ARTICLE TITLE

Topic: Ethics and information security

Yinqiao Li

2024.03.29

CONTENTS

ABSTRACT

This part is less than 200 words.

Joint Institute, Central China Normal University, University of Wollongong

1 INTRODUCTION

In recent years, the incidence of data breaches and security issues has surged dramatically. In 2017, approximately 5 million medical records were exposed globally, and by 2018, that number had tripled. 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 aprudent 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 its customers, employees, and other stakeholders, in case of a data breach or other information security incident, specifically, in the aspects of physical security, operations security, communications security, network security, and information security. 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 Infosec objectives made by organizations, due diligence is characterized by spontaneous investigations of human nature, preventing harm from the perspective of the independent individual. In the information era, the complication of security protection mission can be viewed as a nightmare. The complexity of the network, the diversity of the information, and the rapid development of technology devices, all of these factors make the Infosec protection more difficult. The implementation of due care and due diligence highly relies on the development and enforcement of robust policies. Policies are structured guidelines that outline the organization's approach to maintaining 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 behavior of the organization. Policies act as the structural underpinning for due care, contrasting with laws, which are established societal mandates, serving as a roadmap for decision-making and provide a clear framework for the organization's response to the dynamic landscape of cyber threats. While policies navigate internal conduct, laws set the binding legal standards. Due diligence involves the proactive pursuit of potential Infosec vulnerabilities. Both stand as fundamental tenets of cybersecurity, ensuring that an organization's practices adhere to both legal obligations and ethical standards. Due care in Infosec is an organization's dedicated effort to protect against data breaches, a mandate that has grown in complexity with technological evolution. This principle, alongside due diligence, forms the bedrock of robust cybersecurity policies. Policies, distinct from but informed by laws, provide a structured approach to navigate the intricate network of Infosec challenges, ensuring that ethical standards and legal compliance are met. Together, they create a cohesive framework that underpins 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 the 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 based on conceptual foundations for IS continuity[**?**]. 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 organizations should make sure to exercise due care in its usual course of operation, including liability, interests 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 own regulations, however, due care can be examined by the employees themselves, from 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 staffs[**?**]. 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 in due diligence had been proven ineffectual[**?**]. 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[**?**]. Based on the penetration of several researches on due care and due diligence, it has been deduced that the effectiveness of non-mandory supervision is negligible on resolving ethical and security issues.

2.2 Policy and Laws

In contrast, policies are the mandatary guidelines with responsibility enforcement, and laws are the societal mandates that are binding and compulsory. Siponen et al. performed a 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 that 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[**?**]. 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

In regarding to address these three general categories of unethical and illegal behavior, many attempts have been made. As discussed in the previous, continuous awareness education and training has a 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, it is imperative for companies to 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 way to guarantee 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 clearly demonstrated that a static and uniform security model is insufficient for modern information security needs[**?**]. 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[**?**].

4 CONCLUSION

This part 250 words.

REFERENCES