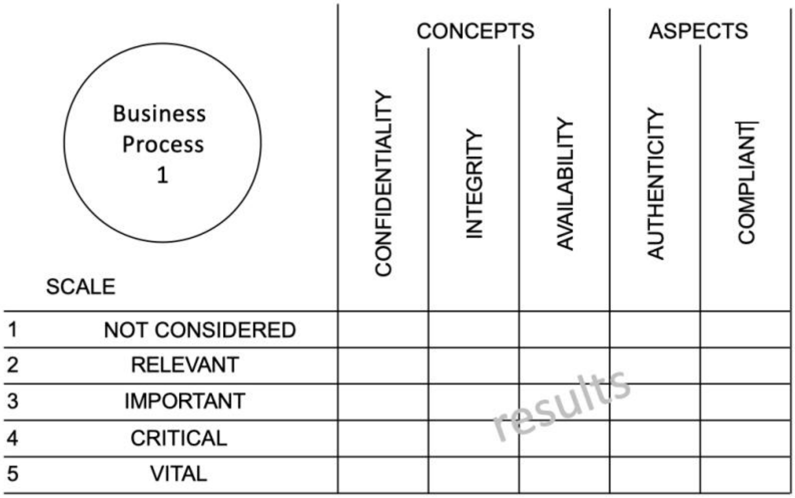
- Mapping the relevance of the critical business processes.
- Involvement of managers with a holistic view of the business.
- Perception of the important factors considered by managers involved.

3. CIDAC[3] Study of Impacts

Once the critical business processes have been identified in the previous activity, it is time to conduct studies that will indicate the sensitivity of each of them in the face of a possible security breach, specifically the concepts of confidentiality, integrity, availability, and the aspects of authenticity and compliance. The study is carried out through isolated interviews with the manager of each process and the same criteria of the classification scale used in mapping relevance are applied again, but this time without considering the business as a whole.

To better understand how business processes would react to the possibility of a breach of the three concepts and two aspects of information security, by measuring their sensitivity, represents an important detail to help in the sizing and modeling of the security master plan, which will occur in the final stage.

[3] In other sources, you will find in this model reference to legality as one of the aspects to be evaluated regarding the sensitivity of business processes to a possible security breach. Consistent with what we defined in Chapter 4, we have changed the model to include compliance as the aspect to be evaluated instead of legality, given its broader scope.



Business Process 1		CONCEPTS			ASPECTS	
SCALE		CONFIDENTIALITY	INTEGRITY	AVAILABILITY	AUTHENTICITY	COMPLIANT
1	NOT CONSIDERED					
2	RELEVANT					
3	IMPORTANT					
4	CRITICAL					
5	VITAL					

FIGURE 6.9

Scale table for rating the sensitivity of business processes.

Expected result of this step:

- CIDAC sensitivity rating of each business process.
- Involvement of managers with an isolated view of specific processes.
- Insight into the important factors considered by managers involved.

4. GUT priority study

Still meeting individually with the main manager of each business process listed as critical, we begin the stage of study and scoring of priorities, applying the GUT matrix: gravity, urgency, and tendency.

The definition of the final priority is composed of the analysis and product of the three GUT dimensions, following this model for conducting the questionnaires:

Gravity Dimension

- It would be very serious for the business process under analysis if any fact were to affect any of the concepts and aspects, causing a breach in the security?

This line of analysis must consider the *severity* of the impacts directly and exclusively associated with the analyzed business process.

For example: what would happen to a financial institution's credit approval process if the client database - main raw material of the activity - *were corrupted*, with its integrity compromised?

Urgency Dimension

- If information security is breached regardless of the concept or aspect affected, what would be the urgency to solve the effects of what happened and to reduce the risks in the business process under analysis?

This line of analysis must consider *the duration* of the associated directly, and exclusively, with the analyzed business process. For example: what would become of the credit approval process of a financial institution if the client database - the main raw material of the activity - *remained corrupted* for two consecutive days, having its integrity attained?

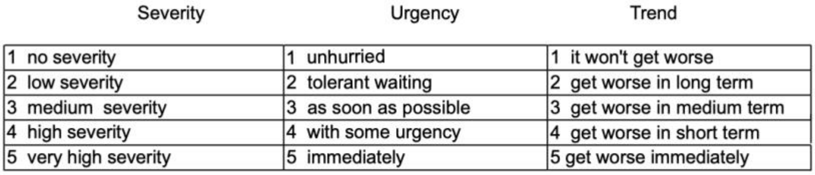
Tendency Dimension

- Considering the short, medium and long term plans associated with the evolution of the business process under analysis, what would be the trend of security risks if no preventive or corrective activities were applied?

This line of analysis must consider the *oscillation of importance* of the impacts associated directly and exclusively with the analyzed business process. For example: what would become of the credit approval process of a financial institution if the client database - the main raw material of the activity - were *corrupted in the short, medium and long term* with its integrity compromised?

Criteria

The methodology applies values within the range 1 to 5 to indicate the degree of priority, and this number is directly proportional, increasing the prioritization as the score approaches 5. In addition, the association of the scales with words and expressions makes the mapping process more elucidative, making it easier for those involved to measure the priority among the processes. However, it must be careful not to generate a misinterpretation of the expressions adopted in the scales. They should be seen only as a way of weighing and measuring the importance of each business process, and should not be interpreted isolated.



Severity	Urgency	Trend
1 no severity	1 unhurried	1 it won't get worse
2 low severity	2 tolerant waiting	2 get worse in long term
3 medium severity	3 as soon as possible	3 get worse in medium term
4 high severity	4 with some urgency	4 get worse in short term
5 very high severity	5 immediately	5 get worse immediately

FIGURE 6.10

Scale table for prioritizing business processes.

Because they are dimensions that make up the GUT, pointing out the priority of the business process in relation to the others, the values are multiplied, generating the final GUT; this way, the final possible value range is from 1 to 125.

Aiming to facilitate the quick identification of processes and their priorities, the final GUT is positioned in blocks identified by colors, in which the ranges from 1 to 42, 43 to 83 and 84 to 125 are signaled, respectively, by the colors GREEN, YELLOW and RED, respectively.

Expected result of this step:

- Mapping the priority of each business process.
- Perception of the characteristics of each process according the GUT dimensions.

5. Study of perimeters

Continuing the security master plan methodology that aims to build a relationship and dependency map among business processes, applications, and physical, technological, and human infrastructure, the study of the assets that support each of the business processes. This is justified by the technical profile of many activities that will make up the corporate information security solution and, therefore, by the need to identify the infrastructure targets that are directly and indirectly related to each of the business processes treated individually (see Figure 6.11).

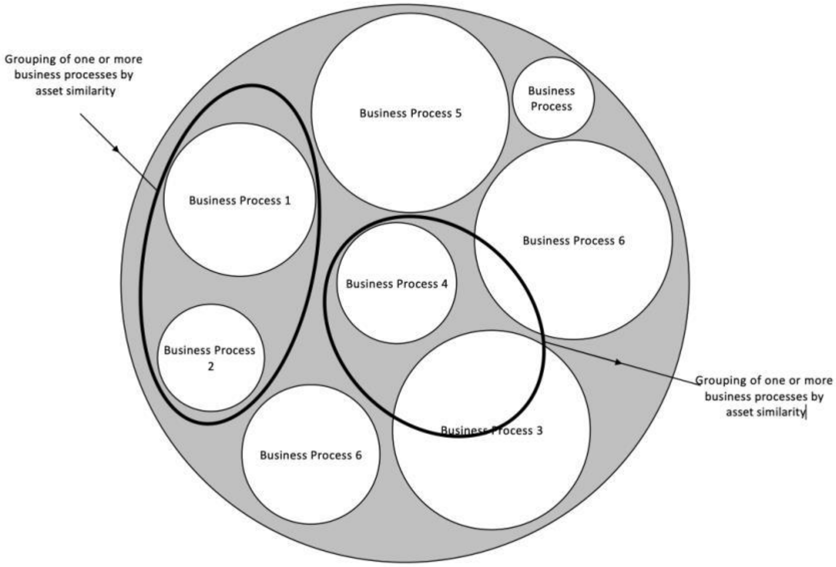


FIGURE 6.11

Hypothetical representation of the division of the company into business processes and the consequent groupings based on the similarity of the physical, technological, and human assets that support them directly or indirectly.

In possession of the process mapping, we already have the elements that generate pain, their location, the possible impacts on the body if affected, and the priority to reduce the impact risks, the time has come to identify the assets - infrastructure, technology, applications, information, and people - that sustain and support business processes. According to the aspects and concepts of information security, the assets have vulnerabilities that should be eliminated, minimized and managed by the actions of security controls. Differently from the previous activities, this one brings together interviews with the main managers of the technical-tactical sphere who will gather numbers and topological information, physical and technological, directly and indirectly linked to the business processes.

Given this, the activity becomes primordial so that the projects necessary are identified and become part of the security master plan.

It is common, in this stage, to request floor plans that reveal the secrets of the physical environment, topological maps, inventory of equipment, systems, and applications in the most diverse platforms. Remember that this is the moment to discover which assets are behind the functioning of the business processes. Everything that is important to your operation must be listed, even seeking to identify its operation, information exchange relations, and data flow (see Figure 6.12).

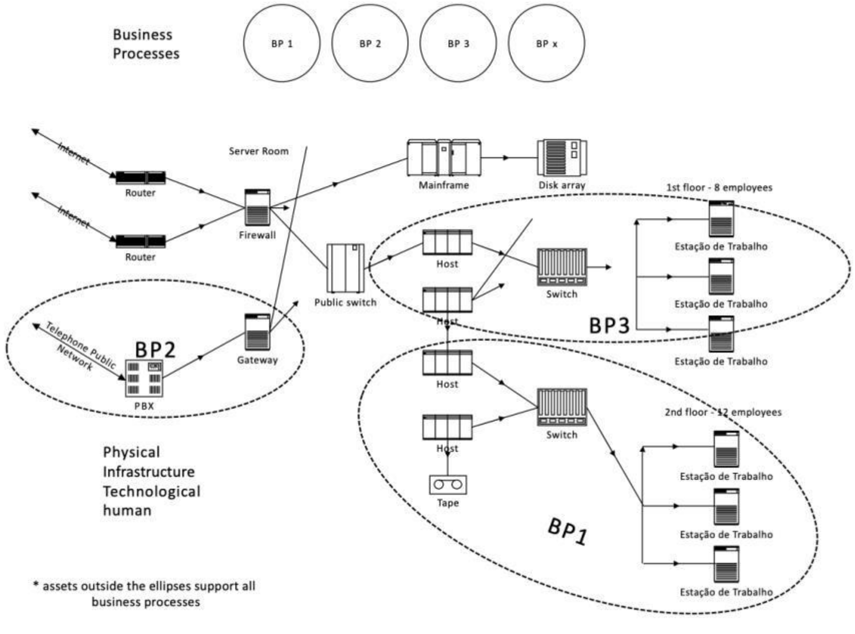


FIGURE 6.12

Illustration of the relationship between assets and business processes.

Once again overusing the analogy with the human body, as if we did not know its engineering functioning, the goal of this step is to find out which organs, functions and biological elements are used by each the respiratory, circulatory, digestive, etc. systems.

Only by obtaining an accurate mapping can we define activities and their priorities in subsequent steps.

Expected result of this step:

- Asset mapping.
- Mapping of the relationship between assets and business processes.

6. Activity Study

This is the time for the medical specialist to analyze the pain complaints, the test results, the context, usual behavior, and the present and future needs of the patient (according to his/her plans) to dimension the corporate security solution, composed of projects that will support the modeling of the PDS.

It's time to plan the actions that will take place in distinct and isolated perimeters, but that will be coordinated and, above all, will be in compliance with the company's security guidelines, proposed by the corporate information security management model.

This step begins the process of preparing the security master plan, indicating the necessary activities/projects and distributing them over time and according to the priority extracted from the perception of relevance of the business processes.

It counts on numerous meetings for the analysis and interpretation of the information collected, crossing them with the business plans, available resources, and the current security level versus the recommended one for the nature of its activity.

Expected result of this stage:

- Asset mapping.

- Mapping of the relationship between assets and business processes.

Organization of the corporate security committee

Parallel to the information gathering and diagnosis activities, it is a critical success factor to start organizing a group, conventionally called the corporate security committee. The first activity is to define the responsibilities for planning, execution, monitoring, their positioning within the company's organization chart, ensuring that they have access to decisive spheres that can act on the entire corporation. The next step is the internal disclosure and make this group official, made up of representatives from various strategic areas of the company, bringing together distinct specialties and visions. Its main role will be to organize, concentrate and plan the security actions that will interfere in all environments and processes, having the possibility of redirecting the plans according to the physical, technological and human changes that will inevitably occur.

Security Office Organization

This position must officially exist within the company whose responsibilities and skills are directly associated with leadership of the corporate security committee and interaction with interdepartmental security committee leaders. Technical profile, corporate vision, and management skills are fundamental elements to channel efforts in a way that is coherent with the macro-objectives of security and the business itself. By the way, business and security should coexist in harmony, with the former pointing out the needs, strategies, and necessities of new applications, and the latter striving to reduce the risks and the potential impact through well-deployed corporate controls. The Security Officer has to be a mediator, a mentor, a questioner, analyzer of threats, risks, impacts and the consequent feasibility study of next steps.

Organization of inter-departmental security committees

With a smaller scope, these committees play an important role in the information security management model. Although they are being guided by larger guidelines in the corporate security committee, they must measure the results of specific environments, report on new needs and situations that expose information.

The critical success factors have been explained above within the corporate information security management model, we can didactically synthesize the proposed structure through the expression: local action guided by global vision.

Regarding that, I imagine the reader will realize, from now on, how necessary it is to apply this model in your business, which makes it convenient to use a word of encouragement: "Security Master Plan: You can do it too!"

6.3 **BUSINESS CONTINUITY**

Early in the last decade, the Disaster Recovery Institute (DRI) presented statistics showing that out of every five companies that experienced a one-week interruption in operations, two went out of business in less than three years. Nothing leads us to imagine that this statistic has changed positively since then, with companies being able to interrupt their activities for longer without adverse consequences.

Thus, thinking about how to guarantee the continuity of activities in the face of some event that interrupts the operation of one or many business processes is one of the essential tasks of information security management, as defined in ISO 27002.

The focus is, more precisely, on ensuring the continuity of processes and information vital to the company's survival, in the shortest possible time, with the aim of minimizing the impacts of a disaster.

The theme is so complex that it has motivated in-depth studies, once again initiated in the British community, and once again published by the British Standards Institute. In 2006, published the BS 25999-1 standard, which defined a code of practice for business continuity management. The following year, the same institute released the second part of this standard, which defined the Business Continuity Management System (BCMS).

In 2012, in the same way as it did with ISO 27001, ISO released the ISO 22301 standard, which defines BCMS, enabling companies to certify their business continuity management systems.

The core of BCM

Defining a BCMS requires a series of steps, as in ISO27001, including planning how the organization will manage its continuity processes, the establishment of a continuity management policy, and, through the steps of business impact analysis, the definition of contingency strategies, and construction of the contingency plans themselves, which must be prepared with the clear objective of contingence security situations and incidents that cannot be avoided. They must be as effective as the reserve parachute in the event of failure of the main parachute, guaranteeing, despite the scare, the life of the falling parachutist.

We suggest working with three primary plans, minimally, as follows (Figure 6.13):

- Crisis management plan.
- Operational continuity plan.
- Disaster recovery plan.

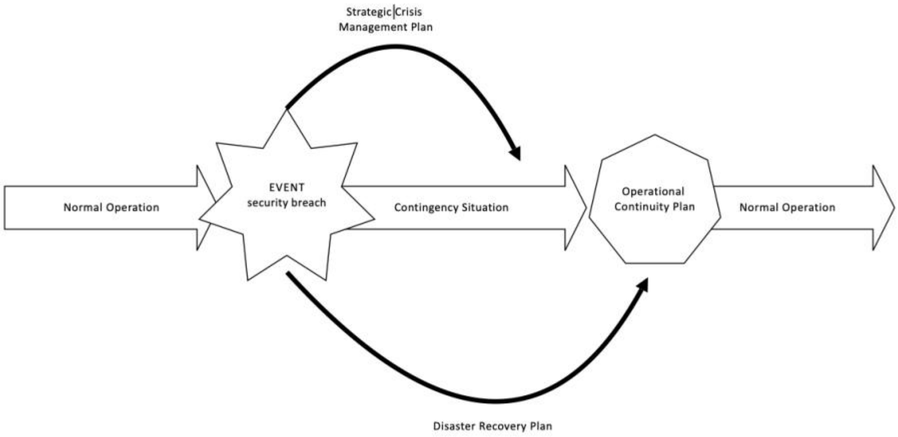


FIGURE 6.13

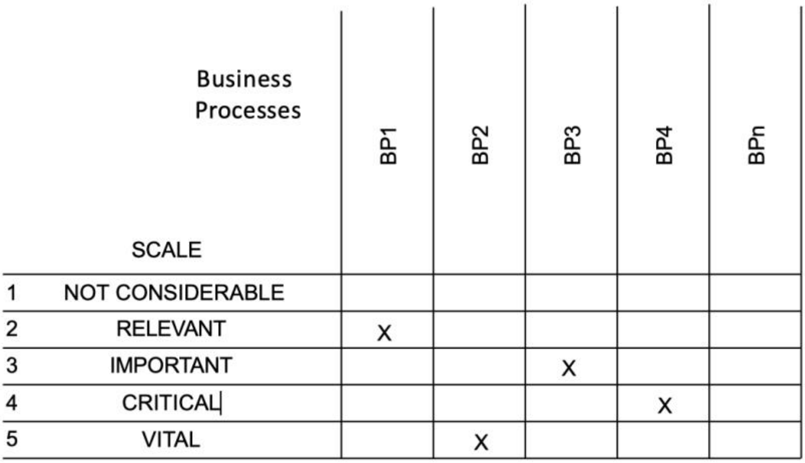
Illustration of the roles of the crisis management plan, operational continuity plan , and disaster recovery plan

A contingency plan may take several forms, depending on the object to be contingent and the scope of its action. Differently from what many people imagine, a company does not have a single plan, but several integrated plans focused on different perimeters, whether physical, technological or human and directed to multiple potential threats. This segmentation is important; after all, a company has processes whose tolerance for failure varies, impacts are variable too, as is the level of security required by the nature of the information handled.

Whatever the object of the contingency - an application, a business process, a physical environment, and even a team of the company must select the strategy that best leads the object to operate under a controlled level of risk. Despite a common conceptual base, there are many variants of methodology for the elaboration of a continuity plan; therefore, you may come across other nomenclatures or new groupings of strategy. In any case, the continuity solutions will be customized according to the context, by the characteristics of a market segment or specific fact, such as occurred in 1999 because of computers with difficulties in managing the date representation, nicknamed "the year 2000 bug" or "millennium bug".

Business Impact Analysis

Known worldwide by the acronym BIA (Business Impact Analysis), this first step is essential for providing information for the perfect dimensioning of the other phases of
construction of the continuity plan. Its objective is to determine the degree of relevance among the processes or activities that are part of the contingency scope as a function of business continuity. Next, the physical, technological and human assets that support each of them are mapped, so then determine the quantitative impacts that could be generated with their total or partial or total stoppage.



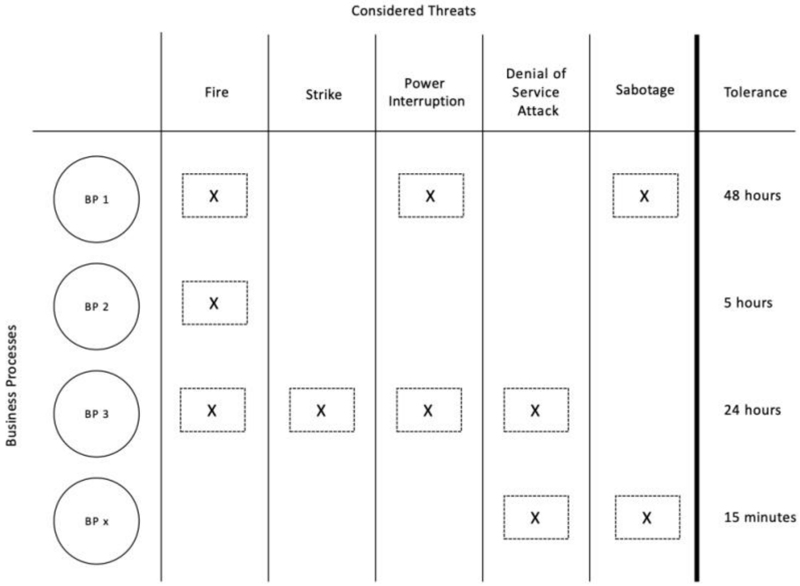
	Business Processes SCALE	BP1	BP2	BP3	BP4	BPn
1	NOT CONSIDERABLE					
2	RELEVANT	X				
3	IMPORTANT			X		
4	CRITICAL				X	
5	VITAL		X			

FIGURE 6.14

Illustration of the ranking of relevance among the processes belonging to the scope of the plan.

Holding the BIA analysis, it becomes possible to define the contingency priorities, the unavailability tolerance levels of each process or activity belonging to the contingency, and also group the assets according to their nature and dependency relationship with the processes. From then on, you have a snapshot of the processes' functionality, and the only thing left to do is to define the threats you want to contingency. The choice of threats to be considered for each process is directly linked to the probability and severity of an incident.

We will realize later that many of the tasks performed by the BIA could be complemented by the results of a risk analysis, which is therefore the first and most important activity to guide all information security actions.



Considered Threats

Business Processes	Fire	Strike	Power Interruption	Denial of Service Attack	Sabotage	Tolerance
BP 1	X		X		X	48 hours
BP 2	X					5 hours
BP 3	X	X	X	X		24 hours
BP x				X	X	15 minutes

FIGURE 6.15

Illustration of the selection of threats to be considered by the plan and the perceived tolerance of each business process.

If this inheritance were to occur effectively, the BIA would boil down to quantifying the impacts and selecting the threats to be considered by the business continuity plan (see Figure 6.15).

Contingency Strategies

Hot site

It gets its name because it is a "hot" strategy, or one that is ready to go into operation as soon as a hazardous situation occurs. Once again, the operationalization time of this strategy is directly linked to the object's fault tolerance time. If we applied it to a technological device, a database server, for example, we would be talking about milliseconds of tolerance to guarantee the availability of the service maintained by the equipment.

Warm-site

Following the nomenclature of the first strategy, this one applies to objects with a higher tolerance to downtime, being subject to unavailability for a longer period of time, until the activity is operational again. Let's take, as an example, the email service that depends on a communication connection. We see that the process of sending and receiving messages is more tolerant than the example used in the first strategy, since it could be unavailable for minutes without, however, compromising the service or generating significant impacts.

Operation Reallocation

As the name implies, this strategy aims to divert the activity affected by the event that caused the security breach to another physical environment, equipment or link, belonging to the same company. This strategy is only possible with the existence of "slack" resources that can be allocated in situations of crises. Very common, this strategy can be the example of redirecting data traffic from a router traffic from a router or server with problems to another that has processing slack and supports the accumulation of tasks.

Bureau of Services

This strategy considers the possibility of transferring the operationalization of the affected activity to an outsourced environment; therefore, outside the company's domains. By its very nature, which requires a longer tolerance time according to the activity's operational reactivation time, it is restricted to few situations. The fact of having its information handled by third parties and in an environment outside its control requires attention to the adoption of procedures, criteria and control that ensure security conditions that are adequate to the relevance and criticality of the constrained activity.

Reciprocity agreement

Very convenient for activities that would require contingency investments that are unfeasible or incompatible with their importance, this strategy proposes the approximation and a formal agreement with companies that have physical, technological or human characteristics similar to yours and that are equally willing to have an alternative of operational continuity. Together they establish contingency situations and define procedures for sharing resources to allocate the affected activity in the other company's environment. In this way, both companies obtain a significant reduction in investments. Despite the notorious benefit, all the companies involved need to adopt customized procedures and mechanisms that reduce the exposure of information that, temporarily, will be circulating in a third-party environment. This risk is aggravated when the reciprocity occurs between pseudo-competitors that unite exclusively with the purpose of reducing investments, needing to do so due to the specificity of their activities, for example, in the newspaper printing process.

Cold-site

Within the classification model adopted in the first two strategies, this one proposes a contingency alternative starting from an environment with minimal infrastructure and telecommunications resources, devoid of data processing resources. Therefore, it is applicable to situations with an even higher unavailability tolerance.

Self-sufficiency

Apparently a thoughtless strategy, self-sufficiency is often the best or the only possible strategy for a given activity. This occurs when no other strategy is applicable, when the possible impacts are not significant, or when they are unfeasible, financially, technically, or strategically. The choice of any of the strategies studied so far depends directly on the level of tolerance that the company can bear and the level of risk that its executive is willing to take. This decision presupposes the guidance obtained from a risk and impact analysis that generates subsidies to support the right choice.

Contingency plans

These are developed for each threat considered in each of the business processes belonging to the scope, defining in detail the procedures to be executed in a state of contingency. It is rightly subdivided into three distinct and complementary modules that deal specifically with each moment experienced by the company.

Crisis Management Plan

This document has the purpose of defining step by step the operation of the teams involved in triggering the contingency before, during and after the incident occurs. In addition, it has to define the procedures to be executed by the same team in the period of return to normality. The company's behavior in communicating the fact to the press is a typical example of the treatment given by the plan.

Business continuity plan

This document has the purpose to define the contingency procedures for the assets that support each business process, aiming at reducing the unavailability time and, consequently, the potential impacts to the business. Guiding actions in case of an internet connection failure exemplifies the challenges organized by the plan.

Disaster Recovery Plan

The purpose of this document is to define a plan for recovery and restoration of the functionalities of the affected assets that support business processes, in order to reestablish the environment and original operating conditions.

It is a critical success factor to properly establish triggers for each contingency plan. These triggers are tolerance parameters used to signal the beginning of the contingency operationalization, avoiding premature or late activation. Depending on the characteristics of the contingency object, the parameters can be: percentage of affected resource, quantity of affected resources, unavailability time, financial impacts, etc.

The notorious complexity of the business continuity plan - due to the diversity of objects, their customized characteristics, the scope of possible threats considered, and the necessary integration of crisis management plans, business continuity plans, and disaster recovery plans - makes it essential to build a dynamic model for document maintenance and testing.

It is an important piece of corporate information security management, mainly because it is the last resort after all others have failed, the three plans need to go through severe batteries of testing and approval, in order to ensure their efficiency and allow adjustments in the face of predictable physical, technological and human changes that occur frequently in the corporate environment.

Other plans may be mentioned in other literature or models, such as the incident response plan or the return plan, among others, but they can be evaluated as by-products of the three plans detailed here.

6.4 **INFORMATION SECURITY POLICY**

For the purpose of providing guidance and support for safety management actions, policy plays a fundamental role and, up to a point, has a similar importance to security management as a federal constitution for a country. In this way, it has a wide range and, because of this, is subdivided into three blocks: guidelines, norms, procedures and instructions, aiming, respectively, to the strategic, tactical and operational layers. operational layers.

It establishes standards, responsibilities and criteria for the handling, storage, transport and disposal of information within the security level that has been tailor-made by and for the company; therefore, the policy must be customized.

The guidelines, which in themselves have a strategic role, need to express the importance the company gives to information, as well as communicate to employees its values and its commitment to add security to its organizational culture.

The need for top management involvement is evident, reflected by the official character with which the policy is communicated and shared with employees. This instrument must express the executives' concerns and define the lines of action that will guide the tactical and operational activities.

Owner responsibility and cost for information, Security Office structure, security level metrics, indexes and indicators, legal compliance controls, user education and training requirements, physical and logical access control mechanisms, accountability, auditing the use of resources, incident records, and business continuity management are some of the dimensions to be addressed by the security policy.

With a tactical nature, the standards are the second level of the policy, detailing specific situations, environments and processes, and providing guidance for the proper use of information. Based on order of magnitude, we can estimate 10 to 20 guidelines in companies of any size, but we have to multiply this number by 100 or more to estimate the volume of applicable standards. This volume tends to be proportional to the size of the company, the heterogeneity of its physical, technological and human assets, and also the degree of detail required to the company to operate at the appropriate level of risk (see Figure 6.16).

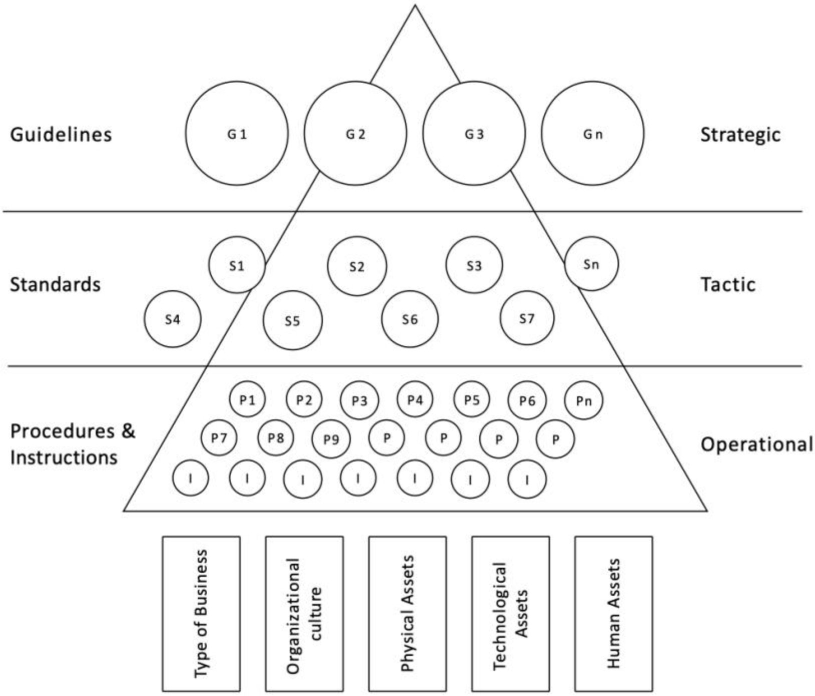
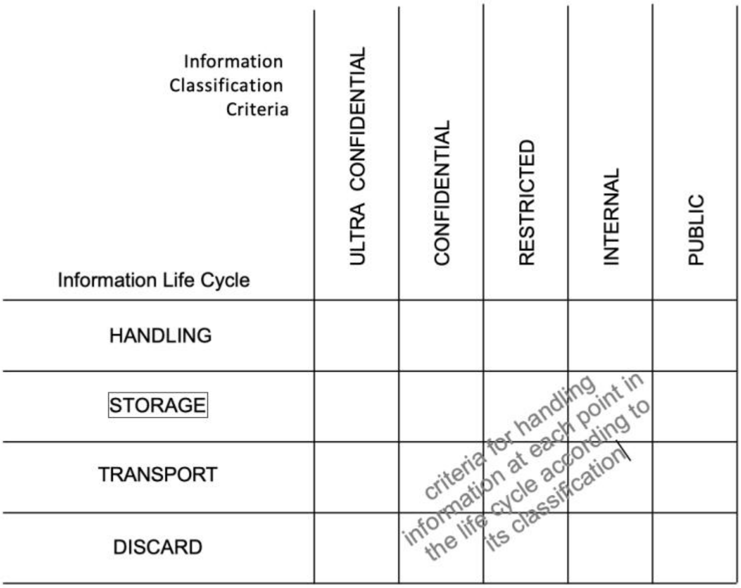


FIGURE 6.16

Concept diagram of the policy components and their pillars of personalization and support.

Standardized criteria for hiring and firing employees; creation and maintenance of passwords; disposal of information on magnetic media; systems development and maintenance; Internet use; remote access; laptop use; contracting outsourced services; and information classification are good examples of the rules of a typical security policy.

In particular, the information classification standard is a critical success factor, because it assumes the responsibility for describing the necessary criteria in order to signal the importance and value of the information, an important premise for the elaboration of practically all the other standards. There is no preconceived rule to establish this classification, but it is necessary to understand the profile of the business and the characteristics of the information that feed the processes and circulate in the corporate environment so that the criteria must be customized (see Figure 6.17).



Information Classification Criteria Information Life Cycle	ULTRA CONFIDENTIAL	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
HANDLING					
STORAGE					
TRANSPORT					
DISCARD					

criteria for handling information at each point in the life cycle according to its classification

FIGURE 6.17

Illustration of the relationship between classification and treatment defined in the policy for the information life cycle.

Procedures and instructions should be present in the policy in larger amounts due to their operational profile, where it is necessary to meticulously describe each action and activity associated with each distinct situation of information use. For example: while the directive strategically guides the need to safeguard information classified as confidential, and the standard defines that it must be encrypted at the time of sending the email, the procedure and specific instruction for this action must describe the steps necessary to perform the encryption and send the email. The detailed nature of this policy component means that it requires even more frequent maintenance.

From this, you can already see how complex it is to develop and, more importantly, keep the information security policy with all its components up to date. This perception becomes even more latent when considering the dynamism of the technological park of a company and, also, the predictable and unpredictable changes that the business may undergo.

Thus, the important thing is to kick-start and form a working group with executives from the most representative areas and departments, integrating visions, perceptions and multiple needs that will tend to converge and generate the policy instruments. Start by elaborating the guidelines, involve the executives and get their support. Establish the people responsible and the direct managers for the maintenance of the policy. Develop a program to disseminate the policy's guidelines, norms, procedures and instructions as a tool for disseminating culture and raising employee awareness. Make use of seminars, posters, gifts, official communications, conventional or online courses, screensavers and everything else that applies to the profile of the company and the nature of its activity. The important thing is to involve all employees, making them feel co-responsible for the health safety of the business and, mainly, responsible for the protection of the information they hold in custody.

Compliance with legal requirements, involving contractual obligations intellectual property rights, software copyrights, and all possible regulations and all possible regulations that affect the company's business company's business must be respected and, therefore, must be the line of conduct in the construction of the security policy.

6.5 **RISK AND VULNERABILITY ANALYSIS**

Conducting a security analysis is already a priority for the vast majority of companies, which demonstrates the perception of the need to diagnose risks. However, there is still a big "gap" in the understanding of what a real risk analysis is.

Returning to the pillars that support the business, we see vulnerability mapping initiatives focused purely on technological assets, i.e., instruments designed to analyze and identify failures of computers, networks, and systems. Of course, these are important activities, but not enough, in isolation, to accurately diagnose the real risks that involve the company's operation. Many other pillars coexist with the technological ones and, depending on the nature of the business, these may be even more relevant for support (see Figure 6.18).

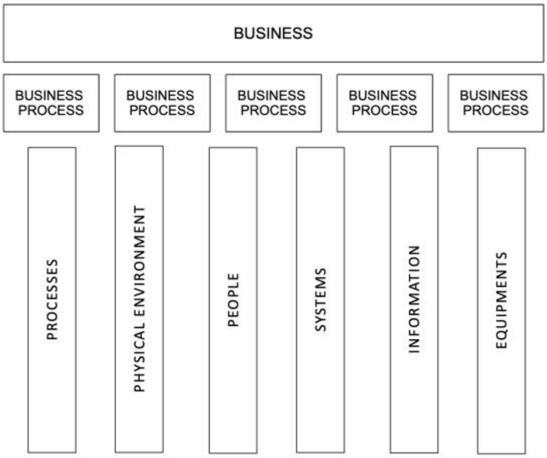


FIGURE 6.18

Dependency relationship between assets, business processes and the business itself.

There is a paradigm shift in understanding that the risks of a company are not only associated with the volume of technological failures, the qualification of the threats that could explore them, or the potential impacts. Diagnosing involves the analysis of endogenous variables that go beyond technological aspects; therefore, they must also consider the behavioral aspects of human resources, the physical, legal, and a wide range of exogenous variables that interfere directly or indirectly in the protection of the business. A strategic change - a new business unit - the presence of a new competitor or a representative factor of the economy can cause oscillations in the level of business risk, taking the company out of its comfort zone.

Therefore, risk analysis has to be seen as a fundamental instrument to diagnose the company's current security situation, through the synergy between the understanding of the business challenges, the mapping of the functionalities of the business processes and their relationship with the diversity of physical, technological, and human assets that host security gaps.

There are, fundamentally, two methodological lines to guide a risk analysis. The quantitative one is oriented to measure the financial impacts caused by a security breach situation based on the valuation of the assets themselves. The qualitative one is oriented by criteria that allow estimating the impacts to the business caused by the use of a vulnerability by a threat. Both have positive and negative points; however, with the great degree of subjectivity in the process of asset valuation and also the cascading impacts, direct and indirect, potentially caused by a security breach, the qualitative analysis methodology has demonstrated superior efficiency.

Applying the methodology for mapping business processes adopted in the security master plan, or inheriting the results of this activity, we have the relationship map and asset dependency. In this phase, the activities of evidence collection and identification of threats and vulnerabilities potentially present in the assets begin. It is important to understand that vulnerability by itself does not cause any damage to the asset. It is only a situation of fragility. The damage will only occur through the exploitation of the vulnerability by a threat.

Aspects considered in a risk analysis:

- Relation of relevance that a business process has to the business.
- Relation of dependence that one or more business processes have on the asset.
- Projection of the impact resulting from the realization of a threat's action.
- Probability of the threat exploiting a vulnerability.
- Potential severity of the exploitation on the asset.
- Qualification of the vulnerabilities present in the assets.
- Qualification of potential threats.

We see, from this list, the possibility of assembling a relationship map in which it is possible to project cause and effect situations. The multiple links, the scoring and qualification of the threats and vulnerabilities, associated with the probability and impact studies, become elements that subsidize the risk calculation.

As we are talking about an analysis that contemplates physical, technological and human assets, the identification phase of threats and vulnerabilities must be guided by interviews with managers and users, behavioral observation of human resources, physical inspection in person in the environments, document study and technical analysis of technological assets in order to collect evidence of the presence of failures.

These activities are supported by methodologies and support tools, commonly based on market standards, specific norms, such as TIA/EIA 568 and NBR 14565:2000 structured cabling, and by specialized systems on specific platforms and technologies. The justification for face-to-face actions, interviews, physical analysis, and even part of the technical analysis is given by the natural impossibility of collecting all the evidence through automated or computerized devices. If we take a network operating system as an example, we will see that in its universe of potential failures part of them could be identified by scanning systems or scanners, whereas another representative part would require human intervention, either to collect or measure the probability and potential impact. This perception leads us to conclude that a consistent risk analysis must rely on human resources with diversified skills, automated tools to support and manage the survey, and above all, a constantly updated security knowledge base.

We can say this Security Knowledge Base, or knowledge base of vulnerabilities, threats and new technologies, is the brain of a competent risk analysis. It is responsible for storing, managing and supporting actions, providing up-to-date information that will allow analysts to experiment with the most efficient techniques, locate the most recent failures and thus provide greater accuracy in measuring the company's level of risk.

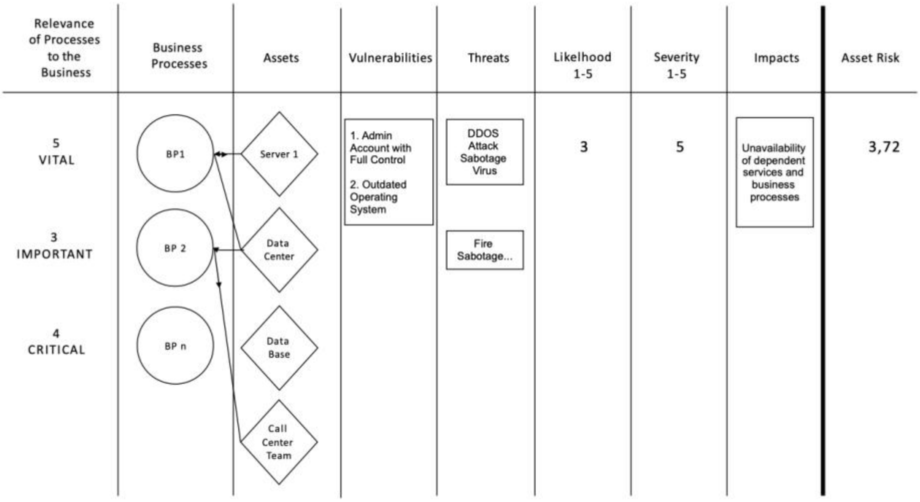


FIGURE 6.19

Illustration of the information collected for risk calculation purposes.

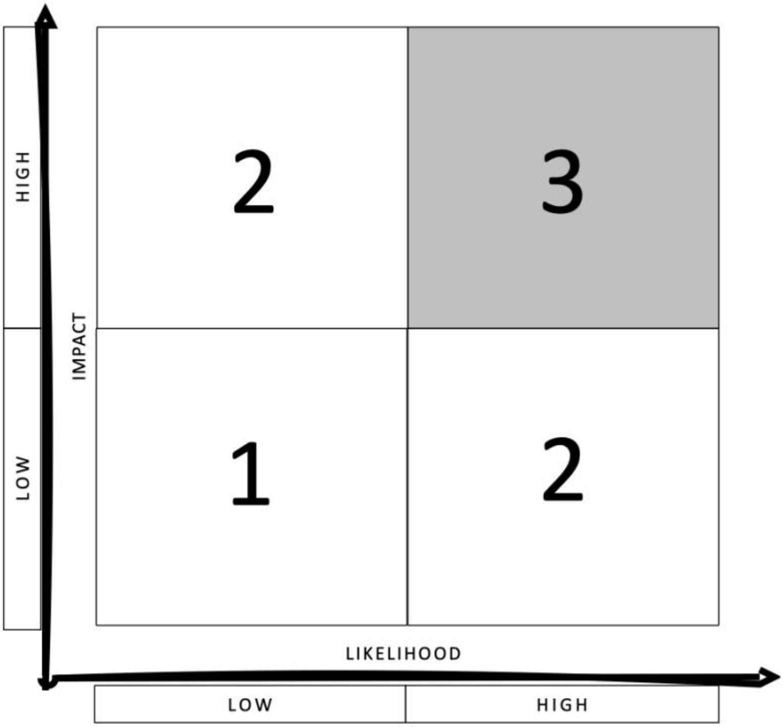


FIGURE 6.20

Quadrant of risk measured illustratively by the relation of probability and impact.

Once we calculate the probability and severity of a threat exploiting each of the vulnerabilities found on the assets, we obtain the final risk level for each asset. With these partial results, we can project the risk level of each business process, considering the risks of each asset that supports it. From this point on we can estimate the risk of the business as a whole by weighting the risks of each of the business processes that support it (see Figure 6.20).

The result obtained allows us to organize priorities and dimension an action plan for the short, medium, and long term, based on the distribution of the business processes and/or assets in the risk quadrants map. This way, we have the necessary guidance to support decisions and model specific countermeasures for each perimeter of the company, such as eliminating the risk, reducing the risk, transferring the risk, or accepting the risk. In any of these situations, budget limitations, technical difficulties, or external factors tend to prevent the full implementation of the specified countermeasures, leading any company to seek the level of controlled risk and in accordance with the nature of its business (conscious positioning).

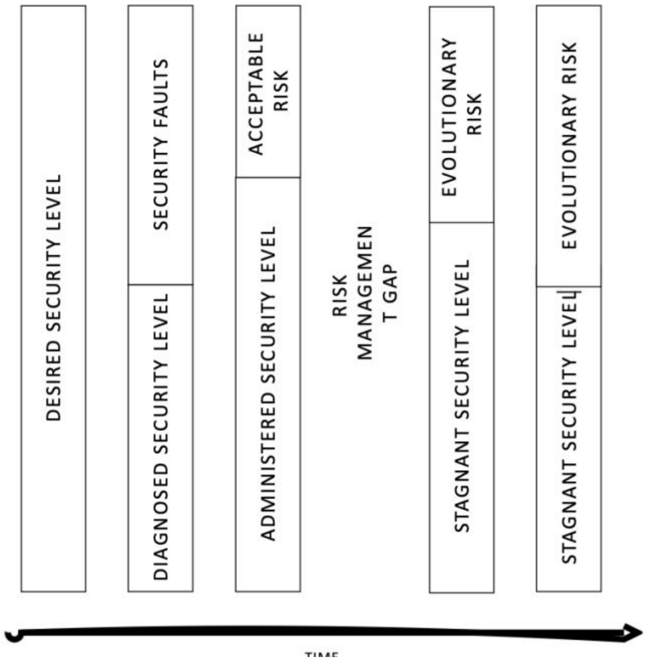


FIGURE 6.21

Overview of the applicability of risk analysis.

Security is about managing risks. Every company has its own characteristics, objectives, and specific plans; therefore, it needs to find the most appropriate level of risk to operate at. Within this panorama, risk analysis is the perfect instrument to measure the current security situation, making the company aware of the risks and guiding it to seek solutions that lead it to the acceptable risk level. However, due to the dynamism of the changes suffered by the corporate atmosphere, due to environmental, market, strategic, economic, technological, structural etc. factors, risk analysis must be part of a continuous management process, capable of diagnosing new vulnerabilities and threats, thus guaranteeing the maintenance of the controlled risk level.

The most current trend is to perform risk analysis based on measuring the presence and absence of security controls, and not only on the vulnerabilities present in the assets as the main axis. This movement is a consequence of the credibility acquired by the information security management standard ISO 27002 and also the ISO 31000 standard.

Its proposal is based on the interest and main need of security managers to protect the asset without, however, having to worry about eliminating or managing each one of the vulnerabilities individually. Thus, instead of having to map and seek individual solutions for each of the hundreds of vulnerabilities in an operating system, for example, the concern focuses on verifying the presence or absence of patch application, or correction program, made available by the producer. This way, there is a gain in performance, efficiency in obtaining results and, mainly, the company comes closer to the controls recommended by ISO.

While the risk analysis methodologies do not fully adhere to the security controls proposed by the international security standards, as an instrument of measurement and recommendation of actions, it is up to the Security Officer to move towards the tuning with standards and best practices. The results of the analysis and risks should be aligned with the controls suggested by ISO 27002 and identify the level of compliance achieved by the company by measuring adherence to each of the 114 security controls.

6.6 **PENETRATION TEST**

Despite the distorted interpretation of the market in general, considering it to be a marginal activity and necessarily performed by young technicians, the penetration test has an important and complementary role in the mapping of the company's risks. Its objective, unlike the risk analysis, is not to map all the threats, vulnerabilities and impacts, but to evaluate the degree of security offered by the security controls of a certain perimeter. To do so, it simulates improper access and invasion attempts from different points, and adopts different methods and techniques, however, with a well-defined objective. It is a premise to guarantee the quality of the activity to clearly define the perimeter that you want to test, the action of what type of threat you want to evaluate the protection, and also the validity time of the test.

The quality of an intrusion test is measured by the degree of similarity reproduced by the simulation in relation to real intrusion attempt practices, and not by whether positive or negative results are obtained. The more realistic the test is without however, effectively exposing information and compromising the company's operation, the better. What is expected as a result is a description of the test format, methods and techniques employed, evidence of the attempts and possible positive results.

There are, basically, four formats for the penetration test that arise from the multiple combination of two of the factors described below:

Internal

Defines the internal environment of the target company itself with the analyst's point of presence for test execution. This model has proven to be very efficient due to the high rates of attack attempts and intrusions carried out by employees and outsourced ones, which makes it very close to reality.

External

Defines an environment external to the target company itself with the analyst's point of presence for the test execution. This model has proven to be efficient in situations that aim to simulate external accesses to the corporate environment, such as in remote accesses, responsible for a representative slice of the attacks and invasions.

Blind

Defines the absence of access to privileged information about the physical, technological, and human structure in order to support the analyst in the execution of the test. This model has not shown great efficiency due to the low rates of attempted attacks and intrusions without any information about the target. Even if this is the initial status of an attacker, for real he/she tends to perform a previous information gathering, adopting social engineering techniques, garbage analysis, telephone tapping, electronic tapping, etc., in order to increase the chances of the attack.

Non-blind

Defines the presence of access to privileged information about the physical, technological, and human structure in order to subsidize the analyst in the execution of the test. This model demonstrates efficiency by its similarity with real attack situations. And it is further reinforced by the high incidence of internal attacks; therefore, it is executed by people who already have knowledge and often privileged access to information and environments.

As we can see, the invasion test proves to be a great resource to raise awareness among executives and potential sponsors of corporate actions, since it simulates the exposure of the company or of a specific perimeter to attack and invasion attempts that simulate reality. As this is a critical activity, potentializing the exposure of the company, its information and processes, it must be carried out by qualified professionals and guided by a methodology that ensures the control of actions, the follow-up by the Security

Officer and does not represent an additional moment of risk for the business.

6.7 **IMPLEMENTING SECURITY CONTROLS**

Implementing is acquiring, configuring, and applying the security control mechanisms in order to achieve the appropriate level of risk. Usually, this activity is part of a guideline obtained by risk analysis or by suggestions from specific security standards, such as ISO 27002, or even specific standards such as EIA/TIA 586 for structured cabling.

The universe of applicable controls is enormous, since we are talking about mechanisms for physical, technological, and human security. If we think of peopleware, that is, human capital as one of the most critical and relevant links for risk reduction, we will have, for example, the following controls:

- Awareness seminars.
- Training courses.
- Campaigns to divulge the security policy.
- Identification badges.
- Specific procedures for dismissal and admission of employees.
- Specific procedures for treatment of outsourced staff and equipments
- Term of responsibility.
- Confidentiality agreement.
- Access auditing systems.
- Content monitoring and filtering systems

Many of the human controls mentioned interfere directly or indirectly in the physical environment, but this must receive the implementation of another set of mechanisms aimed at controlling access and the conditions of physical environments, signaling, registering, and authorizing access and states, such as:

- Physical access control routers.
- Room acclimatize.

- Smoke detectors.
- Water triggers for firefighting.
- Fire extinguishers.
- Structured cabling.
- Safe rooms.
- Biometrics devices.
- Smartcards.
- Digital certificates in tokens.
- Internal television circuits.
- Alarms and sirens.
- Physical protection devices for equipment.
- UPS.
- Magnetic media storage devices.
- Paper shredders, etc.

As with physical and human controls, the list of devices applicable to technological assets is extensive; after all, in addition to the diversity and heterogeneity of technologies, we still have to consider the creative speed of the industry that presents us with a new tool or equipment practically every day. The instruments applicable to technological assets can be divided into three families.

Authentication and authorization

Aimed at supplying the identification processes of people, equipment, systems and agents in general, authentication mechanisms are fundamental to the current standards of computerization, automation and information sharing. Without identifying the origin of an access and its agent, it becomes practically impossible to perform authorizations consistent with the access rights, which may lead the company to share valuable information without control. Authentication methods are divided into three groups due to the degree of security they offer.

What you know

A widely adopted method based on the definition of a password, therefore a personal and non-transferable string given to the authorized agent to use it, and a proof copy is kept in the controlling instrument. Natively, this method already reveals weaknesses, because security depends on internal factors, such as the structure of construction and maintenance of the password, as well as external factors to the method, such as the behavior of agents who may have deviations of conduct, leading to the compromise of the mechanism. Sharing the password, selecting a weak password, not keeping it secret, or even handling it without the proper criteria can jeopardize the entire efficiency of the method.

Demystifying the popular classification of weak or strong passwords, take the academic and practical classification criteria as a basis. Academically speaking, a password can be classified as strong if it is longer than six characters, mixes numbers, uppercase and lowercase letters and special characters like brackets, asterisks, etc. In addition, it can be classified as weak if it is less than six characters long, if it is constructed only of numbers, upper or lower case letters, and especially when, despite its larger size, it represents some real-world information, i.e., first names, license plates, dates of birth, etc.

On the other hand, adopting the practical classification criterion, a password may be labeled as strong or weak depending on three factors: the value and importance of the information it protects, the length of time the password will be fulfilling its protective role, and the power, interest and willingness that an alleged interested party would spend to gain access to the protected information.

What you have

A growing adoption method based on the use of physical devices that are presented in access authentication processes. There is a large set of devices that fit this profile. The choice of the best mechanism is directly linked to the level of security required for the information and inevitably the available budget.

- Bar code card.
- Magnetic card.
- Smartcard.
- Token etc.

What you are

Still being popularized and cheapened, this method employs physical devices that perform biometric metrics to identify people who exercise the right to access information, environments, etc. They are usually costly equipment due to the state-of-the-art technology employed because they are based on reading information from the human body, which is unique to each individual. The level of security offered by the device depends directly on the metrics used and the number of comparison points available for each part of the body that is analyzed.

- Hand geometry.
- Face geometry.
- Digital identification.
- Voice recognition.
- Iris reading, etc.

With so many authentication options and the offer of different levels of security provided by each method, it is a critical success factor for the security manager to analyze in detail the target authentication perimeter, the real protection needs imposed by the criticality of the information, and the impacts related to performance and amount of investment required. Even so, situations may arise in which a single method does not meet the minimum security requirements, making it necessary to combine one or more methods. These hybrid solutions have been a constant in specific segments, such as the financial sector, in which the customer, besides having a magnetic card, has to enter a fixed password and personal information to prove his or her identity.

Fighting attacks and invasions

Aimed at supplying the technological infrastructure with software and hardware devices for protection, access control, and consequently to fight attacks and invasions, this family of mechanisms plays an important role in the security management model, as electronic connections and improper access attempts grow exponentially. In this category, there are devices for monitoring, filtering and logging logical access, as well as devices aimed at perimeter segmentation, identification and treatment of attack attempts.

Firewall

An old familiarity in network environments, this device, which can take the form of software and also incorporate specialized hardware, has the role of performing packet flow analysis, filtering, and logging within a network structure. As the name implies, it represents a wall of flame that executes pre-specified filtering commands based on sharing needs, access, and protection needs required by the network and the information available through it.

Looking for a didactic model, we can compare it to the traditional domestic water filter that, in principle, is formed by an empty compartment through which supposedly polluted water passes and by an element or candle, containing filtering layers made of various materials. When the water passes through this compartment, already with the filter element, the various layers of the element retain the impurities in the water. In this way, the filter can be considered efficient if it can retain all the impurities and allow all the other health-giving components, such as mineral salts, etc., to pass through. The firewall is similar to the filter in that it also requires the detailing of specific filtering layers for each company and situation, with the purpose of preventing undue access that occurs from inside or outside the network, recording these occurrences and, above all, allowing the normal traffic of legitimate data packets. Because it is based on binary analysis of parameters defined in the filter, the firewall always acts in the same way and without considering external variables that can modify situations; therefore, the efficiency of protection of this device is directly linked to the proper specification and maintenance of filtering rules.

It is important to remember that a category of firewall aimed at the end user, called the personal firewall, and has emerged with the purpose of extending security and complementing protection. Obviously these are software resources with low performance, but adequately proportional, in most situations, to the volume of data traffic on such a connection.

Intruder detector

Usually called IDS, an intrusion detector is a complementary device to the firewall that adds more intelligence to the process of combating attacks and intrusions. The basic role of the IDS is to passively identify suspicious data packets on a network by comparing them against a set of predetermined rules and patterns. Unlike a firewall, IDS can be driven by a dynamic database containing information about suspicious behavior of data packets and attack signatures. It is a real encyclopedia of threats that is consulted all the time so that the device can transcend the binary analysis of situations and evaluate the probability of an access being a known type of attack or a new invasion technique. We are not talking about artificial intelligence yet; after all, the tool does not learn from its own experiences and does not generate conclusions autonomously, but the device demonstrates its potential as a signaling device for situations that deviate from normality. It is important to emphasize that, because it has a degree of inference about possible risk situations, the intruder detector is responsible for many false positives, i.e., for signaling situations that appear strange, but are legitimate.

The evolution of the IDS is the IPS, which incorporated to its predecessor the ability to, in addition to warning about possible attacks or problems, take actions, also predetermined, in the face of an identified risk situation, and may, for example, block data packets coming from a particular logical address, preventing or ordering the firewall or edge router to prevent an attack on the network protected by them from continuing.

Depending on their nature, IDS and IPS are placed at different points in a network. The former is basically a watcher, eventually warning of possible problems. The second is an active participant, where network traffic must pass through in order to enable effective action of this mechanism. Due to these characteristics, several companies use these two mechanisms together in order to increase their security. In this case, it is interesting to evaluate the placement of the IPS at the edge, so that it acts more quickly and effectively, avoiding, for example, zero-day attacks, and the IDS after the firewall, which can alert on internal threats and ensure greater control over security events.

Besides IDS and IPS, there are other devices that, despite having been originally developed for other purposes, have incorporated, over time, features that assist and often reinforce activities to block and combat attacks. The router with filter, for example, incorporates part of the functionality of a firewall, and the switch, naturally intended to improve network performance and management, has great applicability in the logical segmentation of networks, reducing the efficiency of attack attempts that monitor the media, clipping it in order to capture relevant information. Similarly, the proxy, a software with the purpose of increasing the performance of Internet Web service access, through content management, as if it were a cache memory, has the potential to filter and record prohibited accesses that signal non-compliance with security policy standards.

Communications Privacy

It is inevitable to talk about cryptography when the subject is communications privacy. Cryptography is a science that studies the principles, means and methods to protect the confidentiality of information through the encryption or ciphering process, and that allows the restoration of the original information through the decryption process. Widely applied in data communication, this science uses mathematical algorithms and cryptanalysis to confer more or less protection according to its complexity and development structure. When we see message encryption systems or, for example, applications that adopt cryptography, we are facing situations in which the science has been employed and materialized as computer programs. There are two main techniques of cryptography.

Symmetric or private key cryptography

A cryptographic technique that uses a single password, or key, to encrypt information at its source and decipher it at its destination. Despite its excellent performance, among other things because of the existence of a single key that speeds the mathematical processes of calculation, this method has a native vulnerability in the process of sending or sharing the symmetric key with the recipient. Using a hypothetical example, if you want to send an encrypted message from user A to user B, the first step would be to create a symmetric key and send a copy of it to the recipient so that he can decrypt the message after receiving it. The risk occurs precisely at the moment of sending the copy of the key to the recipient because no protection process has been adopted. If, exactly at this fragile moment, despite the small window of time of the operation, the confidentiality of the key is broken, the entire encryption process will be compromised; after all, anyone who knows the symmetric key will be able to decrypt the message.

One of the most widely used symmetric key algorithms in the world today is AES (Advanced Encryption Standard), published in 2001 and to this day used as a standard by the US government, with a block size of 128 bits and a cryptographic key size of up to 256 bits. The size of the cryptographic key is directly linked to the security level of the algorithm, due to the exponential increase in the number of possibilities and attempts necessary to "crack", i.e. to find the right key that can decrypt the protection.

Asymmetric or public key

Cryptographic technique that uses a pair of keys for each of the interlocutors, more specifically a private key and a public key for the sender and recipient. Thus, with asymmetric cryptography created in 1976 by Diffi and Hellman, the parties no longer need to share a single, secret key. Based on the concept that to decipher cryptography it is necessary to have both mathematically related keys, public and private, the sender only needs the receiver's public key to ensure the confidentiality of the message and to enable the receiver to decipher the message.

As the name implies, the private key belongs exclusively to its owner and must be kept secret. The public key, on the other hand, can and should be shared and made available to anyone interested in sending an encrypted message. This technique still reserves complementary resources, such as the digital signature, obtained by using the private key to make a "binary mark" on the message, indicating that it was written and sent by its owner. The digital certificate is an electronic instrument that certifies the veracity of the user's public key, conferring authenticity to the digitally signed document.

We cannot forget, also, the HASH function, which provides the possibility of verifying the integrity of a message by comparing, at the destination, the result obtained by applying the function. When the results obtained by the function at the source do not coincide with the results obtained at the destination, there is an indication that the message has suffered some kind of alteration, even if it is very small.

Apparently, this technique is perfect, if it were not for the fact that it has low performance, consuming hundreds or thousands hundreds or thousands of times more time to process compared to the symmetric technique.

Due to the problems present in both techniques, a hybrid solution was found from the union of techniques that allowed to take advantage of the symmetric technique's performance and the security and satellite functions of digital signature and integrity validation provided by the asymmetric technique. With the public and private key pairs, the sender generates the symmetric key and inserts a copy in a new message, a method conventionally called enveloping, encrypting it with the recipient's public key. The recipient, in turn, upon receiving the confidential message, uses his private key to decrypt it, gaining access to the copy of the symmetric key. From this moment on, when both parties have the symmetric key safely sent and received, the encrypted communication process can be restarted by adopting the same symmetric key that will provide the necessary speed to enable the exchange of information. the exchange of information.

Virtual Private Network

This solution, commonly called by the acronym VPN, is the result of applying encryption between two distinct points over a public or third party owned network. The result of adopting cryptography is the creation of a secure tunnel that ensures the confidentiality of information without, however, absorbing the risks native to a network that transcends its control limits. Thus, the company has a virtual private network, i.e., the technology enables the use of a natively non-safe network as if part of it were private due to the security added by tunneling. To fulfill the role of extension of your corporate network, the VPN needs to ensure minimum performance in order to enable connections with branches and partners, thus enjoying the benefits of capillarity and redundancy that the Internet, for example, offers. Thus, they are implemented by specialized software and hardware capable of processing the encoding and decoding of data packets with extreme speed and competence.

There is also a category of Virtual Private Network aimed at the end user, called personal VPN, with the purpose of allowing secure remote connections. With the current technological advances, the performance of such solutions, implemented software solutions, which originally were far inferior to those implemented by hardware, has become fully satisfactory and adequate, in most situations, to the volume of data traffic over this type of connection.

Public Key Infrastructure

It is possible to notice the great applicability of the digital certificate in authentication and encryption processes, in the publication of information, access to physical environments, applications and equipment, sending electronic messages, virtual private networks or in the electronic exchange of information in general. Its versatility and growth potential bring up a possible problem: the management of the issuing, revocation, safekeeping, and distribution process; after all, for documents and processes to assume the credibility of the agent or user of the device, it must have been inherited from the device management process. Because of this need, PKI technology (public key infrastructure) brings together software resources and services to support the assembly of a certificate management process. Looking for an example that favors didactics, we can make an analogy with traditional notary offices. In order to purchase a good, many documents need to be authenticated by a structure that has public faith or, at the very least, the confidence of the parties involved in the transaction. This process requires the physical presence to identify the parties through documents, visual proof of the authenticity of the original documents, and then to extend the originality to the copies. Similarly, the process of digital certification implemented with PKI infrastructure requires the prior identification of the parties and only then to issue the digital instrument. Moreover, this same structure must be guided by a specific policy and be able to reissue, revoke, distribute and, most importantly, keep under high criteria of confidentiality, integrity and availability the secret of the process: the private key and its design criteria.

The perception of the technical importance of the subject and, especially, of the legal factors involving the accountability of individuals and companies for the electronic relation of information recognized as legitimate has already reached the public sector. The government's interest is to guide and subsidize a common base for the construction of public key infrastructures in order to, in a first moment, guarantee the mutual recognition of companies and the federal public administration within the country and, in a second moment, enable recognition by other integrated international structures, which will foster electronic commerce, government and company relations. The result of this movement materialized in August 2001, through Provisional Measure 2002-2, establishing a Brazilian Public Key Infrastructure, or ICP-Brasil.

Steganography

There are other privacy-oriented techniques for sending information. This one, in particular, has gained public knowledge through secret agent movies and the tragic terrorist attack of September 2001. The technique proposes the use of methods to camouflage sensitive information in seemingly harmless messages and files that could only be extracted by the recipient, who has the knowledge of the camouflage map. These methods can be applied to binary files, analog voice, electronic images, and even video, where seemingly ordinary gestures can cover hidden messages. This method shows a positive point, due to the fact that it does not signal to potential attackers that a given message carries information that is notoriously secret, unlike encryption, which, because it is encrypted, already denounces its condition and classification.

6.8 **SECURITY TRAINING AND AWARENESS**

Human resources are considered the weakest link in the chain, as they are responsible for one or more phases of the information security process. This situation is ratified by the fact that peopleware does not have a binary and predictable behavior in which one can eliminate all the vulnerabilities present. The human being is a complex machine, endowed with initiative and creativity, which suffers interference from external factors, causing behaviors never experienced before. The surprise factor is one of the neuralgic points of security processes that depend on people. If we specify rules for creating, handling, storing, transporting and disposing of passwords, implement technological resources for auditing and authenticating access to make an environment more secure, and we may have the efficiency of these initiatives called into question as a human resource disregards the security policy instructions and shares his or her supposedly personal and non-transferable password.

These risks need to be dealt with progressively, aiming to form a security culture that is integrated into employees' activities and becomes seen as a self-protection tool. The actions must have the strategy of sharing responsibility with each individual, making him/her a co-author of the security level achieved. Only in this way will companies have, in their employees, allies in the battle to reduce and manage risks.

There are many ways to start building a security culture. Some of them apply to publics with different profiles; others apply to all profiles, however, at different times.

Seminars

The work must begin with open seminars aimed at sharing the perception of risks associated with the company's activities, the potential impacts on the business, and, mainly, the compromising of critical processes if any threat were to materialize. This way, each employee starts to see himself/herself as a cog in the machine and co-responsible for its good functioning, being able to generate direct impacts to his/her process and indirect impacts to adjacent processes.

Disclosure campaign

It is important that the company has a safety policy that is updated and aligned to the needs and strategies of the business, but it is essential that it is recognized by the employees as the company's safety manual. Its guidelines must be known by all, and its norms, procedures and specific instructions should be presented to each group with a similar activity profile. In this way, each member realizes his/her responsibilities within a single security model, motivating them to collaborate. However, this is not enough. Remember that the effective results of commitment occur slowly and often require complementary actions.

For this reason, the campaign will need to use a variety of tools to communicate the standards, criteria and operational instructions, such as posters, games, promotional pieces, screensavers, informative emails, email alerts, internal communications, specialized pages on the Intranet, etc.

President's letter

As an instrument to formalize the company's interest in adapting the level of security of its information with the involvement of all hierarchical levels, it is advisable that the president or CEO officially expresses this will. The president's letter has this role and is made available, if not forwarded to each employee, giving a formal character to the movement. Sometimes this seemingly simple document is responsible for many spontaneous support and the natural strengthening of the strategic plan for information security.

Liability and Confidentiality Agreement

Considered to be another important instrument for awareness and culture building, the liability and confidentiality agreement aims to formalize the employee's commitment and understanding of their new responsibilities related to the protection of the information they handle. In addition, this term is in charge of disclosing the applicable punishments for misconduct and also to clarify that the company is the legitimate owner of the assets, including the information that flows through the business processes and is now temporarily held in custody by people.

Training and certification courses

Within the workforce, there are professional profiles that require greater mastery of security concepts, methods, and techniques, and their area of interest and depth may vary. Network administrators, for example, need to be prepared to react to attack and invasion attempts or to contingency risk situations. The Security Officer, on the other hand, must be able to define, measure, and evaluate security index and indicators to support his/her management plans and work planning, in order to ensure the total integration of actions and, most importantly, achieve the objectives. For all these cases, seminars, awareness campaigns or a letter from the president are not enough. They need formal training through specialized courses, which propose a certification as an instrument of competence recognition. Due to the heterogeneity of the profiles, demands for vertically technical courses arise, aimed at training resources in certain security technology, as well as demands for the orientation and preparation of Security Officers. However, it is relevant to highlight the need for continuous processes of sensitization and training of people, otherwise the team will be stagnant and soon unprepared for the administration of new risk situations.

6.9 **INCIDENT RESPONSE TEAM**

The speed with which a company responds to situations, such as the appearance of a new vulnerability, the unavailability of assets, attacks and intrusions, and sabotage attempts, determines how long the company will be exposed and subject to the associated impacts.

Because of the complexity of technology parks, the speed with which new security flaws and computer viruses appear, and especially because of the growing demand for integration, connectivity, and sharing, having and maintaining a security team makes the difference.

As mentioned before, this complexity can demand such a large volume of resources that it may no longer be interesting to maintain them. Investing disproportionately in security teams when your company's core business is far from this end is not one of the smartest things to do, with some exceptions when it is worth the investment due to the nature of the company's products and services.

In both cases, whether with resources in-house or outsourced, the company needs to build a model for hiring and deploying teams that are integrated and tuned in such a way as to offer efficiency and speed of response to incidents. Part of the positive results of this model is linked to the figure of the coordinator, more specifically the Security Officer, who, from the knowledge of the business and the corporate vision, will define the work guidelines of the teams.

In any case, we see the dependence on professionals specialized in multiple technologies and constantly updated, to keep them able to react before it becomes too late.

6.10 **MANAGING AND MONITORING SECURITY**

It is common to think that this activity may mean the end of the work, but in fact, it represents a new beginning. It is a feedback loop in the safety management process, with the binary purpose of measuring the results achieved by the predecessor activities and generating new indicators of change. Through the monitoring of security indexes and indicators defined by the Security Officer, it becomes possible to perceive deviations in conduct, infrastructure overload, attack and invasion attempts, inefficiency of the implemented controls and, above all, the presence of physical, technological or human changes that may cause the oscillation of the level of security.

Auditing is part of this universe and can be done with automated and manual instruments. These are devices capable of recording access, signaling the crossing of perimeters, blocking behaviors in physical and electronic environments, as well as methods that require physical presence in search of material evidence that denote inadequate environments, non-compliance with policy, and risky behavior by human resources. Complementarily, there are also devices classified as Policy Enforcement: physical and technological instruments that aim to force compliance with the rules defined by the company, imposing them to be followed. If there is any prohibition to access a certain Internet site, for example, and an employee ignores the restriction and tries to establish the connection, software can fulfill the role of controller, block the access and register the occurrence. By the way, the logging mechanism is a fundamental tool to ensure the success of security administration and monitoring. It is a great source of information to measure the degree of adherence of employees, the efficiency of the controls, and also to notice security flaws that remained even after the implemented controls.

It is imperative the Security Officer identifies the appropriate controls that will generate indexes for monitoring, according to the company's specific needs. It is quite true that many of them apply to all companies, but there is always the customization to meet, mainly, the monitoring expectations of the sponsoring executives. Many times, depending on the degree of maturity of the board of directors, this monitoring generates a Security Index that becomes part of the Balance Score Card set of corporate indexes.

It is worth remembering the tendency of risk analysis to be guided by security controls, such as those suggested by ISO 27002. These same controls, added to the criteria, standards and rules defined by the company's own security policy, are an excellent reference to support auditing actions, serving as a compliance parameter. Today, in fact, we already notice in many companies the synergy of the concepts employed in the establishment of the quality management system, the ISO 9001 and the information security management system, of the ISO 27001 standard.

6.11 **THE COMPLIANCE RISK**

The GRC model, as already described in Chapter 4, emerged in the first decade of this century as an acronym for the concepts of governance, risk, and compliance. This model brings the responsibilities of the Security Officer closer to the companies' top management, for the aspects of control and ensuring that the organization is not negatively affected by inadequate management, making it act in a way to ensure the direction of investments in security controls based on the real needs of the business.

As in any new management model, there is still a lot to evolve and mature in order to be fully effective, but there are already some assessments of the best ways to follow and what to avoid in this process. The main thing is perhaps to avoid a distortion of focus that causes the model to tip to one side and become unbalanced.

A strong trend is to use a compliance-driven approach to security, strongly advocated by auditing firms and auditors, in the belief that by identifying the regulatory, legal, and standards requirements with which you must ensure compliance and implementing the necessary controls in order to achieve, for example, certification, your organization would be sufficiently secure. Actually, this cannot be considered true. Compliance with a standard guarantees that, in the scope assessed, the requirements of this standard were achieved. Nevertheless, even if the scope is the entire company, which may make a certification or even an audit unfeasible, it will hardly be possible to guarantee that no more vulnerabilities exist that has not been adequately controlled and could be exploited in this scope.

According to the SANS Institute (www.sans.org), "Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed."

Perhaps the best strategy for the Security Officer is to combine several approaches and imagine that the best way forward is to work to ensure organizational survival. In fact, the focus of security from this perspective would be to detect and respond to any security breach quickly and effectively, always seeking to limit the negative impacts of an event to a minimum, so the operation continues despite degraded conditions. This philosophy is based on the premise that it is impossible to completely protect an organization from the threats it is exposed to. Therefore, in addition to constantly work toward the best possible implementation of the necessary security controls and GRC, the organization must plan itself for failure, so it happens as predictably and safely as possible, based on sound processes and adequate business continuity management.

Chapter 7

Knowledge

Checkpoint 3

Security Officer Orientation

Corporate solution on information security

CONCEPT: Security is the intelligent management of information in all environments, regardless of its form. Control and segmentation are the best words to represent this challenge.

Security master plan

CONCEPT: The methodology applied in the preparation of the security master plan already adopts diagnostic activities, but in a more strategic way and oriented to the needs of the business as a whole; therefore, there is no conflict with risk analysis. A well-structured PDS is fundamental for the coherence and integration of the subsequent activities in the PDCA cycle.

Business continuity

CONCEPT: To ensure the efficiency of business continuity management, you must build a dynamic process to maintain all documents, ensuring integration and effectiveness in disaster situations. Developing the necessary plans from a prior risk analysis and business impact analysis is the best way to increase effectiveness and return on investment.

Information security policy

CONCEPT: Form a multidisciplinary group, integrating different and enriching needs and views. Define a process for the creation, maintenance and dissemination of the policy. Involve the top management and start the work with the elaboration of guidelines and key standards. Start small, but think big. Its human assets directly link the security maturity of a company to the comprehensiveness of its security policy and the culture dissemination.

Risk and vulnerability analysis

CONCEPT: To extract the full potential from a risk analysis, it is necessary to consider in its scope the entire spectrum of assets present in the corporate environment that directly or indirectly support your business processes. In addition, it is a critical success factor to map the relationships between processes and assets. Only then will it be possible to generate a diagnosis that is effectively guiding and aligned with the company's interests.

Penetration test

CONCEPT: The penetration test does not propose to map all security flaws, but to experiment the exploration of any security control in search of a vulnerable point, in order to demonstrate the company's fragility. Its quality is directly linked to its efficiency in reproducing situations that are close to reality.

Implementing security controls

CONCEPT: The success of the implementation of security controls is directly linked to the preliminary stage of sizing the needs, projection of impacts, and especially the segmentation of physical, technological, and human perimeters that will allow the use of the right controls that offer the most appropriate level of security for each situation.

Security training and awareness

CONCEPT: The security level of a chain is equivalent to the resistance offered by the weakest link. Peopleware represents exactly that link; therefore it should be the target of a continuous and dynamic program, capable of keeping human resources motivated to contribute, aware of their responsibilities, and prepared to act upon old and new risk situations.

Incident response team

CONCEPT: The security of the business depends on how long the company keeps its assets vulnerable and at the mercy of threats that can exploit them. Due to the complexity of the environments and the speed with which changes arise, it is necessary to maintain a multi-specialized team capable of acting in an integrated manner and with speed to reduce the exposure time, minimizing the impacts.

Managing and monitoring security

CONCEPT: The security level of an organization tends to oscillate whenever an endogenous or exogenous change occurs; because of this, it is a condition for success to set up a security controls administration and monitoring model, formed by indexes and indicators that are important for the business, in order to feedback the management process coordinated by the Security Officer. These inputs will cause changes in direction, prioritization, and optimization of the return on investment.

The compliance risk

CONCEPT: Be careful not to believe that because your company is compliant, or even certified to a standard, it is safe. This is not true. Focus on detection and response, aiming at continuity of operation even in degraded conditions. Work diligently and constantly to implement adequate controls and plan ahead for failure. Put in place consistent processes that, in case of failure, do so as predictable and safe as possible.

Chapter 8

ISO 27002 compliance

What is an ISO standard for? Many of us have never asked this question, despite being in daily contact with certified products, with companies that have the recognition of certifying bodies and, in some cases, with business-to-business commercial relationships that only occur due to the mutual presence of conformity with a certain standard. In a didactic way, we can say that a norm has the purpose of defining rules, standards and control instruments that guarantee the standardization of a process, product or service.

But why do so many companies seek adherence to these standards? In a traditional and healthy economy, companies represent cogs in a complex system in which there is a constant exchange of goods and services, using currency, to materialize financial relations. Given this, it is healthy that all companies seek a common ground that facilitates interaction and trust among them and, in due course, seek elements that project them further, conquering competitive differentials. This is the law of the market. The standards emerged to suggest common ground, each with its own specificity, as we see in ISO 9001 (Quality) and ISO 14000 (Environment). These are examples of criteria, standards and control instruments, applicable partially or totally depending on the nature of each business, which ended up forming a culture and receiving worldwide recognition from specific segments.

The market has reached a level of automation, information sharing, and dependence to such an extent that it is the elaboration and compilation of a specific norm to guide the standardization of a common base aimed at information security management. This standard is NBR ISO/ IEC 27002:2013, published by ABNT (Brazilian Association of Technical Standards, or in Portuguese, Associação Brasileira de Normas Técnicas).

Originally derived from the first part of the British standard BS 7799, which gave rise to the international standard

ISO/IEC 17799:2000 after evaluation and minor adjustments were proposed, ISO 27002 defines a code of practice for information security management. Besides the four initial sections, which define general security aspects, the standard contains 14 sections (or domains) that present a total of 35 groupings that expand into 114 controls. Because it is a code of practice, this part of the standard is not subject to certification, but it does recommend a broad set of controls that subsidize those responsible for corporate information security management.

Domains:

- Information security policies
- Information security organization
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Security in operations
- Communications security
- Systems acquisition, development and maintenance
- Supply chain relationships
- Information security incident management
- Aspects of information security in business continuity management
- Compliance.

Complementary to ISO 27002, NBR ISO/IEC 27001:2013, derived from the second part of the British standard BS 7799, defines the ISMS (information security management system), which allows the certification of companies, in the same way as ISO 9001.

8.1 **FRAMEWORK AND THE SECURITY CONTROLS**

The security framework defined by ISO 27001 establishes an ISMS (information security management system) and includes the same 114 controls suggested and detailed by ISO 27002, serving as the object for obtaining certification.

Thus, companies can conduct security actions under the guidance of a common base proposed by ISO 27002, and indirectly prepare themselves for the recognition of compliance assessed by accredited bodies, based on ISO 27001. The security certification, similar to the reflexes obtained by the achievement of the ISO 9001 quality certification, promotes improvements in business-to-business and business-to-consumer relations, and adds value to the company by representing a competitive differential and a public demonstration of the commitment to the security of its clients' information. This differential, which at various times represented a position of prominence, innovation, and maturity of the certified company, has been fading year by year and is starting to become a requirement, with about twenty-eight thousand certified companies around the world (more than 830 in Brazil).[4]

The path that leads to the recognition of compliance, however, is long and requires efforts dedicated to planning, selecting applicable controls and coordinating the activities that will prepare the object of certification. As occurs in practice, the object of certification does not necessarily need to be the whole enterprise, but should start with a narrow scope, usually a representative process for the nature of the company's activity. Thus, the work begins and unfolds in seven main phases:

- Definition of security policy guidelines.
- Definition of the ISMS.
- Perform a risk analysis.
- Definition of a risk management framework.
- Selection of control objects and applicable controls.

[4] Data updated in February 2022.

- Preparation of the controls applicability statement.
- Implementation of the controls.

The standard represents a path that guides companies willing to structure themselves to manage information security risks; therefore, it merely indicates what should be done without, however, saying how it should be done. Due to the involvement of multiple specialties and managerial and technical competencies, it is recommended that companies that undergo preparation for certification count on external support in order to add experience, know-how accumulated by the execution of other projects and, mainly, by the vision free of vices that add quality to the work.

A relevant factor for those responsible was the direction ISO 27001 took, seeking to be in tune with the standards adopted by the ISO 9001 quality standard. This element added facility by allowing the use of the experiences lived through the preparation process, which requires the registration of controls and the construction of the quality manual, enabling the convergence of the two certifications. Faced with so many direct and indirect benefits provided by this new security certification, and the opportunity to be part of a still select group of Brazilian companies (more than 830), identify your level of compliance by taking the test suggested below and take courage to begin work. Good luck!

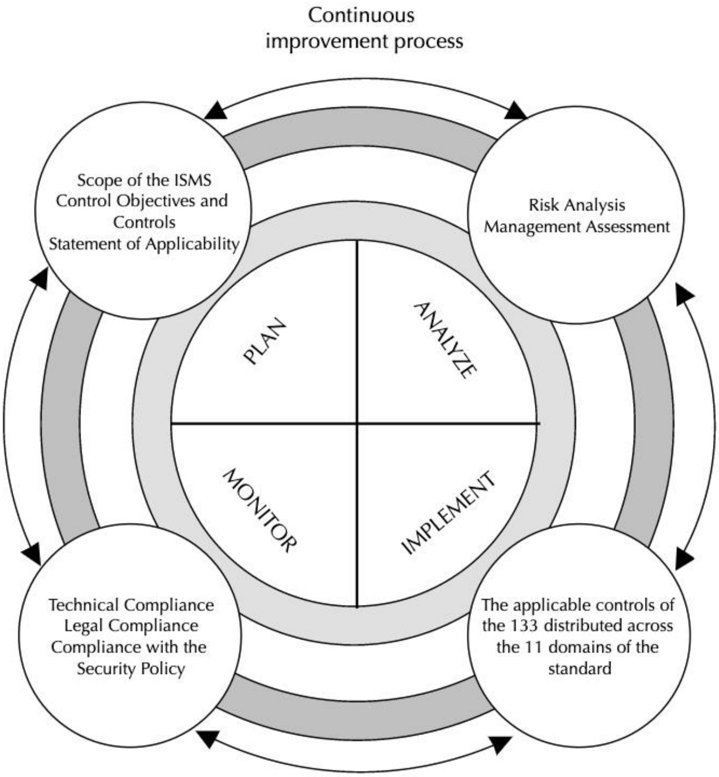


FIGURE 8.1

Sample ISMS framework.

8.2 **COMPLIANCE TESTING**

This tool will help you see how well your company is adhering to the information security recommendations of ISO 27002. Due to the natural superficiality of this type of test, it is commonly referred to as ISO 27002 Gap Analysis Light, that is, a simple and quick diagnosis, based on objective questions with an associated score that will reveal your adherence index.

Objective of the testing

To allow perception of the organization's degree of adherence to the controls suggested by ISO 27002.

Instructions

Choose only one answer for each question and calculate the final score.

Your company has:
1. INFORMATION SECURITY POLICIES
Is there na information security policy?

- Yes
- Yes, but outdated
- No

2. ORGANIZATION OF INFORMATION SECURITY
Is there one person responsible for managing the security policy?

- Yes
- Yes, but is not performing this function
- No

Is there a clear definition of the responsibility attributions associated with information security?

- Yes,
- Yes, but outdated
- No

Is there a segregation of duties and responsibilities policy?

- Yes
- Yes, but outdated
- No

Are there cooperation agreements with authorities and special groups?

- Yes
- Yes, but outdated

- No

Are there security practices in project management?

- Yes
- Yes, but outdated
- No

Is policy defined for mobile device usage and remote working?

- Yes
- Yes, but outdated
- No

3. HUMAN RESOURCES SECURITY

Are there criteria for personnel recruitment and hiring?

- Yes
- Yes, but outdated
- No

Are there processes for user training and qualification?

- Yes
- Yes, but outdated
- No

Are there disciplinary processes established?

- Yes,
- Yes, but outdated
- No

Are there defined procedures for termination and dismissals?

- Yes,
- Yes, but outdated
- No

4. ASSET MANAGEMENT

Is there an inventory of physical, technological and human assets?

- Yes
- Yes, but outdated
- No

Is there an information classification criterion?

- Yes
- Yes, but outdated
- No

Are there mechanisms for media security and handling?

- Yes
- Yes, but outdated
- No

Are there media disposal procedures?

- Yes
- Yes, but outdated
- No

5. ACCESS CONTROL

Are there business requirements for access control?

- Yes
- Yes, but outdated
- No

Is there user access management?

- Yes
- Yes, but outdated
- No

Are there definition of user responsibilities?

- Yes
- Yes, but outdated
- No

Is there network access control?

- Yes,
- Yes, but outdated
- No

Is there an operating system access control?

- Yes,
- Yes, but outdated

- No

Is there an access control to the applications?

- Yes,
- Yes, but outdated
- No

6. CRYPTOGRAPHY

Is there a policy for using cryptographic controls?

- Yes
- Yes, but outdated
- No

Are there policies for managing the life cycle of cryptographic keys?

- Yes
- Yes, but outdated
- No

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Are there definition of perimeters and physical access controls to the environments?

- Yes
- Yes, but outdated
- No

Are there resources for equipment's security and maintenance?

- Yes,
- Yes, but outdated
- No

Is there structure for adequate electricity supply?

- Yes
- Yes, but outdated
- No

Is there cabling security?

- Yes,
- Yes, but outdated
- No

Are there procedures for reuse and disposal of equipment?

- Yes,
- Yes, but outdated
- No

Is there a clean desk and clear screen policy?

- Yes
- Yes, but outdated
- No

8. SAFETY IN OPERATIONS

Are there operational procedures and responsibilities defined and documented?

- Yes
- Yes, but outdated
- No

Is there a change management process?

- Yes
- Yes, but outdated
- No

Is there a capacity management process?

- Yes
- Yes, but outdated
- No

Are there processes for segregation between development, testing and production environments?

- Yes
- Yes, but outdated
- No

Is there protection against malicious code and moving code?

- Yes
- Yes, but outdated
- No

Are there procedures for backups?

- Yes

- Yes, but outdated
- No

Are there procedures for monitoring and registering logs?

- Yes
- Yes, but outdated
- No

Are there procedures for installing and updating software?

- Yes,
- Yes, but outdated
- No

Are there procedures for auditing information systems?

- Yes,
- Yes, but outdated
- No

9. COMMUNICATIONS SECURITY

Are there network management and controls?

- Yes
- Yes, but outdated
- No

Are there procedures for network segregation?

- Yes
- Yes, but outdated
- No

Are there policies for information transfer?

- Yes
- Yes, but outdated
- No

Are there procedures to protect information in electronic messages?

- Yes
- Yes, but outdated
- No

Are there standardized confidentiality and non-disclosure agreements?

- Yes
- Yes, but outdated
- No

10. ACQUISITION, DEVELOPMENT AND MAINTENANCE OF SYSTEMS

Are there system security requirements?

- Yes
- Yes, but outdated
- No

Are there processes for securing applications on public networks?

- Yes
- Yes, but outdated
- No

Are there policy and procedures for secure system development?

- Yes
- Yes, but outdated
- No

Are there procedures to control changes to systems?

- Yes
- Yes, but outdated
- No

Are there documented tests of system acceptance and security?

- Yes
- Yes, but outdated
- No

Is there data protection procedure for testing?

- Yes
- Yes, but outdated
- No

11. SUPPLY CHAIN RELATIONSHIP

Are there security requirements for supplier relationships?

- Yes
- Yes, but outdated
- No

Are there security requirements for the supply chain for products and services?

- Yes
- Yes, but outdated
- No

Are there service delivery management procedures?

- Yes
- Yes, but outdated
- No

12. INFORMATION SECURITY INCIDENT MANAGEMENT

Are there mechanisms of notification of weaknesses and information security events?

- Yes
- Yes, but outdated
- No

Are there procedures for managing information security incidents and improvements?

- Yes
- Yes, but outdated
- No

13. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Are there procedures and requirements for information security continuity management?

- Yes
- Yes, but outdated
- No

Are there redundancies to guarantee the availability of information processing resources?

- Yes
- Yes, but insufficient
- No

14. COMPLIANCE

Are there documented legal and contractual compliance requirements?

- Yes
- Yes, but outdated
- No

Are there controls for the protection of privacy and individual rights defined and implemented?

- Yes
- Yes, but outdated
- No

Are there procedures to critically review the approach and implementation of security in the company?

- Yes
- Yes, but outdated
- No

Score Table

Add up the points corresponding to the answers according to the following table:

Answer A:	add 2 points
Answer B:	add 1 point
Answer C:	do not add or subtract any points

ISO 27002 compliance rates

After completing the 59 questions on the test, you will have noticed the breadth of issues addressed by the standard and, of course, the complexity of planning, implementing, and managing all security controls to protect the confidentiality, integrity, and availability of information. The first objective of this exercise is to make you aware of all the aspects involved, guiding you to dimension the magnitude of the challenges.

It would be naive to promise with this test the same result as a risk analysis; however, through the indexes obtained with the final score, it will be possible to see how far your company is from what has been considered a national and international reference in information security management.

It is very likely that your company does well in one or more domains. This situation is present in most organizations and commonly happens due to the absence of a comprehensive diagnosis able to integrate the survey of threats, impacts, physical, technological and human vulnerabilities, associating them to the real needs of the business. Without a risk analysis, the actions become disoriented, poorly prioritized, redundant, many times, and, thus, wrong by not offering the expected return measured by the level of security of the company.

See now how far your company is from compliance with the norm.

Score between 78-118

Congratulations! Your company should be outstanding in its market segment because of the comprehensiveness of the security controls it applies to the business. Although we cannot see the uniformity of actions, spread across the 11 domains, we can say that your company is aware of the importance of security to the health of your business. The situation is even better if all actions and controls applied have been decided based on an integrated risk analysis and under the management of a Security Officer.

Score between 39-77

Caution! This result could have been achieved in many ways. Your company may have adopted almost all the controls, but most of them may be outdated, obsolete, or inactive, which shows a good level of awareness, but also a deficiency in the management structure, or a lack of financial strength to subsidize the administration resources. It could also have a representative portion of the controls in order, leaving the others inoperative or even non-existent. Therefore, it is convenient for us to warn of the great possibility of evolution, as well as the possibility of stagnation and biased reduction of the security level due to lack of guidance. Once again, the absence of a risk analysis can be the cause for the disorientation of investments and the difficulty in prioritizing activities.

Score between 0-38

Beware! The situation is not comfortable for the company. Information security is not being treated as a priority, and the score indicates absence or ineffectiveness of many of the controls recommended by the norm. The causes may be a lack of knowledge about the risks and a lack of awareness among executives and top management. I dare say that your market segment is not very competitive or that security is not seen by your customers as a critical success factor because of the nature of your business. Another hypothesis is that there may be isolated actions - from one department or another - that, although commendable, do not uniformly distribute security and end up minimizing the increase in the security level of the company. Nevertheless, this is no time to be discouraged. There is always time to reverse the situation. Start with a risk analysis and good luck.

NOTE: It is important to consider, when obtaining the results that they reflect a market moment, an evolutionary stage of information security; therefore, these diagnoses perpetuated in the book tend to oscillate over time, and may lose their effectiveness.

Chapter 9

The New Boundaries

Virtualization is definitely back. In fact, it probably never stopped existing, since it was first implemented. Keeping in mind the overriding and healthy goal of sharing and better utilization of hardware resources by various instances of diverse operating systems, mainframes have been using virtualization for decades. And this has always been a possible solution, used to a greater or lesser extent on multiple other platforms. What has changed is its large-scale application on SPARC, ×86, and ×64 platforms.

Security in virtualized environments, in the face of this growth in the use of technology, has become a strong concern for security managers, not because the security of these implementations is a technological mystery, but rather it is generally an unknown vector for most teams responsible for implementing security in organizations. In other words, virtual systems carry with them the same vulnerabilities and consequent control needs as "real" systems. According to one of the largest creators of virtualization systems, "data does not leak through virtual machines, and applications can only communicate over configured network connections." This somewhat simplistic statement is not unreasonable considering that hardware concerns also exist on non-virtualized platforms, but it fails to take into account a new element in the virtualization model: the hypervisor, the system on which virtualization is performed and which is responsible for managing the resources that are used by the different virtual machines. According to the Cloud Security Alliance (CSA), "virtualization brings with it all the security concerns of the guest operating system and adds to them the security concerns with new threats specific to the new model".

To illustrate the scope, besides the hypervisor, another abstraction layer that carries its own security risks for virtualization environments is the data network. Virtualized environments use software-based rather than hardware-based network connections, since the hardware is unique and is managed by the hypervisor, which in many slightly older implementations created a single hub through which all the VMs communicated. This meant that the various virtualized systems in the same fabric had open access to all the data passing through that domain. If two VMs shared the same virtual network interface, both machines could see all traffic between the host and the VMs. This is still true today in bridge mode network sharing configurations used in some virtualization systems. Even the most modern configurations, which implement multiple virtual interfaces, are equivalent to connecting multiple servers to a switch without segmentation into vlans.

Then, an attack on the network stack, for example, that would originally be restricted to a single system or similarly configured systems in a network, can do great damage to multiple virtual servers, on different platforms, but virtualized on a single host.

We could expand these lines to other areas, such as drive sharing, where the hypervisor has a superuser credential that has access to the guest system's kernel, and to weaknesses associated with sharing management consoles, among others, but we believe that the matter to raise, which is that the security and technology areas need to prepare for virtualization, has already been reached.

Security in virtualized environments depends on specialized tools, specialized personnel, specialized processes and, above all, on thinking about where the security of virtualized environments should take us in order to ensure that this new boundary, which is already a reality in most companies, is made viable in a safe way for the business.

9.1 **CLOUD COMPUTING**

One of the biggest trends and issues being discussed by the technology and information security fields in recent years is cloud computing. In fact, what is meant by cloud computing is the possibility of taking what you currently have "in house", in your data center, on your own servers, to "somewhere" on the Internet, whose infrastructure and administration (or at least part of it) are no longer your responsibility. While the menu of cloud services, with interesting and marketable names such as Software as a Service, Platform as a Service, or Infrastructure as a Service, offers flexibility, scalability, and economies of scale, in the Security Officer's mind there are several security concerns that need to be addressed. As more data is transferred to the cloud, the potential for compromise of personal and private data grows proportionally.

To begin with, we need to be aware that in order to meet the elasticity premise defined by NIST (National Institute of Standards and Technology) for cloud computing, a key component to its viability is virtualization, whose security concerns we illustrated in the previous section. All aspects previously addressed are present and will need to be addressed to a greater or lesser extent, depending on the contracted service model, and the security concern should also involve the legal-contractual issue, which should ensure aspects such as SLAs (Service Level Agreements) and accountability for failures or problems, and should be assessed in terms of the security of the cloud. for failures or problems, and aspects such as hiring, training and improvement of employees of the companies providing the services.

Although virtualization offers risks, it is inevitable. The gain in scale it provides cannot be ignored. Similarly, it is possible to imagine that a CSP (Cloud Service Provider) has the scalability to have trained and qualified professionals in larger numbers than small and medium enterprises, which counts as a positive point for the adoption of cloud computing, compared to in-house virtualization. In any case, the possibility of the CSP having better professionals should be subject to an assessment by the contractor of the services.

By the same logic, knowing that many CSPs meet standards of compliance with good practices in information security (ISO 27001), health (HIPAA) or finance (PCI), for example, seeking with these certifications to offer customers a greater sense of security and trust, a company could be safer if it hired services from these suppliers. On the other hand, as we have seen, a certification denotes concern with the establishment of adequate practices and controls, but this certification alone does not guarantee a risk-free operation. In any case, the on-site evaluation of cloud computing service providers is, in most cases, unfeasible, making the confidence provided by certification bodies and auditors a differential in hiring cloud services.

Resource availability is also another point to be addressed in SLAs. Virtualization brings with it the possibility of logical multi-tenancy - through a pool of environments in which applications and data from more than one organization are hosted on the same infrastructure, for example within the same server. This type of infrastructure sharing can generate an over-provisioning of resources, with the allocation of more systems or applications than the infrastructure can support in case of full use, which can cause contention and even denial of services (DoS), especially in applications that are sensitive to latency or make high use of disk I/O - read and write operation on disk - or processing (CPU). Ideally, the CSP should guarantee the mapping of logical resources to physical resources, limiting the possibility of resource over-provisioning.

Other points to ensure when evaluating a cloud computing environment are network isolation - crucial also in virtualized environments - security monitoring, availability of logs and intrusion detection - preferably with the use of VMI (virtual machine introspection) technologies, the existence of an incident response procedure and the possibility of encrypting data stored and in transmission, in addition to the physical security controls we usually maintain for our data centers, involving high availability requirements, backup and continuity of operations.

Many will advocate that once your data leaks on the Internet, even the best SLA will not guarantee that your operation, and especially your credibility, will not be severely affected. Among their arguments they claim that no compensation is worth the loss of confidentiality, integrity or availability of valuable information. But here again we have to realize that, regardless of any considerations, companies and governments will continue to move to the cloud in an effort to reduce costs, improve efficiency, and reduce administrative overhead. There is no stopping this trend.

To minimize the risks somewhat, some companies are adopting mixed structures, choosing to host in the cloud only what is internally classified as public or of low criticality or relevance to the organization, and keeping the rest in the internal infrastructure. This strategy seems interesting in terms of security, but has the possibility of negatively impacting the business, given the characteristic of today's organizations, increasingly geographically scattered and in need of flexibility and convenience, and the high costs of maintaining their own or individual structures compared to the costs in the cloud - part of the eternal accounting discussion between opting for CAPEX (Capital Expenditure) or OPEX (Operational Expenditure).

9.2 **MOBILITY AND BYOD**

Wireless networks have been around us for about a decade. But if a few years ago no one cared if they didn't have access to the Internet, today the reality is very different: we have become used to being connected all the time, anywhere, at any time. Smartphone sales have already surpassed those of desktops since 2011. The boundaries between personal and professional life have become blurred. More and more employees want and are using their personal devices at work, creating a wave of mobile devices that access corporate networks and store organizations' information, called BYOD, an acronym for Bring Your Own Device. According to a 2012 survey by the SANS Institute, more than 60% of companies already accept BYOD practices by their employees, despite the fact that many have no formal rules on the subject and that many of these devices were created with the end consumer in mind and not for business use, with its specific security needs.

As businesses implement corporate use of mobile devices and applications, they need to identify the risks they are exposed to, which can range from loss of confidential data to malware infections, breaches of private and corporate data to legal and regulatory compliance issues, and they must ensure that adequate controls are in place to properly manage them.

Intrusions and exploits on mobile devices are occurring through many means, including users browsing malicious websites, clicking on malicious links in SMS and email messages, installing malicious apps, or using unsafe Wi-Fi connections. To make matters worse, there is a plethora of operating systems, in multiple versions and with customizations per producer and per device, which makes the picture even more chaotic. In this scenario, the role of the Security Officer is essential, to support the organization in this moment of transformation and paradigm shattering, developing strategies that ensure the security of this transition.

The most widely accepted solution today to mitigate the risks of what is being called the "consumerization" of IT - the growing trend for new technologies to emerge in the consumer market and then spread to organizations and government, rather than the other way around as seen in past decades - in organizations is the use of network access control (NAC) systems. Basically, the use of NAC systems makes it possible to securely provide access to a wired or wireless network to devices that fall outside the scope of what that network considers "normal", through guest networking, making it possible to identify and enforce a security policy for all types of network users and devices.

The ability of the NAC system to classify network users and their devices gives organizations greater choices about how to treat new devices as they appear in the marketplace, allowing for, rather than case-by-case decisions, the establishment of a network access control policy that defines what types of devices can be used and what security policies should be implemented on each device if an employee or guest wants to connect a personal device to the company network to use work-related applications or resources.

The complexity to define these policies and the operation of a NAC system, however, considering the universe we are dealing with, tends to be quite high and of slow and gradual implementation. Initially, an evaluation of the use cases of personal devices on the network should be done, seeking an understanding of the need and risks. Next, it must be defined who and which devices should be accepted, as well as the authorized applications and the expected security level for these devices. Finally, the process should include exception handling, the registration and authorization process for new access, and problem handling, for instance, the remediation of nonconformities. Generally speaking, it is suggested to start simple, by directing unknown devices to a guest network that allows access to the Internet, but not to the internal network itself.

Another interesting possibility for security is to combine the use of NAC and MDM (mobile device management) systems, especially geared towards the security of smartphones and tablets, and usually consisting of a management server and an application on the mobile device to enable, for example, user and device authentication, secure remote access, management of applications installed on the devices, and protection against data leakage.

As with the previous topics, trying to stop this trend from taking root in your organization seems like a losing war to us: employees are bringing their devices into the enterprise, and will increasingly do so. According to research by the Gartner Group about 50% of the world's companies, instead of enabling employees to bring their devices to work, will require them to do so. The best thing to do, then, is prepare for this reality as best you can and start working on implementing the necessary controls as soon as possible.

It is always important to keep in mind also the legal and regulatory compliance issues, which vary from country to country, and which may impact even the possibility of implementing of certain controls, for example, those involving monitoring and remediation on personal devices, which are perfectly accepted in the United States and in Brazil, and can generate impacts for the organizations with regard to what is established in the national labor legislation.

9.3 **SOCIAL MEDIA**

Social media has become a major influencer of consumer purchasing decisions, setting itself on the path to becoming a strategic endeavor for any organization. The problem is that social networking sites also present huge opportunities for abuse and misinformation, as well as malware distribution and fraud execution. So as organizations increase their use of social media to capture business benefits, they must also put strategies in place to manage the risks that come with this new practice. Expectations must be set regarding permissible activity on social sites, and corporate policies regarding this topic must be widely publicized and known, seeking to balance corporate interests with freedom of expression. Tools and techniques will also be needed to mitigate the risks of incidents and protect the company against social media-based attacks.

We can list five major lines of concern:

- What is (and what cannot be) published on the official profiles of companies and official company representatives on social media.
- What is (and what should not be) published on private profiles of employees on social media.
- What is said about companies on social media.
- What is (and what should not be) accessed on social media and can be a threat to companies.
- What is said (and done) about attacks on social media and can impact companies.

The threats that organizations should consider are information leakage, identity theft, damage to the company's image or reputation and, in cases of attacks or malware, loss of data or operational capacity. The best thing to do to mitigate these risks is to address them in a preventive way, with the definition of a clear policy for the use of social media, including the definition of responsibilities and a code of conduct, enhance the awareness of employees and executives on the proper use of social media and what should be shared on these networks, and training on safe Internet surfing. A practice to be considered is the centralization of control of the official profiles of the company and its official representatives on social media, and also the creation of an approval process for messages to be published on these media. Action plans should also be created for incident response and crisis management, involving multidisciplinary teams, including areas of expertise, such as marketing, public relations and legal, in addition to technical areas.

By following these steps, your organization's life on social media will, for sure, be smoother.

9.4 **BIG DATA**

The concept of big data, where the main focus is on the storage of large amounts of data and increased capacity and speed in processing them, has generated considerable frenzy in the information security community.

On the security benefits side, the arguments are interesting: the new technology brings with it significant potential to increase the power of data analysis, which can improve the ability to detect cyber attacks and malicious activity by synthesizing and analyzing user and system behavior data, playing an important role in changing the information security model and making it more effective.

On the risk side, it is not just the security industry that is excited about big data: marketing and a number of other departments naturally see benefits in the technology, extending its use broadly: it can be used to generate deep market insights, provide tailored services to customers, and create operational intelligence. This range of possibilities, however, comes with inherent risks, as we have yet to fully understand the privacy and security risks when customer and business information is being collected, combined, processed, and stored at unprecedented scales and speeds. Greater volumes of data and greater ability to analyze that data across multiple areas of the enterprise minimally means more information available and spread around, with more work to control or protect it to prevent problems from occurring.

Again, the ways to address the new risks are through prevention, education and control. In the field of prevention, information classification policies need to be strengthened, with special attention to the definition of what can be shared and with whom, also covering aspects of legal and regulatory compliance and considering the specific requirements of each country, which will lead, for example, to the need to increase the robustness of access control structures. In the realm of education, it will be necessary to strengthen the technical knowledge of professionals, for example, by developing competence in data flow mapping in the security team. Finally, at the control level, the most likely path is the migration of the security vision to a data-centric protection model, which accompanies information in all phases of its life cycle. Another aspect to be analyzed is the acquisition or development, together with technology vendors, of tools to support the risk management of these large volumes of data, including the possibilities of better masking this data, meta-tagging, data classification, and refined access control.

According to Gartner Group, some of the technical challenges that relate to big data and will be part of the reality for information security professionals in the near future involve:

- Building more accurate models, malware heuristics, and malicious activity based on broad visibility and more computing power to perform the analysis.
- Community-based malware detection (model where multiple entities contribute to a common process).

- Creation of real-time reputation services that correlate information from multiple logical entities simultaneously, such as IP addresses, user identities, URLs, email, and file objects.
- Performing massive parallel static analysis of source code and binaries to identify vulnerabilities.
- Correlating threat data across multiple companies.
- Establishing security controls and policies that follow the user as they move between networks that they do or do not control.
- Cross-platform data correlation in the latest generation security platforms.
- Searching for patterns of abnormal behavior in large volumes of data on monitored transactions.

In summary, security will undergo major changes in the next few years, driven by this new trend in technology and use of information.

Conclusion

As proposed, this chapter provides an overview of some of the topics that are on the agenda of companies and Security Officers around the world, but it is far from exhausting the discussion. The themes covered need to be dealt with in depth, which is not our place to detail in these lines, which are intended to illustrate in a comprehensive way what needs to be evaluated and considered to ensure business security in virtualized environments, cloud computing, mobility/BYOD, social media and big data.

Most of the suggested concepts and controls will also help to ensure the security of information regarding new developments that may appear on the horizon in technology and information security. Nevertheless, the continuous search for updates, knowledge and information, always considering the reliability of the sources, especially on the Internet, must be part of the Security Officer's daily routine. Seminars and events about security happen constantly, in person or online, and are also important items to be part of the routine of security and technology professionals. Organizations such as SANS Institute, Gartner Group, ISACA and (ISC)², among others, as well as some technology vendors, are good sources of information and suggestions for best practices, and you should always use common sense to assess the applicability of each implementation to your business.

For the rest, it is the Security Officer's job as always: to remain attentive and diligent because, as the saying goes, "the devil is in the details".

Final Remarks

Regarding this compilation of shared perceptions and visions around security aspects, we should not be fooled into thinking that the subject is a new ingredient in the recipe. Security has been studied, planned, and applied for decades in the most diverse activities and for the most diverse purposes. If we take a brief look back in history, we will see different eras in which the assets, which held the attention and were therefore valued by companies in their business, changed dynamically.

Without much effort, we remember the importance of machines that represented all the competitive differential when applied in the automation of production lines, the large iron cabinets that stored more and more documents, and specifically files, with all the secret of the business, and now we see all the value and differential accumulated in electronic files circulating on computer networks that are increasingly connected, capillarized, and distributed.

The assets have changed, the values have changed, the pillars that support the production processes and operationalize the business have changed, the way to represent, handle, store, transport, and dispose of the company's assets has also changed and will continue to change dynamically and in an ever-increasing speed.

Given this, we have to extract the valuable essence of all these experiences, including the one we are going through right now, trying to accumulate them in order to continue the process - which seems infinite until proven otherwise - of planning the protection and management of information-related risks.

Regardless of future transformations related to the processes, the form and the technology adopted to promote the flow of data in the company, these will always be supporting information that cannot get out of our sights.

Extra Chapter 10

Security by Information: A futuristic exercise

This is an extra chapter and exclusive for the English translated version of the book and has the tone of story after participating in the Security Leader RIO 2017 as a speaker and debater.

The event, already traditional in the Brazilian calendar, seems to have arrived in good time. The Windsor Copacabana was literally crowded on the morning of April 27 when the monitors scattered through space already revealed the themes of lectures and debates. In the agenda of the day a varied menu that counted on investigation of cybercrime; breach of secrecy and privacy; safety in the workspace; cloud protection; threats and predictive methods; digital transformation; Industry 4.0; cognitive computing; risk appetite; Internet of Things; exercises of futurology and the long awaited National Information Security Policy. Definitely a day surrounded by interesting subjects and people with the purpose of thinking collectively about the dilemmas and gaps that permeate the routine of the Chief Information Officers (CIOs) and the other executives' nightmares.

It turns out that at some point, after seeing the vision of different people representing different roles such as supplier, consumer or simply thinker, and still varying in breadth of vision from the most strategic top to the most operational base, I noticed evidence of a mismatch about what the roles, responsibilities, and real complexity imposed by current information security risk management really are.

Immediately I remembered the book based on an old Indian fable and written by Ed Young, a Chinese born in 1931, named SEVEN BLANK MICE. The fable describes the routine of seven blind mice deciding to go out, one by one, to check out what was the strange thing they found near the pond, each returning with a different response. The red mouse thought it was a pillar. The orange mouse exclaimed to be a fan. The blue mouse claimed to be a snake. The next three mice also came back, each with a different idea. Until the last mouse upon returning and realizing that his perception did not resemble anything that the others had felt as well, he decided to coordinate the mess and collectively to hear each idea together to conclude that it was an elephant.

It was in this way that I realized the subject of information security being addressed throughout the day, lecture after lecture, debate after debate. Technical, tactical and strategic visions mixed by shooting in appliances, tunnelling, protocols, performance indexes, steganography, malware, zero day vulnerabilities, botnets, honeypot, deep web, BYOD, user behavior, rules for contracting cloud services, fear of the cloud, cloud types, cloud future - by the way, let's stop talking about cloud as if it were an E.T. Cloud service is a no-return path, just set your security requirements and hire the one that caters to you - plus intelligence artificial, cognitive computing and GDPR (General Data Protection Regulation). All legitimate views and purposes, it is true, but without seeming to be linked to a holistic, comprehensive view and attacking the imminent problem: the LIQUID INFORMATION of a liquid society, paraphrasing the concept established by Zygmunt Bauman.

For the author, we live in a time marked by the flexibility that causes a certain fragility as our relationships about things or people. This liquid society is compared to water because this natural element has the potential to change its shape according to its container.

We need to assume the liquefaction of information.

If we stop to reflect on the concept for a moment establishing a connection analogous to the knowledge society and the power of information, we will see great similarity. Let's see… The planet is totally interconnected and by fast paths. At the ends of these tracks are formerly only electronic devices or simply information technology equipment, but already coexist in exponential growth with physical-electro-mechanical devices or simply equipment of operation technology. IoT or Internet of Things is shipping connectivity and processing power into just about anything after it has overcome the barriers of miniaturization, power capacity, and the limits of communication. Still at the ends of the same pathways, we have people. People who live socially, but who have their habits changed in relation to devices and information in a general way. Devices that handle, store, transport, and dispose of information will be everywhere. We will be able to interact with things, talk to them, ask them for information, dress them and even ingest them. We will live virtualization to the extreme. We will no longer know where the information will be, what it will be doing with it, how, where, when, or who, if we simply continue to adopt the same perimeter-based security mechanisms that have lasted for decades!

We need to assume the liquefaction of information. Understand that there is no more boundary, time and space. We need to think about providing information about mechanisms of self-protection and self-management. Embark intelligence in the information itself so that, following rules defined by its owners regarding handling, storage, transportation and disposal, they themselves can decide where to go, how to go, with whom to go, when to go, or even when to remain confidential, entire and available.

Imagine the possibility that information, in the form of a data file, refuses to be handled, stored, transported or discarded just because the security policy established by its owner prohibits it?

Forget the concept that information acquires security by transferring trust in interlocutors, people, machines or systems. This border also no longer exists. The world needs interoperability, virtualization, decentralization, the ability to operate in real time, modularity and service orientation. If we study the evolution of security concepts in the last 20 years, we will see exactly this movement of decentralization, from CPD to end-point, as with banking services. Security has come out of the super coffers, migrated to the bank branches, then to the value transports, to the ATMs and finally to the user's mobile device. But one last step is still missing. Security must reach the last layer, the "centre of the onion": the information itself.

INFORMATION itself is the new and ultimate protection perimeter.

Obsession and the ability to keep secrets have driven the course of wars, monarchies and influenced life in society since ancient Egypt. The science of secrecy is transforming the way we perceive and guarantee privacy and data protection. As a witness to recent technological progress and information security practices in a fraction of the history represented by just under three decades, the exponential relationship of dependence between society and information in this new Digital Economy seems evident.

It is not necessary to resort to statistics that map the digital footprints of the world's citizens to recognize the volume with which we are producing digitized information, and the acceleration of the process of virtualization of the services we consume.

A brief analysis of our own behaviors will produce compelling evidence. We don't call people anymore; we no longer write letters; we no longer travel to a store or a public office; we no longer sign so many paper contracts; we no longer interview candidates by meeting them in person; and we hardly pay our everyday expenses with cash any more. Instead, we started composing emails; to send instant text and voice messages; to buy everything on e-commerce; to sign documents over the Internet; to establish human contact by videoconference; and to conduct almost frictionless financial transactions through mobile devices.

Where only material in the form of paper, pen, handshake and eye-to-eye was seen before, now we see a machine, a computer program, a network and an electronic signature.

The possibilities provided by the applied technology are limitless. Socio-economic relationships will never be the same, and the pivot of all this digital transformation is NET INFORMATION. For the Digital Economy to function widely, it is necessary to allow information to travel at speed, security and with a high capacity for interoperability, which means that it needs to be able to interact with multiple and distinct interlocutors, assume multiple forms, and react to multiple heterogeneous stimuli so that they do not succumb to potential operational barriers.

The concept of liquid information is anchored in the attributes of liquid media due to the ability to change its shape according to its container.

All theoretically evolutionary and functional, were it not for the side effects that such a transformation can generate. I exclude from this equation, at least in this article, the potentially negative effects on human relationships and the physical and mental health of individuals, just to name a few, and I focus on the impacts on information security.

Traditional perimeter-based security approaches, and therefore, the security offered by the containers that guard the data, do not offer broader effectiveness. Time took care of transforming the containers and their onboard security. Evolutionarily, they adapted to changes in information use behavior and managed, to a certain extent, to maintain acceptable levels of confidentiality, integrity and availability. We have seen the effect of decentralizing and pulverizing data. The decline of the mainframe, the private data center, the on-premise server, and now we witness the ineffectiveness of security at the endpoint perimeter, knowing that protecting a desktop, notebook or smartphone, for example, does not shield exposed business intelligence. in hybrid environments, wearable devices and IoT, susceptible to differentiated and innovative threats.

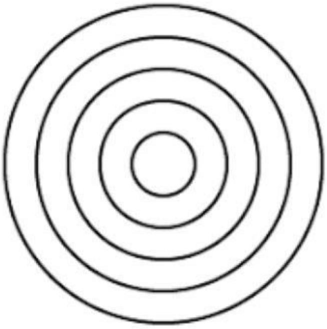


FIGURE 9.1

Visual representation of security approach by concentric perimeters in concentric data environment.

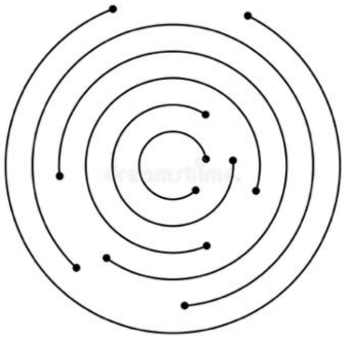


FIGURE 9.2

Visual representation of security approach by concentric perimeters in liquid and dispersed data environment.

I think that we have reached or are very close to reaching - depending on the degree of digitization of the country and/or the industry in question - to the limit of perimeter protection as we know it. Similar to what we are seeing with Moore's Law of 1965, established by Gordon Earl Moore, co-founder of Intel, which said that computer processing power would double every 18 months due to the pace of miniaturization of components and increasing transistor density. In computational terms, we have reached the limit of a physical perimeter and entered a new perimeter of atomic dimension, leading us, for example, to think differently and discuss necessary innovations such as quantum computing, as scientist Stanley Williams also understands.

Abandoning Moore's Law is a necessity to advance computing and drive processor manufacturers to innovate.

We therefore need to do the same with concentric perimeter-oriented data protection practices: deconstruct to rebuild. Data is on the path to becoming fluid, liquid, adaptable, interoperable, imperceptible, volatile, ubiquitous and, for all that, it needs to be protected in a more autonomous, intelligent and independent way, facing information itself as a new and final perimeter of protection: SECURITY BY INFORMATION.

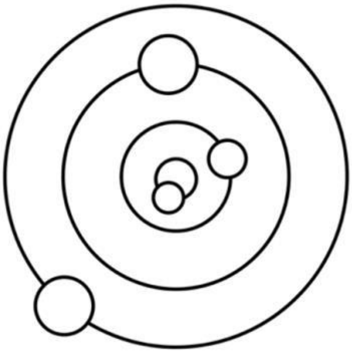


FIGURE 9.3

Visual representation of the hybrid security approach combining concentric perimeters and security by information in a liquid and dispersed data environment.

The information itself will have to acquire attributes of self-management and self-protection, in order to gain intelligence and autonomy. It will itself take care of exchanging credentials with its interlocutors: networks, devices, operating systems, apps and users, strictly following a treatment policy, which reads: handling, storage, transport and disposal, defined by its owner in some public repository. , available and reliable as in a blockchain environment, potentially incorporating artificial intelligence attributes that provide even more autonomy for decision-making if the information comes across some undefined scenario and not previously established by the treatment policies developed by its owner or influenced by laws and relevant regulations in your 'jurisdiction'.

By the way, this is an opportune moment to illustrate the SECURITY BY INFORMATION functional model, connecting it with the General Data Protection Law. In the time of LGPD and assuming the existence of an interoperable digital ecosystem in which security management is oriented towards the autonomy of the information itself, we would no longer need to worry about the conduct and adherence of interlocutors in the numerous commercial and/or consumption relationships in which processing of personal data.

The processes owned and managed by the controllers and operators of personal data will, by virtue of a globally accessible policy and published by the data subject, compulsorily respect the limits of purpose, suitability, necessity, free access, quality, transparency, security, prevention, non-discrimination and accountability, as conferred by law on the holders of these same data

Back to the liquid state of data and, consequently, of society, it is worth exploring the fragment of thought of the Polish sociologist and philosopher, Zygmunt

Bauman, born in 1925 and died in 2017 in the United Kingdom, who said that: "Society's liquidity is due to its inability to take a fixed form. It is transformed daily, it takes the forms that the market forces it to take, it does not favor the elaboration of long-term life projects."

In view of everything already exposed, we need to assume the liquefaction of information and react quickly and positively to it. Understand that there is no longer a border, time and space. That we need to work together and orchestrated to make the ecosystem of this new digital economy more intelligent, autonomous and prepared for the interoperability that new information demands. Combining new rules for manufacturing machines, protocols and computer programs as if paving a new path for a new information 2.0 that now needs to manage and protect itself.

Security by Information for information

In a new digital economy where services tend to be highly personalized oriented to the individuality of each consumer, we need to follow the same path, personalizing information security for information. If all this happens, we will see profound changes in attack and defense intelligence, and consequently, in the vectors of survival and business development.

Recommended Bibliography

1. NBR ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security management. Brazilian Association of Technical Standards, 2013.
2. KRAUSE M. and TIPTON HE. Handbook of information security management. 6th edition. Boca Raton: Auerbach Publications, 2007.
3. HUTT AE et al. Computer security handbook. 3rd edition. New York: John Wiley & Sons, Inc., 1995.
4. RUSSEL D and GANGEMI GT. Computer security basics. 2nd edition. California: O'Reilly & Associates, Inc., 2006.
5. HERNANDEZ S (ed.). The Official (ISC)² Guide to the CISSP CBK. 3rd edition. EUA: (ISC)² Press, 2012.
6. PARKER D. Fighting computer crime: a new framework for protecting information. New York: Willey Computer Publishing, 1998.
7. ISO/I EC JTC 1/SC 27 SD6. Glossary of IT Security Terminology. Information technology security techniques. 2013. Available at: http://www.jtc1sc27.din.de/sbe/sd6
8. SCHNEIER Bruce. Schneier on security. Indianapolis: Wiley Publishing, Inc., 2008.
9. PELTIER, T. R. Information Security Risk Analysis. Boca Raton, US: Auerbach Publications, 2000.
10. NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. Washington, US: US Government Printing Office, 2001. Available at http://www.nist.gov
11. NIST Special Publication 800-30: Risk Management Guide. Washington, US: US Government Printing Office, 2001. Available June 2003 at http://www.nist.gov
12. NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems. Washington, US: US Government Printing Office, 2003. Available at http://www.nist.gov

13. Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg, US: National Institute of Standards and Technology, 2004. Available at http://www.nist.gov
14. NBR ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management. Brazilian Association of Technical Standards (ABNT), 2011. 87 pp.
15. NBR ISO 31000:2009. Risk management. Principles and guidelines. Brazilian Association of Technical Standards (ABNT), 2009. 24 pp.
16. NBR ISO/IEC 31010:2012. Risk management. Techniques for the risk assessment process. Brazilian Association of Technical Standards (ABNT), 2012. 96 pp.
17. GUTTMAN, B and ROBACK, EA. NIST Special Publication 800-12, An introduction to computer security: The NIST handbook. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1995. 296 pp. Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Author

Marcos Sêmola
CISM®, CIPM®, CDPSE®, PCI-DSS®, ISO27K®LA

Information technology executive, expert in security: governance, risk and compliance with over 30 years of experience and international career with a track record at Módulo (BR), Schlumberger (BR), Atos Origin and Atos Consulting (BR/UK), Shell (NL/BR) and EY (BR).

Ernst & Young Partner accountable for the Cybersecurity Consulting Services in LAS, leading data privacy and protection and professional services for energy sector in the region, providing strategic GRC consulting enabling clients to understand and manage privacy and cyber risks through an integrated approach to build business trust.

MBA Professor at Fundação Getúlio Vargas business school since 2000 and at Fundação Dom Cabral, ranked the 10th best business school in the world by the Financial Times executive education ranking. Book writer author of seven, international keynote speaker, founder board member and counselor of ISACA®RJ chapter, vice president cybersecurity of SmartCity Institute, member of ABINC® Brazilian Association of IoT and AMCHAM® American Chamber of Commerce, former advisor of the CEBDS® Brazilian Business Council for Sustainable Development, member of IAPP® International Association of Privacy Professionals and IBGC® Brazilian Institute of Corporate Governance, founder member of the CSEC® Cybersecurity Enterprise Council Brazil, social leadership mentor at Gerando Falcões ONG, former director of RJ Founder Institute startup accelerator, entrepreneur, Endeavor business mentor and startup angel investor of Anjos do Brasil.

Bachelor's degree in Computer Science from the Universidade Católica de Petrópolis, Master in Business Administration in Applied Technology from Fundação Getúlio Vargas, Postgraduate degree in Strategy and Negotiation from London Business School, Postgraduate degree in Disruptive

Strategy from Harvard Business School, ongoing Master's degree in Innovation from HEC Paris. Trained by the Brazilian Institute of Corporate Governance as a Board Member.

Brazilian – Italian Citizenship, married, father of two kids, amateur street photographer, Ironman triathlete and Brazilian jiu-jitsu practitioner.

Major interests:
- information risk management
- digital transformation
- entrepreneurship
- education

www.marcossemola.com
www.linkedin.com/in/semola

This book enables companies to understand and manage privacy and cyber risks through an integrated approach to build business trust.

Information Security Management has long ceased to be a subject restricted to technology and has become a mandatory topic on the agenda of executives C-Level in Board of Directors meetings as a critical factor of success and survival for any business. Faced with this challenge, the author, who has dedicated more than three decades to the subject, shows in this book in a logical, didactic and direct way how risk management must be effectively elaborated in the adoption of personalized and integrated physical, technological and human controls that enable the risk reduction and management, leading companies to operate at a level of security adequate to the business appetite. This new translated edition of Information Security Management not only answers questions about why, when, where, what and how to plan an information security program, but also provides insights and useful tools for professionals involved directly or indirectly with the management of information assets and to all persons who hold information.

Author

MARCOS SÊMOLA

A 30 years' seasoned information technology and infosec senior executive. EY Cybersecurity Partner, Data Privacy & Protection Leader for LAS. Specialist in governance, risk and compliance, MBA professor, entrepreneur, keynote speaker, writer with seven published books, former vice president of ISACA-RJ, advisor at ABINC, AMCHAM, ISACA and SmartCity Institute, IAPP member, founding member of the Brazilian Business Council for Cybersecurity, former-director of the startup accelerator Founder Institute, social leadership mentor at Gerando Falcoes ONG, Endeavor business mentor and angel investor.

ISBN: 978-65-00-39842-7

9 786500 398427