The effectiveness of governance and regulatory bodies in protecting information security.

James Robinson

East Carolina University

ICTN 6823

***Abstract*-Appropriate and proper understanding and of IT security should be considered an essential and pertinent requirement within any modern business amongst its executives and employees. But, as we have seen throughout recent news, this has not been the case for many companies. This text explores the effectives of governance and regulations as it relates to protecting our information security. This text focuses on the different organizations' businesses have implemented with hopes of increasing security standards. The articles, figures and tables used in this paper will further elaborate the importance of these organizations and practices within companies**.

I. Introduction

Governance in any organization, whether it is either a business or a nation, is a critical asset that provides structure and a general body of rules which everyone agrees to follow. Without governance or regulation, there would be grounds for chaos and uncontrollable and unpredictable risk. There would be no balance of interests between the customers, executives, and many of stakeholders, posing a threat to internal security. Governance doesn't necessarily have to be an approval body whose sole responsibility is rubber stamping things. Rather, organizations have tackled this issue from many different angles. An organization's governance body could be a group of semi dedicated individuals from cross discipline teams who gathers together to decide upon things related to company policy, and in our case their security posture. This organization

could also be a group of dedicated individuals who partner across the organization to set standards and best practices related to their own domains. However, the one question which can vary in answers across different organizations and perspectives is how effective are these organizations or regulations which are responsible for protecting information security. In this paper we will discuss the different types of organizations businesses have implemented to drive strategy in protecting its data and systems; how these organizations operate and what type of policies or standards are implemented by these organizations. Finally, we will discuss how effective these organizations are or was at protecting its businesses interests including its data. This paper will attempt to tie together the importance of identifying the correct governance model for your organization. because as we will discuss in the paper there is no one size fits all when it comes to implementing a governance model or process within your organization.

II. Consequences of not having security standards.

Before we dive into the different types of organizations businesses and governments have implemented to protect their information security; let's discuss the impacts and consequences of not having this type of body of regulations and standards. The retailer Target has become the foot of every security breach joke for its famous security breach which compromised over 40 million customer credit cards and debit cards. Customers' financial and personal information were in jeopardy of being compromised. "The absence of a chief information security officer was a "root cause" of the major computer systems breach at Target last year, said a former manager at the retailer". [1] Clint Boulton, Wall Street Journal, 2014. Without governance bodies having oversight over things such as best practices and implementing standards around information security, instances such as the Target breach will most likely occur. It's also not enough to just to

have standards; standards can become useless as well as governance bodies if there's no way to enforce these standards or regulations.

III. Internal Risk Management

Internal risk management is just one of the many organizations' companies develop in strives to protect their private or critical information and applications. "The high-level strategic security policies are specified at each consecutive level down the hierarchy and finally implemented in information systems and operational procedures. The process phases are linked forward and backward through the communication structure linking the governance spheres. This allows change in requirements at any level to propagate requisitely through the organization. Intermediate levels in this chain of propagation filter out aspects that are not relevant for the next level, e.g. operational level micro design focuses only one facet of the overall policy that is implemented in an information system" [12] J. J. Korhonen, M. Yildiz and J. Mykkänen, "Governance of Information Security Elements in Service-Oriented Enterprise Architecture," 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsiung, 2009. Some smaller organizations or projects which are more innovative or are dynamic in nature tends to manage their own risk as a project level. Larger organizations or projects which are business critical, tend to follow a more centralized body of regulations. According to the Harvard Business Review, there are three different types of risk management organizations that businesses introduce to bring governance and standards across their organization.

A. The first is independent experts, "JPL, for example, has established a risk review board made up of independent technical experts and their role is to challenge project engineers' design, risk assessment, and risk-mitigation decisions. The experts ensure that evaluations of risk take place periodically throughout the product-development cycle. Because the risks

are relatively unchanging, the review board needs to meet only once or twice a year, with the project leader and the head of the review board meeting quarterly." [2] Robert S. Kaplan and Anette Mikes, Harvard Business Review, 2012. Risks Review Boards are an effective way to manage risk in organizations, because doing so would increase awareness of information security across the organization. This model particularly encourages an ownership mindset for employees or individuals working or participating in related activities. They also feel empowered to enforce and discover security or vulnerabilities which could impact their interests or business.

B. The second type of governance companies may implement to improve their security posture is by utilizing facilitators to aid in managing their security risks and governance. This approach can be very effective, especially when your staff has no direct knowledge of information security or information security across disciplines other than their respective domains. "In order to improve the communication between teams, we union the pattern of communicate with people related to risk; we often implement risk management together with specific risk management patterns, such as the continuous process pattern" [10] Robert S. Kaplan and Anette Mikes, Z. Yali, "Teamwork Pattern of Project Risk Management Based on Knowledge Reuse," 2008 International Conference on Information Management, Innovation Management and Industrial Engineering, Taipei, 2008. Having a facilitator ensures communication and collaboration across security risks and best practices. However, there are many critics of this approach as in a way it reduces ownership of security risks by having someone manage the risks who many are not an expert of the overall technical ecosystem outside of the realm of security. This approach could also become less effective when your managers or project owners start focusing on

making deals with the facilitators or other managers as opposed to having a focus of identifying and mitigating security risks. When managers become distracted on the financial aspect, they sometimes neglect the security risk that are apparent.

C. The third type of governance model embeddes experts within project teams, which is the most effective approach. This model typically involves a security expert being embedded within a project team to be responsible for identifying and mitigating risks. The unique thing about this individual is their reporting structure within the team or company. “Teamwork pattern of risk is usually being used in these conditions, when different teams in charge of different aspect situation in a project. These teams may belong to an organization or may come from other external organizations. Every team have their own internal project risk management, and they have the ability of control and tracking their work that they are responsible for.” [10] Z. Yali, "Teamwork Pattern of Project Risk Management Based on Knowledge Reuse," 2008 International Conference on Information Management, Innovation Management and Industrial Engineering, Taipei, 2008. This approach has better structure and organization. This individual should report to both the in-line manager of the team and a central security governance body, this body is typically represented by the office of the CISO (Chief Information Security Officer). This type of reporting structure encourages the individual to uphold duties inside and outside of the team which they are held accountable for. However, selecting the type of governance structure for to a company’s overall information security posture is not at all simple and as cut and dry as explained above. “In many cases, security groups are themselves divided into different units, dealing with information security, strategic risk and risk management, business continuity, operational security, network operations, infrastructure, architecture

and engineering, policy development, and so on. Reporting relationships also vary between organizations— "most security executives report (directly or indirectly) to the organization's CIO, while some report to executive committees of the company's CEO or the company's general counsel." [3] M. E. Johnson and E. Goetz, *IEEE Security & Privacy*, vol. 5, no. 3, pp. 16-24, 2007.

So, what type of polices or regulations do these governance boards or committees implement? The type of work produced by these organizations can differ depending on the type of board or domain the board represents. Internal risk and security audit teams typically enforce security standards and polices set out by domain experts. Domain expertise would typically come from the teams which are engineering the solutions within an IT organization. The Internal risk and security audit teams would also typically adhere to a set of security policies and controls which are agreed upon by a larger external governing body of security experts. Illustrated below is one of the most popular set of security controls which comes from the center of information security.

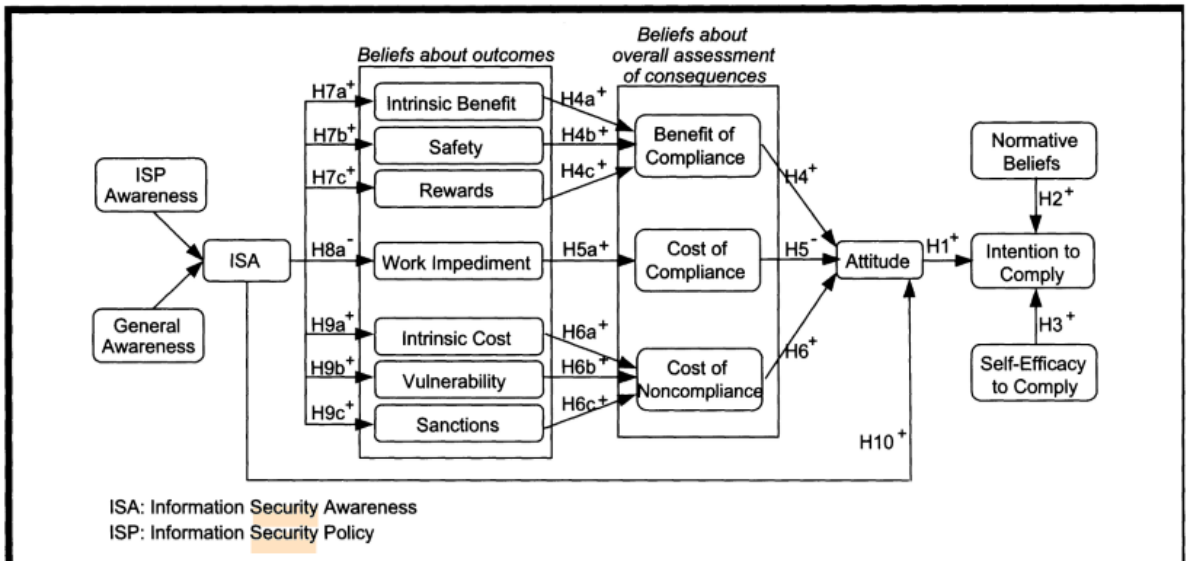

Figure 1. A Proposed Model of the Antecedents of ISP Compliance

Table 1. Definitions and sources of constructs taken from the theory of planned behavior		
Construct	Definition	Sources
Attitude toward compliance with the ISP	The degree to which the performance of the compliance behavior is positively values.	Theory of Planned Behavior
Normative beliefs	An employee's perceived social pressure about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers.	Social Bond Theory
Self-efficacy to comply	An employee's judgement of personal skills, knowledge, or competency about fulfilling the requirements of the ISP.	Social Cognitive Theory
Intention to comply	An employee's intention to protect the information and technology resources of the organization from potential security breaches.	Theory of Planned behavior

[figure 1 and table 1] Bulgurcu, Burcu, et al., Harvard Business Review, 2012 MIS Quarterly, vol. 34, no. 3, 2010, pp. 523–548].

Many organization's internal risk teams typically follow this type of model to mathematically identity the company's true security posture. "Risk management is the systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, evaluating, treating and monitoring risk. On top of regular risk repositories and check lists, several specific risks must be stressed in global development projects. They relate to two major underlying risk drivers, namely insufficient processes and inadequate management." [5] C. Ebert, B. K. Murthy and N. N. Jha, 2008 IEEE International Conference on Global Software Engineering, Bangalore, 2008. This allows for data driven decision making as it relates to technical and security related

investments and compliance the internal security policies. Enterprise Architecture is another way large corporation ensure governance across their business. This organization typically consists of various types of technical architects; for the purpose of security an enterprise architect can own the domain of security for the company. Their responsibility would be working with various teams to develop and implement best practices and security polices and guidelines across the organization. "IT governance focuses on overall enterprise development from organization, responsibility, strategy, performance, resources and conformance and etc. and makes overall evaluation and gap analysis for enterprise IT. It can help leaders make right decisions based on comprehensive understanding of the enterprise through setting up unified architecture, investment strategy and decision method." [11] S. Zhang, S. Yang and J. Song, "Research on collaborative IT governance model oriented to business architecture," Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Whistler, BC, 2013. Within Enterprise architecture there could be another architect who's responsible for ensuring project work adheres to the standards being developed by other domain architects such as the security architect. This architect works closely with the project team and acts as either a governance representative or a more involved solution architect for the project or product. Both the solution architect and the security architect work together to ensure the security posture of the company meets expectations. "The amount of the innovation risks can be determined through calculations that show that for every ten venture firms one or two of them are successful. However, the risks affect the profits several times higher than development of another business activity type. This quality allows innovations to exist and develop actively. The innovation risks will increase in the context of localization of the innovation project. If there are many projects, and they are applied by industry-types, according to the law of large numbers,

risks are minimized, but the probability of innovative entrepreneurship success increases. It is also important that the profit from the successful innovative projects is so significant that it justifies the costs of all other failed developments" [6] C. Ebert, B. K. Murthy and N. N. Jha, 2008 IEEE International Conference on Global Software Engineering, Bangalore, 2008

IV. IT Governance

"IT governance provides a basic structure aligning IT processes, IT resources, and organizational needs of implementing strategy to achieve more effective values through relationships of organizations. IT governance is inseparable from organizational success of ascertaining measurable improvement of online business processes. It enables effective organizational strategy through strategic alignment of IT and businesses. IT governance is the structure of relationships and processes directing and controlling organizations by providing additional values of the use of IT." [8] S. Kosasi, Vedyanto and I. Dewa Ayu Eka Yuliani, 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018. Many of the different types of governance models all have some type of impact on the organizations which they serve. The effectiveness truly depends on the culture and overall stance and awareness of security at an organization. Businesses who tend to invest more in security typically come out better than those who do not. This is not just because of the substantial financial investment made but the awareness of security within the culture of the company. Companies who have a CISO (Chief Information Security Officer) are fortunate because they have someone accountable for taking on security risks of the company proactively as their day to day. This organization will typically drive the company to invest more into their security perimeter as well as security education for the organization. The more employees are educated about security the better off the company will be when it comes to defending itself against cyber and modern threats. Organizations with some type

of ownership mindset around security encourages better practices and creates a culture of security awareness. This is critical for a company to effectively manage and mitigate cyber threats. "It is important, however, to understand how security program management and governance are distinct. The function of governance in information security is to establish security strategies and objectives that align with business strategies and objectives [15]. By setting these strategies and objectives, information security program managers understand where risks are tolerated, and to what level that toleration exists. "Governance also establishes levels of resources and the risk-mitigation priorities for such resources, whether those resources be funds, personnel, or other capabilities"[7] W. LIdster and S. S. M. Rahman, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications. Without this understanding, organization's efforts for security governance can pretty much diminish as the focus becomes timelines and due dates as opposed to ensuring the best possible security posture or stance for the company. Ensuring proper balance between the roles of line manager or product owner and facilitator and creating the most appropriate governance model which fits your organization should be the focal point. There's no cookie cutter approach however to implementing the perfect governance model. This is something which can depend on a vast amount of variables which all would depend on things such as the size of your business or organization, the size of the project or the number of projects which would come through this governance process as well as but not limited to the timeline and frequency of the projects. "Structures are relevant to the governance process as they provide enabling mechanisms to facilitate contact between IT and the board of directors. In this paper IT board involvement is identified as a structural aspect likely to influence alignment." [9] W. LIdster and S. S. M. Rahman, J. Kuruzovich, G. Bassellier and V. Sambamurthy, "IT Governance Processes and IT Alignment: Viewpoints from the Board of Directors," 2012 45th

Hawaii International Conference on System Sciences, Maui, 2012. This level of contact is extremely important as it makes these governance boards more visible to the stakeholders which ultimately will decide how the business is conducted; given the organization is setup such as corporations. Visibility at this level allows the governance organization to articulate their concerns arounds security, policy and funding among many other concerns. The more transparent these types of organizations are, the increased the visibility becomes, which as a result increases the effectiveness of the organization overall. This in return will improve the overall security and risk posture of the organization or business the governance organization is representing. "The mapping between security governance tasks and roles as well as the development process phases to the Agile Governance Model is quite straightforward. This mapping helps us organize information security governance in complex enterprises." [12] J. J. Korhonen, M. Yildiz and J. Mykkänen, "Governance of Information Security Elements in Service-Oriented Enterprise Architecture," 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsiung, 2009. Depending on the type of software delivery lifecycle (SDLC) your organization runs on would be a good indicator of which governance model to implement. The Agile methodology has been around for a while, but it is still pretty new to the industry, however this method can be one of the most straight forward to implement in an organization which already supports agile. Tntroducing this into a waterfall like organization would take more thought, time and effort to implement properly.

V. Conclusion

Overall, governance can be an effective part of your business or organization's ecosystem and thrive. Proper governance also ensures that adequate security measures are in place, protecting pertinent information. However, it's extremely important to understand the nature

of your business which will ultimately decide what governance model is most appropriate to implement at your business or organization. Governance organizations as we discussed previously can come in many different forms and shapes; some of these forms could be as an organization such as Enterprise Architecture or an Internal Risk and Security management team. One of the most important areas to consider, which is almost the most important of all these processes, is ensuring executive or C level support within corporations or businesses. The equivalent level would be needed for non-business entity organizations. This level of support is important because it was a direct affect on the amount of support and resources which would be allowed for IT security. This level would also be able to provide some type of guidance and governance around how process and operations should work-day to day.

Works Cited

1. C. Boulton. “Target’s Lack of CISO Was ‘Root Cause of Systems’ Breach.” *Wall Street Journal*. Sept. 30th 2014. [Online]. https://blogs.wsj.com/cio/2014/09/30/targets-lack-of-ciso-was-root-cause-of-systems-breach/. [Accessed July 16th , 2019].

2. R. Kaplan, A. Mikes. “Managing Risks: A New Framework.” *Harvard Business Review*. June 2012. [Online]. https://hbr.org/2012/06/managing-risks-a-new-framework. [Accessed July 15th, 2019)

3. M. E. Johnson and E. Goetz, "Embedding Information Security into the Organization," *IEEE Security & Privacy*, vol. 5, no. 3, pp. 16-24, May-June 2007.

4. Bulgurcu, Burcu, et al. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.” *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 523–548. JSTOR, www.jstor.org/stable/25750690.

5. C. Ebert, B. K. Murthy and N. N. Jha, "Managing Risks in Global Software Engineering: Principles and Practices," 2008 IEEE *International Conference on Global Software Engineering, Bangalore*, 2008, pp. 131-140.

6. A. S. Nechaev, S. V. Zakharov and A. O. Troshina, "Innovation risk minimization and neutralization methods," 2017 *International Conference "Quality Management, Transport and Information Security, Information Technologies*" (IT&QM&IS), St. Petersburg, 2017, pp. 552-555.

7. W. LIdster and S. S. M. Rahman, "Obstacles to Implementation of Information Security Governance," *2018 17th IEEE International Conference On Trust, Security And Privacy In*

Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 1826-1831.

8. S. Kosasi, Vedyanto and I. Dewa Ayu Eka Yuliani, "Effectiveness of IT Governance of Online Businesses with Analytical Hierarchy Process Method," 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018, pp. 1-6.

9. J. Kuruzovich, G. Bassellier and V. Sambamurthy, "IT Governance Processes and IT Alignment: Viewpoints from the Board of Directors," *2012 45th Hawaii International Conference on System Sciences*, Maui, HI, 2012, pp. 5043-5052.

10. Z. Yali, "Teamwork Pattern of Project Risk Management Based on Knowledge Reuse," 2008 *International Conference on Information Management, Innovation Management and Industrial Engineering*, Taipei, 2008, pp. 416-419.

11. S. Zhang, S. Yang and J. Song, "Research on collaborative IT governance model oriented to business architecture," *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design* (CSCWD), Whistler, BC, 2013, pp. 116-120.

12. J. J. Korhonen, M. Yildiz and J. Mykkänen, "Governance of Information Security Elements in Service-Oriented Enterprise Architecture," 2009 *10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaohsiung, 2*009, pp. 768-773.