AWARENESS IS ALL YOU NEED

Topic: Ethics and information security

Yinqiao Li

2024.03.29

CONTENTS

ABSTRACT

This report studies the ethics and information security issue, concentrating on due care and due diligence concepts, policies, laws, and how to address unethical and illegal behaviors. It emphasizes the effectiveness of voluntary due diligence is constrained and limited. Besides, compared to the overstatement of other studies, this report highly advocates the effect that self-awareness plays in the aspect of the routine operation of an organization.

1 INTRODUCTION

In recent years, the incidence of information leak and security issues has surged dramatically. A medical data breaches figure can tell, approximately 5 million medical records were exposed in the world in 2018, however, the number had tripled in the next year. The same issues of information security and ethics are even more severe in other industries, making the protection of information security an urgent matter.

Define due care as the level of care that a reasonably prudent person would exercise under similar circumstances, according to Webster's dictionary. In business, due care is the effort made by a prudent party to avoid harm from another party to protect its interests. In the field of Infosec, due care specifies a more focused and specific meaning. It is the effort made by an organization to protect the information of multi-parties, including customers, employees, stakeholders, and managers, in case of a data leak or other information security incident. specifically in this course, in the aspects of physical security, operations security, communications security, network security, and information security.

Joint Institute, Central China Normal University, University of Wollongong

In contrast to due care, the concept of due diligence is the complementary counterpart of due care. While due care represents the continuous effort for information security requirements, due diligence is characterized by spontaneous investigations of human nature, preventing harm from the perspective of the independent individual, instead of self-regulation. In the information era, the complication of security protection missions can be viewed as a nightmare. The complexity of the network, the diversity of the information, and the rapid development of technology devices, make Infosec protection a tough challenge.

The execution of due care and due diligence highly relies on the crafting and application of sturdy policies. Policies are organized recommendations that outline the organization's approach to sustaining due care and conducting due diligence. They are the documented standards and procedures that articulate the organization's commitment to Infosec and the expectations for the behavior of the organization. Policies serve as the foundational support for due care, in contrast to laws, which are ratified societal directives, acting as a guide for decision-making and offering a definitive structure for the organization's reaction to the changing terrain of cyber dangers.

While policies direct internal conduct, laws establish the binding legal standards. Due diligence involves the proactive pursuit of potential Infosec vulnerabilities. Both serve as fundamental tenets of cybersecurity, ensuring that an organization's practices conform to both legal obligations and ethical standards. Due care in Infosec is an organization's diligent effort to protect against data breaches, a responsibility that has grown in complexity with technological evolution. This principle, alongside due diligence, constitutes the cornerstone of robust cybersecurity policies. Policies, distinct from but informed by laws, provide a systematic approach to navigating the complex network of Infosec challenges, ensuring that ethical standards and legal compliance are met. Together, they create a coherent framework that supports an organization's commitment to securing its digital landscape.

2 FOUNDATIONS AND STRATEGIES FOR INFORMATION SECURITY

In this section, the foundations and strategies for ethical information security, including the concept of due care, due diligence, policy, and law, and the three general categories of unethical and illegal behavior will be discussed. Due care and due diligence are two fundamental concepts in the field of information security, and they are closely related to the policy and law, which are the foundation of ethical information security. The interrelationship between these concepts and the three general categories of unethical and illegal behavior will be discussed in this section.

2.1 Due cares versus due diligence

In cybersecurity, due cares include regular updates to security protocols, ongoing staff training, and prompt responses to known vulnerabilities. Here we will answer two questions.

1. Why should an organization make sure to exercise due care in its usual course of operation?
2. Why due care and due diligence are both important?

Many information security breaches are not caused by inadequate protection methods, but rather by a lack of continuity in management practices. Therefore, The organization should make sure to exercise due care in its usual course of operation continuously in order to protect the rights of multi-party stakeholders. Marko Niemimaa and Marko concluded that the necessity of continuous due care in Infosec is based on conceptual foundations for IS continuity[1]. In the actual IT industry, whether it's technology, products, or equipment, everything is constantly being updated, and inevitably, there are threats to information security. They pointed out several reasons an organization should make sure to exercise due care in its usual course of operation, including liability, and interest of stakeholders. It is crucial to continuously implement due care to maintain security.

The effective implementation of due care is a self-assessment of regulations. Mostly, the due care exercise is entirely based on the organization's regulations, however, due care can be examined by the employees themselves, according to the research of Rossouw von Solms and S.H. Basie von Solms. Rossouw von Solms and S.H. Basie von Solms proposed a due care method to evaluate whether due care is properly implemented through several concise self-asked questions for staff[2].

On the other hand, due diligence is a process of assessment from a third-party perspective, assessing potential cybersecurity risks, verifying the vendor's compliance with relevant standards and laws, and continuously monitoring their performance and adherence to security protocols. Garrett, R. D. et al. find voluntary commitment dedicated to due diligence had been proven ineffectual[3]. The emergence of multiple ethical issues indicates that relying solely on corporate voluntary commitments to resist unethical behavior is pale. Sellare et al. pointed out that due diligence is a necessary complement to due care, and it is a necessary measure to prevent unethical behavior[4]. Based on the penetration of several pieces of research on due care and due diligence, it has been deduced that the effectiveness of non-mandatory supervision is negligible in resolving ethical and security issues.

2.2 Policy and Laws

In contrast, policies are the mandatory guidelines with responsibility enforcement, and laws are the societal mandates that are binding and compulsory. Siponen et al. performed research on the organizational compliance culture, discovering that deterrence plays a significant role in the actual adherence to policies, whereas incentives do not have a notable impact on policy compliance. Thus, the effective implementation of policies, due care, and due diligence as discussed in the previous section, are highly dependent on the deterrence of laws. Legal deterrence not only has positive significance for employees to comply with rules and regulations to protect information security but also appropriately adding legal knowledge to employee training can prevent companies from avoiding illegal and unethical circumstances. Crete-Nishihata et al. conducted a study on the effectiveness of law enforcement training and found that law enforcement training is effective in reducing the number of illegal activities[5]. The company's policies can be effectively implemented only under a legal and regulatory system with complete mandatory effect. A law, being a structured set of rules for societal welfare and equity, is more formal, however, a policy, functioning as a mere statement or document of future intentions, is comparatively informal.

2.3 Three General Categories of Unethical and Illegal Behaviour

Three general categories of Unethical Behavior are:

1. Accident: who makes mistakes and result in threats to information
2. Intent: intent of doing wrong
3. Ignorance: they just don't know any better

Although unethical and illegal behavior is categorized into three traditionally, the nature of intent and the other two. Behavior originating from accident and ignorance should be educated rather than strictly punished, and complemented into regulations if necessary.

Regarding addressing these three general categories of unethical and illegal behavior, many attempts have been made. As discussed previously, continuous awareness education and training have an overwhelming advantage compared with other methods like advanced technology, policies, and laws. Although the deterrent influence of laws and policies is advantageous for encouraging employees to comply with regulations to safeguard information security, the effective enforcement of laws and policies largely depends on employees' self-regulation and self-awareness. Awareness of behavior constraints and norms proves to be most impactful. Thus, companies must strengthen educational efforts and training initiatives among employees to bolster their self-awareness and self-regulation abilities.

3 DISCUSSION AND IMPLICATIONS

Many researchers have studied several ways to guarantee ethics and information security. Throughout the journey from regulation to implementation, from legislative formulation to the enactment of policies, and taking into account the principles of due care and due diligence, both managers and researchers have investigated and analyzed a multitude of approaches to ensure the security of information. From a legislative perspective, countries are progressively refining their laws and regulations regarding information security. Although some nations have been late starters, the efforts made by the majority of countries towards policy orientation in protecting information security are noticeable. Kitsios et al. conducted a study on a program implemented in the information technology sector to ensure compliance with the International Organization for Standardization 27000. However, the authors found that a significant portion of risks went undetected and were overlooked after the company adopted these standards. The rapid expansion and iteration of company operations and technology demonstrated that a static and uniform security model is insufficient for modern information security needs[6].

Differing from the focus on law and policy implementation emphasized by other researchers, Mikko et al. observed an inspiring phenomenon: social influence, particularly the culture of compliance within a company, has a significant and positive impact on employees' adherence to information security practices. Drawing from their findings, awareness is key. The authors suggest that managers must guarantee the enlightening of personnel regarding cybersecurity dangers, their potential impact, and the swiftness with which these threats can proliferate within the enterprise[7].

It is undeniable that the standardizing impacts of laws and policies have played an effective overseeing and limiting role in the past. However, long gone are the days when information security and ethics could be ensured through legislation and policies alone. Given the current circumstances, it appears that the effect of laws and policies can be somewhat under-estimation, which unavoidably leads us to ponder on what is the best approach for addressing an unlawful or unethical activity. Countless managers have overestimated the positive effect that policies and laws brought, and innumerable researchers have overstated the self-supervision effect that due care contributed. Administrators have exerted excessive effort in the development of regulations, yet they have overlooked the positive impact of employee awareness. Beyond systematic constructs, the enhancement of awareness through learning and training is indispensable. In the ever-evolving cybersecurity world, there is no such thing as a perfect system. Perfection in systems does not exist. Nonetheless, human consciousness plays an undeniable role in security and ethics.

Different from other studies, what this article wants to emphasize here is that the role of continuous training and supervision of employees in the daily operations of companies and organizations has been underestimated in terms of enhancing employee awareness of information security, standardizing operations, and avoiding ethical issues. As previously mentioned, awareness is the key. Consciousness plays a strong role in the restraint and regulation of operations.

4 CONCLUSION

In the structure of guaranteeing ethical rights and information security, due care and due diligence can be effectively implemented based on complete laws and policies. One best methods to address this is the power of awareness. Perhaps laws and regulations may be slow to keep up with the latest developments and technologies, but the power of robust security awareness for future information security challenges should be emphasized. Therefore, continuous training in relevant security awareness is essential.

REFERENCES

[1] Marko Niemimaa. Information systems continuity process: Conceptual foundations for the study of the "social". *Computers & Security*, 65:1–13, 2017.

[2] Rossouw Von Solms and SH Basie von Solms. Information security governance: Due care. *Computers & Security*, 25(7):494–497, 2006.

[3] Rachael D Garrett, Sam Levy, Kimberly M Carlson, Toby A Gardner, Javier Godar, Jennifer Clapp, Peter Dauvergne, Robert Heilmayr, Y le Polain de Waroux, Ben Ayre, et al. Criteria for effective zero-deforestation commitments. *Global environmental change*, 54:135–147, 2019.

[4] Jorge Sellare, Jan Börner, Fritz Brugger, Rachael Garrett, Isabel Günther, Eva-Marie Meemken, Edoardo Maria Pelli, Linda Steinhübel, and David Wuepper. Six research priorities to support corporate due-diligence policies. *Nature*, 606(7916):861–863, 2022.

[5] Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui, and Ronald Deibert. The information security cultures of journalism. *Digital Journalism*, 8(8):1068–1091, 2020.

[6] Fotis Kitsios, Elpiniki Chatzidimitriou, and Maria Kamariotou. The iso/iec 27001 information security management standard: how to extract value from data in the it sector. *Sustainability*, 15(7):5828, 2023.

[7] Mikko Siponen, Seppo Pahnila, and M Adam Mahmood. Compliance with information security policies: An empirical investigation. *Computer*, 43(2):64–71, 2010.