RISK MANAGEMENT AND INFORMATION ASSURANCE: THE INFLUENCE OF THE HUMAN FACTOR AND ETHICS ON ENTERPRISE'S INFORMATION SECURITY AND CYBERSECURITY

GESTÃO DO RISCO E GARANTIA DA INFORMAÇÃO: A INFLUÊNCIA DO FATOR HUMANO E DA ÉTICA NA SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA NAS ORGANIZAÇÕES

ROGÉRIO GIL RAPOSO

Resumo Alargado

Curso de Mestrado em Segurança da Informação e Direito no Ciberespaço

Lisbon, 2016

Abstract

Information Security and Cybersecurity, though related mostly to the protection of Information Systems and digital information, is nevertheless the end-result of human decisions taken upon concrete or undefined scenarios. Decision processes are normally designed through frameworks that intend to limit subjectivity in the analysis of the situation posed for decision and to provide tools for an informed-based decision that better fits the situation. As long as decisions still continue to be influenced or determined by persons, the set of fundamental principles and beliefs in which those persons have been educated and are living on (in a personal and professional sense) will have influence in the overall analysis made in order to sustain the decision to be made. Risk Management is a process where important and sometimes critical decisions have to be made and Ethics, consciously or unconsciously, frames the set of possible decisions that can be taken.

Keywords: *Cybersecurity, Ethics, Human decision process, Information Assurance, Information Security, Risk Assessment*.

Introduction

Information Security and Cybersecurity, though mostly related to the protection of Information Systems and digital information in technological environments, is nevertheless the end-result of human decisions taken upon concrete or undefined scenarios. Decision processes are normally designed through frameworks that intend to limit subjectivity in the analysis of the situation posed for decision and to provide tools for an informed-based decision that better fits the situation. As long as decisions continue to be influenced or determined by persons, the set of fundamental principles and beliefs in which those persons have been educated and are living on (in a sociological, personal and professional sense) is something that will probably have influence in the overall analysis made in order to sustain the range of possible decisions that need to be taken.

Is it expected to have ethics influencing decisions? In what extent are ethical principles carved in frameworks that intend to transform self-minded decisions into rational and logical driven decision, where emotional factors should not influence the necessary decisions? How does ethics and psychological factors affect Risk Management, as a process where important and sometimes critical decisions have to be made and ethics, consciously or unconsciously, frames the set of possible decisions that can be taken? We firmly believe that as long as decisions and decision models are shaped by humans, ethical postures will have influence in the way the decision-making process is modelled. Ethical issues can also be present in the decision itself, not contradicting an eventual existing framework but in the sense of the evaluation of the impact of that same decision in the light of common or personal ethical principles. These challenges are certainly present, with more or less intensity, in every decision taken over critical or sensitive issues that impact other persons live, even if not having a direct impact.

The human decision process towards Risk

Risk is something that is present in all stages of our lives and inherent to the human decision process. In fact, all of our decisions, more or less critical or important, have as a common baseline the assessing of the risks and benefits offered by the several options available in what regards the decision to take. Also inherent to the human decision process is our capability to make different choices in face of different or equal situations, regardless of them being a threat to us or not.

Humans are a social-driven species, thus human interaction is a social need that follows us with more or less intensity. Those interactions, especially the ones that we are exposed to in regular bases or since childhood, provide us with a common framework of behaviours, beliefs, rules and restraints that have influence in the way we individually do things, how the community accepts or forbids some kind of events and, of course, how our society or nation binds us to pre-determined behaviours. These rules that bind and direct us to a certain way-of-doing things normally have beneath them common accepted principles. These principles of expected human conduct towards what the community or society expects from us are often exposed in the form of rules or regulations, normally accepted as mandatory.

Considering then that we have formal and less formal rules and principles that guide us and limit the scope of possible conducts, we find it acceptable that decisions toward risk management scenarios may be also linked, even though involuntary, to those same rules and frameworks referred above, even though without explicit references to them. We tend to accept this linkage due to several aspects that characterizes the activity of managing risks through more or less complex situations, and

the situations and risks that arise from Information Security, even though “less physical” than “real-life” situation, still have a strong human factor over them.

Ethics and Organizations

The expected conduct and behaviour, the guiding principles in which our common beliefs stand on or the standards from which we judge if an action is acceptable or not. All of these aspects can somehow define or are encompassed in Ethics and summarize the values, duties, responsibilities and obligation that guide our conduct (Freud & Krug, 2002). Despite being abstract in terms of the different interpretations they can acquire if acknowledged through different political, cultural or religious point of view, they are still in line with has been referred above about the human’s social characteristics, as ethics stands as one of the pillars in which societies are built on, modelling and shaping some aspects of nations, enterprises and organizations.

We can find ethical principles “spilled” over laws, rules, policies or general guidance documents that intend to shape and direct acceptable or mandatory behaviours. In an organization, it is common to find ethics coded into acceptable postures for the organization’s employees, aligned to the organization’s culture, which is often aligned to the overall culture of the enterprise’s ecosystem, environment, strategy and culture. Ethical postures are here desired from everyone in order to push the overall performance of the organization to success, imposing duties, fostering intentions and promoting dignity and respect for others (Bowen, 2000). These postures, in spite of being present in every action and decision made, are normally more visible and demanded in face of the responsibility and position of who has managerial duties, for it is up to these roles the task to decide well and to decide in benefit of the organization and the well-being of those who depend on it.

From what has been referred so far, one can understand the importance of ethics considerations in the responsibilities and competences of managerial roles, for it is from these roles that one expects greater responsibility and legitimacy in actions and decisions (Bowen, 2000). Managers are expected to tackle ethical organizational, business and personal problems within the constraints of doing so according to the law, the interests of those affected by its decision and the obligation of doing it for the welfare of others according to the basic principles of justice (Bose, 2012).

Risk Management for Information Security

Looking at what is expected from managers at an enterprise governance level, the need to consider all governance domains (processes, technology, people, internal environment and external environment), as all of these aspects deeply concur for the wanted “health” of the enterprise, is in fact a challenge in terms of professional and personal skills. Information Technology resources are where most of an enterprises’ information is stored, processed and transmitted, thus needing security procedures implemented through risk-based informed decisions. The importance of risks to Information Technology resources arise from the value of today’s digital information, which makes them a valuable asset that needs to be firmly protected from the wide scope of technological threats. Beyond this fact is the true assumption that if the Information Technology resources are handled by humans, then the threat referred above are not only technological but also driven from the possibility of unintentional misuse.

A definition for Risk in the Information Security environment can be found in many different sources and literature, being the most relevant the ones brought to us by the ISO/IEC 27000 and

National Institute for Standards and Technology (NIST) standards, which define Risk, respectively, as a "*effect of uncertainty on objectives*" (ISO/IEC, 2014, p. 8) and "*measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence*" (NIST, 2012, p. 6). Even though not explicitly negative, the normal concept of risk as the likelihood of something bad to happen can have a more positive approach. A different and positive approach to the meaning of risk can underline the possibility of risk to also mean the wanted impact of an event that sustains the Risk's existence, in which case it could be more appropriate to call it an opportunity. Either we consider risk at a negative perspective or a positive one, the existence of risk is an undeniable truth, thus its management has become a need for every organization(s) and enterprise(s) in order to properly plan, organize, coordinate and control how to use its resources to maintain productiveness and overall business strategy, through the assessment and treatment of the risks identified.

The interdependence and interconnections between today's organizations has a clear effect in a wide range of domains that did not affected organizations in the past. Having the information concentrated and dependent on technology and being one of the main benefits of technology the automated procedures, sometimes invisible, in treating and getting the best out of the information available, organizations are vulnerable to threats that in the past wouldn't have such a high impact as they have today. Human errors, hardware failure or software errors are sometimes invisible or stealth threats that can have a tremendous impact in the overall performance of an organization and that can be even potentiated by the size, scope and level of complexity of the technology in place (Laudon & Laudon, 2006). This same reality has also changed the way managers face their responsibilities today, more focused on the environment that surrounds the enterprise but facing internal and external threats as cyberattacks and supply chain management challenges in order to succeed towards the enterprises' goals and objectives (Campbell, 2015). One clear example of the direct impact that these challenges have on their operations continuity can be the importance that a supply chain represents in the organization's systems and processes. In face of the criticality of having trusted and on time products and services, the imperative of having trusted procedures for identifying the activities and resources needed to get or deliver products and services that are necessary for everyone involved in it, clearly emphasizes the importance of an effective supply chain risk management in place. Several strategic objectives and aligned risk-informed decisions concur for the need to have such an effective supply chain management, being cost reduction or control, reputation and especially security some of those objectives. Other aspects worth pointing about Enterprise Risk Management for Information Security, directly connected to the ability, competences and skills needed for a manager, is the need for managerial information in order to make risk-informed decisions that concur for properly addressing the risks facing the enterprise. This information should be pulled of a proper ongoing assessment of the measures taken to treat the previously identified risks. Security assessment and metrics represent the core activities for measuring the effectiveness and suitability of the controls applied or other mitigating risk measures taken, in order to be able to score those metrics against organization or enterprise's goals and objectives, or to address the residual risks that still remain after those controls/measures have been applied. The importance of metrics is already a common accepted idea for enterprise operational

assessment, through several methodologies that, at the end, reflect the performance of the enterprise in face of pre-determined goals and objectives. In what security is concerned and on issues related to risk management, the correct choice of the metric's framework to be used to assess the risk mitigation decisions is a vital step, as the metrics chosen will determine if the risk is being addressed properly, for example to evaluate if the residual risk can still be tackled or is to be accepted as it is, if the effects of the controls and measures applied are the ones that were expected or even to discover previous undetermined risks that were not yet identified.

Risk management applied to Information Security governance is then, in short but holistic terms, the necessary processes to be engaged by the appropriate managerial level of every organization as a way to demonstrate commitment to Information Security and to empower every necessary decision in order to guarantee that the right processes for identifying, assessing, responding and monitoring risks are in place and obey to the existing governance guidelines.

Managers in Enterprise Risk Management for Information Security

Several personal qualities seem to be needed in order to guarantee that managers facing today's complex reality can take the right decisions. Having stated the influence of the social environment and ethics on people, one can probably assume that managers' decisions will be somehow in line with their perceptions of what the society and, at an organizational level, their co-workers expect from them. At this step we find it important to emphasize some of the characteristics that are considered important in today's managers regarding the way they face risks at a professional level, and how their ethical posture, personal and professional, influences the decision they take and the decisions that are expected from them.

Everyone expects leadership qualities from a manager. This seems quite obvious and understandable, as it is expected from him strong and steady actions and decisions to defend, lead and enhance success towards the market where the organization stands on. Leadership qualities, in spite being somehow obvious and desired in managers, can be ambiguous concerning the type of leadership applied by the manager and the acceptance of it by the managed. Inside leadership qualities one can identify several others considered good in the light of the set of qualities that are desired and that can influence the leader to "good" decisions. Some of these sub-qualities are vision, assertiveness, courage, honesty, creativity and solid moral-standards. These leadership's attributes are very likely to be found in most of the literature regarding ethics and ethical behaviours in western societies, as they are widely considered good attributes for everyone to have and to put in practice. We believe that leaders are no exception. In fact, people seem to demand more from managers and from the ones with special responsibilities, as their decisions and actions are more likely to have an effect on peoples' lives than the actions and decisions of someone with no special responsibilities over concrete aspects and assets on which others depend on.

Bringing risk management to the equation of how managers deal with it in face of their responsibilities and their personal (ethical) qualities, we believe that the above referred qualities are crucial and somehow stressed in these situations. Facing risks and deciding over them is, as we have seen before, a continuous and demanding process. Even though supported by technology and by a set of other resources, we consider the act of deciding a lonely act in the overall and crowded risk

management process, where moral discipline regarding the interests of the whole is more important than self-interest (Campbell, 2015). Risk-based decisions are complex and often supported on some amount of subjectivity when assessing the threats that originate the risks. Through a manager point of view, the ethical qualities referred above and a proper ethical framework towards risks are then of the upmost importance to minimize the uncertainty in assessing the risk and how to address it, as to minimize the possibility of overconfidence and self-aspiration for professional competence and personal satisfaction (Marshall & Ojiako, 2013). This is still true even regarding Information Security Risk Management, where well defined metrics with adequate purposes, scopes, objectives and values, assume an essential role in near real-time assessment of the effectiveness of countermeasures in place and the determination of trends, patterns and behaviours useful for the ongoing risk assessment process and decision making initiatives.

Ethics in Managers and Risk Management influenced decisions

Until this point we have stated that risk management, as long as we continue to have people deciding and conducting businesses/operations, will always have a portion of the human side affecting it, most of the times through ethical influenced decisions even if this philosophic aspect is not directly cited or called upon in the decision act. This is inherent to humans and has reflections even on the way risk management frameworks are created, as these frameworks follow the natural and overall accepted guidelines that define the moral boundaries of what is allowed, what is prohibited and what is desired for the well-being of the organization, community and society.

Managers are people who should share the ethical values of the society and organization they belong to or in which they perform their duties. Although being responsible for guiding their organizations to success and compliance with strategic objectives, their performance is also under evaluation through a formal and ethical perspective by the ecosystem in which they operate. Having a managerial role implies having certain rights and obligations that belong to that role, as long as they are assigned to it (NIST, 2013). This consistency cannot be detached from an ethical perspective and evaluation of the managerial performance and it requires specific competences and skills from the manager. Other aspect to be considered is the manager's ability or consistency in making decision that follow the compliance guidelines of the organization but go against its own ethical guidelines. How should a manager perform in face of such a dilemma and how is he expected to behave are two different questions posed to the manager by the ones affected by his decisions and by himself in front of the ethical dilemma. There would probably be as many answers as questions in dealing with such a problem, as compliance in business doesn't always stands for moral accepted conducts (Campbell, 2015). The bottom line in this issue is the ethical framework that binds the manager to deal with stressing situations in the light of his own ethical principles, which should have been part of his characteristics that got him in that specific managerial role. In a "perfect situation", his own ethical principles should be perfectly aligned whit the compliance and ethical principles of the organization in which he performs, thus there wouldn't be the need to decide against his own principles or against the organization's compliance guidelines.

Manager's ethical characteristics can also be in evidence in stressing situations where the personal posture is decisive for a determined threat or risk. These characteristics in specific situations are normally associated and complementary to the leadership qualities referred above. Attributes like

temperance, wisdom, prudence or sense of justice are always personal qualities that define a leader in face of different and stressing scenarios. Sometimes these personal attributes are called upon situations where there is a gap between the organization's compliance guidelines and its ethical framework.

Conclusions

Ethics and ethical behaviours are inherent to humans and they stand as guiding principles and limitations for what we naturally accept as good or positive in our relation with other persons and with other entities. They stand for values, duties, responsibilities and obligations acquired through a person's development, education and socialization process, in social and different aspects as are political, cultural or religious postures.

Risk is something that is present in throughout our lives and leads us into decision makings in the light of an unstructured or structured risk management process. Enterprise risk management for Information Security allows the identification, assessment, treatment and reporting of different risks that arise from the entire ecosystem in which enterprises are inserted, looking to all different inner and outer threats and respective probabilities of them becoming an impact.

Managers are expected to lead enterprises and to decide over risks that can have a negative or positive impact. From managers everyone expects leadership qualities and firm actions towards the collective goals and objectives. These qualities are normally associated with the ethical principles of what is considered good and moral-based, like assertiveness, courage, honesty, creativity and solid moral-standards. These attributes are normally appreciated and part of organization's posture towards its goal and objectives, in what is normally considered the organization's culture. It is expected from leader to impersonate the organization's culture and to perform as the organization and himself where as one, as it is recognized that the manager's actions and decisions will have an effect both on the employees and other people related directly or indirectly to the organization, as in the organization itself, regarding its reputation, robustness, success and resilience.

The interdependence and interconnections between today's organizations and the complexity of the digital environment that shapes and our society is equally responsible for the visibility and globalization of information and businesses and for the vulnerabilities driven from technological and human derived threats that can have a tremendous impact in the overall performance of an organization, specially due to the complexity of the technology in place. This reality has changed the way managers perform today and what is expected from them regarding actions and decisions towards risk.

It is expected from a manager to perform in the light of the organization's principles, using the best of his own ethical values facing responsibilities. Strong and good ethical qualities are importance to tackle uncertainty and fear in assessing the risk, and to limit the possibility of overconfidence and self-aspiration for professional competence and personal satisfaction. Manager's ethical characteristics are also important in difficult situations where leadership qualities are decisive in scenarios where there is a gap between the organization's compliance guidelines and the expected results of the decisions made in the light of those same guidelines, hence the need for including ethics in organizational risk management frameworks.

References

Bose, U. (2012*). An ethical framework in information systems decision making using normative theories of business ethics*. Ethics and Information Technology, 14(1), 17-26. doi:http://dx.doi.org/10.1007/s10676-011-9283-5

Bowen, S. A. (2000). *A theory of ethical issues management: Contributions of kantian deontology to public relations' ethics and decision-making* (Order No. 9982787). Available from ABI/INFORM Global; ProQuest Dissertations & Theses Global. (304606497). Retrieved from http://search.proquest.com.nduezproxy.idm.oclc.org/docview/304606497?accountid=12686 on 02/07/2015

Campbell, K (2015). *Can Effective Risk Management Signal Virtue-Based Leadership?*.Journal of Business Ethics. 129:115–130. doi 10.1007/s10551-014-2129-4 doi:

Freud, S., & Krug, S. (2002). *Beyond the code of ethics, part I: Complexities of ethical decision making in social work practice*. Families in Society, 83(5), 474-482. Retrieved from http://search.proquest.com.nduezproxy.idm.oclc.org/docview/230160167?accountid=12686 on 29/06/2015

ISO/IEC 27000/2014 - *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (2014). ISO/IEC

Kissel, R. (Ed.). (2013). NISTIR 7298 Revision 2 - *Glossary of Key Information Security Terms*. Gaithersburg: NIST. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf on 04/07/2015

Laudon, K. C., & Laudon, J. (2006). *Management Information Systems - managing the Digital Firm*. Upper Saddle River, New Jersey: Pearson - Prentice Hall.

Marshall, A., & Ojiako, U. (2013). *Managing risk through the veil of ignorance*. Journal of Risk Research, 16(10), 1225-1239. doi:10.1080/13669877.2013.788056

National Institute of Standards and Technology. (2012). NIST Special Publication 800-30 rev1 - *Guide for Conducting Risk Assessments*. Final Public Draft. Gaithersburg, MD 20899-8930, USA: U.S. Department of Commerce. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf on 02/07/2015