Positioning Information Security Roles, Processes and Interactions

Dimitrios Papadopoulos[1] · Bernhard M. Hämmerli[2]

[1]Gjovik University College
Biskot188@hotmail.com

[2]Acris GmbH
bmhaemmerli@acris.ch

Abstract

All information security professionals around the globe acknowledge that "everyone is responsible for information security" in a company. This trivial statement looks clever but hides core challenges, "Who is everyone? How does everyone contribute or challenge information security?"

In our researched project we researched in-depth roles, processes and interaction in the corporate information security, by creating a framework for crystal clear defined roles and its associated security obligations and responsibilities. 20 corporate roles are analyzed from management and security perspective; classical interactions between information security roles leveraging and turning down security are given in case studies. Furthermore we generated structured tasks descriptions of the roles and open the road to the fulfillment of an information security consultants dream by creating Job descriptions including its security responsibilities!

We justified the necessity of defining roles and by introducing benefits of this approach:

1. Avoiding unnecessary conflicts and internal politics by establishing security organization with inclusion of all employees' duties.
2. Increasing security-level, efficiency and productivity by assigning clearly responsibilities.
3. Achieving good information security governance by encouraging coordinated team effort and mutual control.

Illustrative corporate examples demonstrate the need to supplement traditional corporate information security governance frameworks with roles and responsibilities for all positions.

1 A new Era of Information Security

We live in a modern world, where society has found a way to adapt to the rapid advance of technology using it in its advantage, providing a safe, secure and balanced environment to live in, in most parts of the globe.

The people in the developed countries of the world found a harmony between nature, technology and society. While nature is unpredictable and yet can't be totally controlled, people found a way to mitigate the risks and protect themselves from it, however the technology and society is well controlled by people. People live in a well-organized society where ground rules are established

H. Reimer et al. (Eds.), *ISSE 2013 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-03371-2_14,

and proper communications of those rules is in place providing a harmonized ecosystem. In which people elect the government, a government that establish the laws, the police departments and courts, which assure that the laws are obeyed and followed. However this ecosystem would collapse if people didn't possess an immanence sense of responsibility! Nothing would work if people were not responsible in our society. Whether this is a doctor saving a patient's life or a person driving a car on a road where children play, it is and always will be the sense of responsibility, combined of course with other people's characteristics such as ethics, beliefs etc. that drives a person to follow the rules create a harmonized ecosystem. The government is responsible to the people that elected it, the police and court authorities are responsible to the government and this creates an inner endless circle of responsibilities. But why we describe all this?

Corporation versus Governance:
A company is no different then a society. It is as well an ecosystem, with the top management also known as C-level executives playing the role of the government, policies, procedures and line managers playing the role of the police and court authority and the employees those of the people. The difference is that a company's goal is different from a society's, that of producing revenue. That's the responsibility of each and every member of a company to play his role and contribute to the process of generating revenue. We speak of revenue which is the ultimate goal but also a requirement for a company. A requirement set by its investors. Investors that are investing their money in a company create a need for protection. This need for protection is establish by laws, laws that will protect the people and their interests. Here is where information security enters the scene playing a vital role. Information security is the solution-means to the legal requirement of the protections of the investors and their investment. We define Information security as "a legal requirement that is met by the use of technology. " However information security is not something new, we have well established frameworks-solutions for information security governance in companies. Unfortunately we often see that the current information security models eventually fail. There are many various reasons for these failures but we wont go into details on these aspects but rather keep the fact. Having this fact in mind we took a holistic view on the bigger picture, we compare the companies with the society there lies the answer! In the society we have crystal clear roles and responsibilities, people know what to do and how to do it when it comes to the safety, the security and the balance of the society. Something that in corporation's level is clearly lacking.

Lack of knowledge:
Although the trivial fact that everyone is responsible for security is acknowledge by all the security professionals around the globe. There is no framework, analysis, research on what appears to be an insignificant word, "everyone". Who is everyone? How do they contribute or challenge corporate information security? That is what we explored. It is common knowledge that every company uses a sort of organizational structure and has crystal clear responsibilities assigned to the business units, managers, personnel etc., assuring that everyone contributes to the revenue process. But is it really remarkable that many neglect the problem, that all contribute to the revenue generation, by knowing their role and responsibilities, but few bare the challenging task to protect it! Which leads us to raise the question: "Are the CISO and security department magicians?" or is it time to realize that information security is a joint effort and responsibility. It is time to have security related responsibilities combined with the already management oriented responsibilities every company has. Thus, what roles and responsibilities study comes to contribute.

2 Chief Financial Officer

The role of Chief Financial Officer came to life in the late 1970s as a response to a new law the American government introduced. During those early years, the CFO was acting as the company's ambassador to its investors and financial analysts. His primary tasks were to manage relationships between shareholders and to assure that their expectations were met regarding the companies stock value among other things, such as managing sales, acquisitions, divestitures and ultimately generate revenue for the company. Furthermore, as the role evolved more and more responsibilities were added. The development of accounting gimmicks to lower taxes, the participation in strategic and operational decisions, the evaluation of business unit performance and invention of new ways to increase capital in the company as well as its protection from adversaries' takeover attempts, became routine things in a CFO's daily-diary.

New Responsibilities:
In the modern world and in the year 2013 we find that the CFO's role has changed from that of day-to-day management into that of a strategic thinker, shaping company's value and exit plan strategy, although it still inherits the characteristics of the previous years. The CFO is still responsible for overseeing all the "ancient" functions to come with the name. One of the newly duties of the CFO's role is dealing with information security. The CFO is one of the most important roles when it comes to security, he "sets" budgets, recommends cuts, provides the means for other departments to implement projects and run processes. Thus said, we understand that he/she is the person who will provide the IT budget, which usually will include the information security budget. Therefore, his understanding and beliefs about security are things that will either help security develop or become a serious drawback. Lack of security awareness and understanding will lead to costs cutting from the security budget and tie the hands of the CISO into managing the security threats of the company. Therefore, the starting point is the budget.

CFO and Security:
In order to set a budget for security the CFO has to understand and accept for a fact that security is not just an IT risk but it is a real business risk, therefore it has to be treated as such. It is a CFO's responsibility to deal with business risks and find ways to mitigate. That will put security on the top of the risk list. A CFO has to understand that security is a continuous process that means that security is a continuous risk and needs constant investment and improvement in order to be mitigated. Thus, a CFO has to acknowledge and fully understand a philosophy that [HoMi10] "The purpose of risk management is to improve the future, not to explain the past." Risk management is just the beginning! Compliance, Merges and Acquisitions, disaster recovery and business continuity plans among others things connect the CFO to information security. We can't go deeper into the analysis of each responsibility of the CFO but rather list them synoptically in table 1 & 2 below and refer you to the detailed study [DiPa13].

3 Chief Human Resources officer

What is a company without people? Can it exist without people? Of course not. They are the alpha and the omega of a company, they make the company. It's their existence that gives breath to any kind of operations or procedures. Thus, creates a need of a person to manage all of these people. That's the reason companies have a Chief Human Resources Officer.

Table 1: CFO Responsibilities

CFO Management Responsibilities	Task brief description
1. Business Strategy	Assess annual organizational performance. Assist in establishing yearly objectives and goals. Oversees strategic long-term budgetary planning and costs management in alignment with the board of Directors.
2. Financial Planning and Analysis	Conducts regular financial planning reports. Conducts analysis of financial conditions of the company and forecasts financial expectations. Develop and execute analysis of various business initiatives. Develop and maintain capital budget.
3. Finance and Accounting	Oversee cash flow planning and ensure availability of funds as needed. Oversee cash, investment, and asset management. Ensure legal and regulatory compliance regarding all financial functions. Lead the development of accounting gimmicks to lower taxes and increase revenue.
4. Insurance and Real Estate	Manage company's insurance program. Manage the company's real estate affairs.
5. Merges and Acquisitions	Plan, develop and execute merges and acquisitions. Conduct analysis, forecast and provide future outcome of penitential merges and acquisitions.
6. Business value and Exit plan strategy	Conduct analysis recommend innovations to grow business value and companies stock value. Develop and oversee the exit plan strategy for the company.

Old versus new:

Employees are considered as valuable resources for a company, but the fact is that they are people, which make it impossible for them to be treated like other material resources. Each and every one of them has their own special characteristics and requires a different approach and treatment. Thus, what the CHRO brings to the table, he humanizes the company's life and introduces human values in the company. But is he just a manager who deals with the employees' everyday? It was so some years ago where a CHRO was responsible for bringing employees and hiring the best employees that serves the needs of the company. Nowadays, they do far more then just bring new faces to the company. Today's CHRO is a complex role that has many requirements and expectations. He is a business partner, driver and talent developer, governance asset, employee recruiter, manager and evaluator. We wont analyze these functions of the role as they are analyzed in our full study [DiPa13]. But rather continue to see why the CHRO makes a difference regarding information security. Nowadays, it is not a secret that CHRO tend to be really well informed about the latest employee legislation, but they usually have no or very limited knowledge of information security. However, the CHRO plays a vital role on information security.

Table 2: CFO Responsibilities

Security Related Responsibilities	Brief Description
1. Security Culture	A CFO should be a security aware person. Allocate appropriate resources and funding for continuous improvement of security. Treat security as a business risk.
2. DRP and BCM	Participate and assist the CISO in the development of Disaster Recovery, Business Continuity strategies and plans.
3. Compliance	Oversee and enforce compliance with regulations to avoid fines and penalties.
4. Ensure financial assets security	Ensure that financial deals, contracts, auctions, forecasts, product launch dates and prices are things that are within the information that has to be protected and can affect the financial well being of a company.
5. Information Security in M&A	Ensure proper Information security infrastructure exists in the acquired company and compliance with regulations is in place and in order.
6. Bring-your-own-device policies	They raise a lot of security concerns and issues, such as data loss, inappropriate usage of devices, unauthorized access to non personal devices of the company and many more yet not fully revealed threats and risks that need to be handled and mitigated. If the CFOs haven't started to pay attention, now's the time to do it!

Employee characteristics:
Every employee that is hired has its own character, personality, education,"παιδεία»(pedia) an ancient Greek word that cannot be translated but means the way that a child is raised. How his character is shaped according to the principles, the beliefs, the values of his parents and the surrounding society he is living in. A person's honesty, dignity, self-respect and respect of others are characteristics that he gains from his early childhood and accompany him through his entire life. The way of thinking, the way of living, the traditions and principles differ from country to country and that what makes people different. Of course every person has a different way of life and different experiences but still, a country shapes the character of its people.

Reducing the Risks:
The CHRO is the person in charge for the hiring process of a company. Therefore it is essential for him to know all the above information for a person. Knowing the cultural background of the employees is essential for security and it gives you way more information about a person then from a curriculum vitae or an interview. It reduces the risk of employing personnel likely to present a security concern. Companies spend a lot of money to protect themselves from outside attackers but most of them forget about the insider threat and human errors, which eventually lead to information security breach and failure. Thus, where the CHRO plays a vital role by reducing the risk of hiring the wrong people and simultaneously being in an ideal position to drive security messages, policies and procedures. Here we would like to quote a phrase from Paulo Coelho. In an interview a reporter asked him whether he could describe the aim of his book in one sentence. "If I could do that, there is no need for me to write a whole book." Thus said, we can't go deeper in CHRO analysis in this paper without describing the whole study. Therefore, we will list the findings of our study of the CHRO role [DiPa13] listed in tables 3 & 4 below.

Table 3: CHRO Responsibilities

CHRO Management Responsibilities	Task brief description
1. CHRO a value creator.	The CHRO is a talent developer, he is a coach that will assist, guide, reward and motivate the employees in order to maximize their efficiency and productivity to assist the company achieve its goals.
2. Excellent recruiter	The CHRO has to be a great analyst and judge of character in order to hire the right people for the right position.
3. Business partner and strategist.	A CHRO as a C-level executive is a business partner, a key advisor to the board of directors and the CEO in the shaping of the companies strategy towards the companies goals and objectives.
4. Performance evaluator	A CHRO will evaluate the employees' performance and take appropriate measures if necessary.
5. Balancer	A person who will solve any conflicts that might rise between employees, despite their rank, top level employees or simple staff and create a happy and friendly working environment.
6. Manager	The CHRO will assist and oversee the daily governance functions of a company, such as arrange board meetings, interact with employees, ensure regulatory compliance and oversee and assure high quality human resources services that include enhancing controls for human capital processes and mitigating risk around HR.

Table 4: CHRO Responsibilities

Security Related Responsibilities	Brief Description
1. Excellent scouter and character analyst.	Knowing the cultural background of a potential employee reduces the risk of employing personnel likely to present a security concern.
2. Employees Awareness and education driver	The CHRO is in an ideal position to drive security messages, policies and procedures.
3. Hiring, Termination and Relocations keeper	The CHRO keeps track of the access privileges an employer has, had to perform his duties and when those have to be terminated.
4. Identity and authentication	The CHRO has to establish that applicants and contractors are who they claim to be.
5. Valuable asset and advisor for security.	The role of the CHRO is to assist and provide counsel and solutions interacting with the CISO in order to mitigate all facing risks.
6. Security incidents investigation asset.	The CHRO will provide valuable insight, in understanding the elements of the job, and they will help prepare the investigator to ask the right questions, and help preserve the rights of the suspect employee.
7. Solid understanding of information Security	The CHRO has to have a very good understanding of what Information Security means to the company and what kind of people and skill-set are needed to perform such job.

4 Cyber Warfare

Today we hear all around us the term cyber attacks on a daily basis. We have seen a group of hackers named "Anonymous" perform various "Denial of Service" attacks and defacement attacks on various Government's web servers and private corporations. On 27th April 2007 Estonia was the victim of one of the biggest coordinated cyber attacks where it also affected the general

public. A foreign government was considered to be the initiator of this attack. We have seen other examples of such attacks like: Titan Rain which was a series of coordinated attacks on American computer systems in 2003, Flame which is a Data-stealing malware that was used for targeted cyber espionage initially in Middle Eastern countries and afterwards spread into Europe and USA. It is labeled as one of the most complex malware ever found, Stuxnet is a computer worm which targeted Iran's nuclear facility which was designed to affect exclusively Siemens supervisory control and data acquisition systems (SCADA) that control and monitor industrial, MiniDuke a highly customized malicious that used a PDF exploit in Adobe Reader creating a backdoor was used to attack NATO and European governments and institutions. These are just some of the few ways today's wars have been transferred to cyber space and terror scenarios have already been developed claiming that a multifaceted cyber attack coordinated professionally could take down air traffic control systems, telecommunication grids, create a chaos in the stock market and even deny people from basic needs such as water, electricity and even emergency services such as ambulance dispatch, fire departments and police if the radio bands are silenced.

This scenario as terrifying as it sounds, with the rapid advance of technology and the constant evolution of networks is not far from becoming a reality. The modern world categorizes these threats with a buzzword as "The advanced persistent threat (APT)". The APT acronym is constantly misused in the IT security scene and a misconception is generated, people tend to think that APT is a sophisticated malware attack. However it is not the sophistication of the malware rather the attacker's determination and resources he is willing to allocate to succeed in his mission. That is the real threat of the APT, It is not a what, but who? The power of the APT lies in the competence, resources and motivation an attacker has who will never stop until he reaches his objectives, whether this is theft of intellectual property or damaging a country or company, he will adapt to the security measures you have deployed and will find a way to breach information security or he will quit if the costs of the attack exceed the value of the prize he is after.

Companies Cyber warfare:
We speak of a cyber war between governments where intelligence gathering and espionage is common practice. This is no different between companies. Cyber attacks on companies are a commonality in our modern world. Attacks such as data theft could be used to blackmail the owners of a company in order not to release the data captured which would expose the information security failure of the company and damage her reputation. The attacker could also threaten the company in performing denial of service attacks taking the company temporary out of business. Both of these cases result in money lost for the company. Cyber threats are a new and evolving source of risks and most of the companies aren't yet prepared to mitigate and handle such risks. There is no secure company in any sector and the threat is growing but nobody can say that the world had not been warned. The world Economic Forum (WEF) in 2012 placed cyber attacks on the top five threats the world is facing, next to threats of weapons of mass destruction, they emphasize that cyber threats shouldn't be underestimated. Written below is an example of how a company can become can become cyber savvy and mitigate one of the most emerging threats the world and companies are facing by having a crystal clear delegation of roles and responsibilities.

Roles & Responsibilities:
The CEO has to understand the risks and the opportunities that the cyber world presents and lead the way to the company's entrance to the virtual world. The CRO has to conduct constant risk assessments of the cyber threats and with the collaboration of the CISO and CIO to ensure that the IT department is constantly evolving its capabilities to deal with cyber risks. The CISO has to

cooperate with other C- level executives and line managers, from which most importantly with the CHRO and the COO in order to develop an awareness campaign and educate the users about the current emerging cyber world and the risks it hides. The CEO with the board of directors has to invest in the development of cyber skills. This means shaping the strategy of the company in order to mitigate the threats by having experts handling the threats. As a consequence, the responsibility of the CHRO is to recruit talented people and to collaborate with the CISO in the development of a plan on providing constant education and cyber skills development of employees, because it is difficult to recruit an expert with those skills in the current market therefore companies have to create their own.

The CEO and board of directors have to allocate resources on the cyber threat and ensure its mitigation like any other threat the company faces and one of the core measures is to sponsor the creation of a Cyber incident response team a team that will be able to monitor, gather intelligence about the constant evolving cyber threats and prepare plans to mitigate them communicating from board level to business operations and even cooperating with other companies to strengthen their knowledge and share expertise. In addition, the company's strategy should be aggressive and active against attackers defending the company with legal means prosecuting the attackers. Thus, the requirement of a great CLO who will be well informed on cyber laws and requirements. Last but not least the CMO has to communicate publicly about cyber threats, incidents and responses promoting the cyber threats risks and promoting an information security awareness and culture.

5 Delegation of Duties

In this section we would like tell you a real life story. An intern was working in a big commercial bank and the director of the branch as well as the deputy director and some senior officers with access privileges to the banks systems due to their overloaded work schedule trusted the intern with their user-IDs and passwords and asked him to perform various tasks for them on a daily basis. Thus a very familiar situation to many people working in a network environment where users privileges and access controls are in place, people do share credentials in order to get a job done. This is a huge mistake and exposes the company's information security to various risks. In the case of the intern, the highest-level officer is the branch director, in many other companies the same situation could happen where a CEO gives his credentials to his secretary or somebody else to do some tasks for him. But lets analyze this situation further, what could the intern or anyone else in the same position do. There are three possible courses of actions a person can do:

1. It's your boss, so it's okay to do this.
2. Ignore the request and hope he forgets.
3. Decline the request and remind your supervisor that it is against security policy.

Choice Dilemma:
The intern chose at first option number two, but this never works. Unfortunately for him, he had no other choice but to accept the trust of the director and the senior officers and hopping that nothing goes wrong. If something did go wrong and an incident did occur, during the investigation he would be the first to take the blame, because he is the weakest link in the circle. The management would face the constituencies for giving out the passwords and would be held accountable but the intern would have to go and prove that he did nothing wrong and that was

a risk for him personally, as specially as it was in the interns case a financial bank where large amounts of money are processed on a daily basis and he could end up facing criminal charges and possibly pay settlements to the bank if any money was lost or stolen.

A lot of us would here raise a question? Why it is that the intern didn't choose the correct answer that is obviously the third option? This is not a choice made only by the intern, but many other employees who don't dare to choose that option although it is the correct choice. There are two explanations, one is that the users don't have security awareness and education which means that they have never read or familiarize themselves with the security policy of the company or because they trust, respect, fear their supervisor and know that a possible answer like that would endanger their relationship with them, something that will lead to possible disadvantages or change of behavior of the supervisor towards them.

Lessons learned:
This example illustrates a very common situation that happens in every company where we have delegations of duties and hierarchical roles distribution. This situation is tough to handle because of its nature and it is based on the relationship between people. Information security can be compromised and exposed by such behavior on some occasions or in the intern's case, luckily everything ends with a happy end. These delegations of roles and responsibilities is a risky game and the CISO has to be a balancer in between managers, C-level executives, supervisor, directors and users ensuring that all are educated and understand the consequences both for the company and themselves on a personal level of such behavior. Thus, understanding that the access controls and user privileges are there for a reason, the same reason we have different roles in a company, therefore avoiding the credentials sharing is a must for every company.

6 Why Roles & Responsibilities make a difference?

We covered only a small part of the studied roles just to illustrate our research [DiPa13], however we demonstrated the necessity of the roles and their responsibilities. And as any other two way relationships wherever there is a need for something there should be a benefit from the solution. Among many others we list bellow the key benefits that crystal clear roles and responsibilities delegation and definition bring to information security governance as a supplement.

1. They establish an organizational structure avoiding chaos, unnecessary internal politics and display compliance with internal policies, laws and regulations.
2. They mitigate the risk of information security staff being a single point of failure and ensure and promote C-level executives support for information security as well as establish formal communication channels with them.
3. Improve security & business processes: By assigning clear responsibilities: security level increases and processes improve becoming more efficient and more productive.
4. They enable greater allocation of company's resources minimizing the costs of provision of adequate information security functions.
5. Achieving good information security governance by encouraging coordinated team effort and mutual control.

7 Conclusion

We opened Pandora's box on an area that clearly lacks research. Thus, of roles and responsibilities. It is essential for companies to understand that everyone within a company is responsible for information security. There can't and shouldn't be only one person to blame if something goes wrong. Security is an overall process and everyone, one way or another, has to contribute in order to make it work. Any control measures can collapse in seconds if people don't understand that they also play a role in the information scene.

References

[DiPa13] Papadopoulos, Dimitrios: Positioning the roles, interfaces and processes in the information security scene, Information Security Management, Gjovik University College 2013.

[HoMi10] Hoehl, Michael: Creating a monthly information security scorecard for CIO and CFO. SANS Institute InfoSec Reading Room. 2010.