ROLE OF CISO IN ORGANIZATION

JAROSLAV REMEN – MILAN KUBINA

***Abstract**: There is no single, recommended organization structure that works for all organizations. There is, however, an optimum one for each organization. All organizational structures have inherent advantages and disadvantages. Information security organization design is influenced by a host of factors specific to each enterprise that must be well understood before the adopted structure can work optimally. Security leaders often have unrealistic expectations about the ability of organizational change to solve problems in their security programs.*

***Keywords:** CISO, reporting, cybersecurity, efficiency, digital security*

***JEL Classification:** D8, L8, M15, M21*

1. INTRODUCTION (PURPOSE OF ARTICLE)

Organizations have diverse understandings of what digital security is and is not. As a consequence, they wrestle with who is responsible and who is accountable for organizations' digital security. This further complicates the question of whether the chief information security officer (CISO) position ought to be considered and instituted. CISO positions and responsibilities are greatly unsettled since digital security crosses many aspects of enterprise transactions, challenging if it is even possible to place boundaries on the responsibilities of the role.

Do organizations expect the CISO to be a technology wizard, business savvy or a hybrid of both? Do organizations expect the CISO to be the responsible and accountable person in securing the computing environment and informational assets in the enterprise? Should the CISO be part of the executive team, or should the role be confined within the information technology (IT) group? The subject of digital security within an organization creates a dilemma within the executive team with regard to defining the CISO role within the organization. There are several key gaps between what senior management may want or expect from the cybersecurity function and how far-reaching the responsibility of the CISO role ought to be that can be identified, and it is important to understand how to bridge and mitigate them.

The CISO can be involved in a wide spectrum of responsibilities depending on the organization's size and/or the lens the executive team looks through for digital security.Certain macrotrends in security organizations have become prevalent during the past five to six years. The main trend has been a tendency to establish a corporate information security function outside of the IT organization (see Figure 1).

2. TO WHOM SHOULD THE CISO REPORT?

To define the role and the location of the CISO in an organization, the organization itself, the type of services and/or products it provides, its relationships with other businesses, the geographic reach of the organization, required laws and regulations with which it must comply, the aspiration of the enterprise, and its future outlook all must be understood. There are a number of unsettled arguments among senior management teams about who ought to own the digital security functions and how to justify the CISO position and roles within an organization.

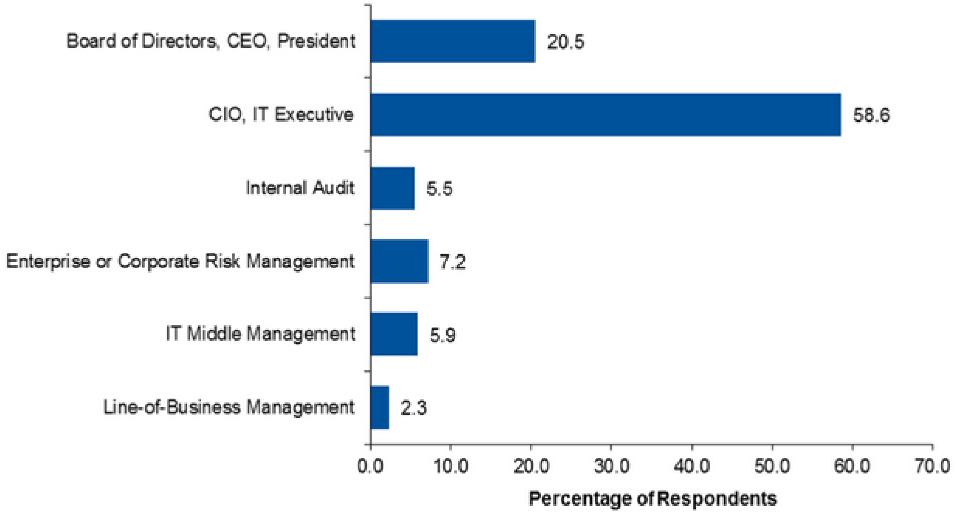

Figure 1: Reporting Line of the Most-Senior-Level Person Dedicated Exclusively to Information Security (Gartner 2014)

The following are a few of the argued and debated subjects within the digital security world:

- The hurdle of justifying the CISO position—The number of issues the enterprise faced would establish some of the foundations in support of instituting a CISO position and the formation of the digital security organization. Any one or combination of these issues could justify the institution of the CISO position, and some of those are internal and external security breaches, monetary losses as a consequence of security incidents, compliance with the country's laws and regulations, protecting the organization's reputation, risk appetite, and several other circumstances.
- Reporting structure—Organizations are debating the appropriate position of the CISO in the organization chart. Among the points to consider is whether the CISO should report to the:
    - Chief information officer (CIO)? Answer: It depends. Digital security was born and advanced out of information systems and technology disciplines. CISOs may argue that information systems and technology groups are the implementers of the technology and systems controls. However, this may represent a segregation of duty (SoD) conflict if the governance and reporting on the effectiveness of IT controls are combined under one entity.
    - Chief executive officer (CEO) of the organization? Answer: Most probably yes. For a mature, complicated and multinational corporation, the CISO position is much better suited to report to the CEO of the organization, where the digital security programs are designed to support the enterprise's business objectives in a top-down approach.
- CISO and unresolved digital security structure—Different assemblies within an organization may argue for or against any of the preceding CISO reporting structures. Motives and politics are part of human nature; different factions within an organization may present several arguable reasons and rationales for various CISO reporting structures.

3. ANALYSIS

Several researches or surveys have been made worldwide. In one security survey conducted by ThreatTrack Security, it was found that out of 203 U.S.-based, C-level executives interviewed, 47 % of CISO's reported to their CEO, 45 % reported to CIO and at least of 8 % reported to positions such as the COO, CRO, CFO or CCO. Another research conducted by PwC in 2014 called "Global state of information security" has questioned over 9000 respondents from around the globe. They answered myriad of questions about cybersecurity. The survey found that in organizations with CISO to CIO reporting structure, there was 14 % more system downtime and financial losses were 46 % higher than in organizations with the CISO to CEO reporting structure.

Realize the Potential Advantages of Having the Strategic Security Leadership

Report Outside of IT

This structure is largely dependent on the maturity of the underlying security processes, with higher maturity making it easier to develop practical responsible, accountable, consulted and informed (RACI) charts. It also requires some experience in a matrixed/collaborative working environment, allowing more flexibility in developing new working relationships.

The potential advantages are:

- It enhances the profile, influence and authority of the information security role.
- This enhanced profile improves the ability to coordinate and standardize key security processes (for example, risk assessment) and principles (such as risk tolerance driving controls selection) across the enterprise. This is especially relevant in decentralized, federated organizations.
- It helps to break the perception in the mindset of the business that "security is an IT problem."
- It positions the CISO to take a more significant and broader role in cybersecurity practices that may include industrial automation and control, as well as physical security responsibilities.
- It enhances the separation of oversight of security compliance (for example, firewall policy) from operational execution (firewall rules maintenance). This segregation of duties is desirable in heavily regulated industries.
- It improves the relationship between security leaders and business leaders through better insight into existing and new business security risks, as well as improved information exchange. This results in more appropriate (from a business perspective) decisions by the CISO.
- It potentially makes it easier to monitor security compliance in enterprises that are establishing sizable shadow IT capabilities outside of IT by avoiding some of the political problems that has been created with the IT organization.

Consider the Potential Disadvantages of Having the Strategic Security Leadership

Report Outside of IT

The potential disadvantages are:

- It raises conflict between the security leader and IT (including the "retained" IT security functions) regarding accountability, ownership and responsibility for various security functions (who owns what).
- It makes aligning IT and information security work activities more difficult.
- The external security function can lose influence and authority within the IT organization.
- It increases the workload of the CISO's management team and draws the team into new and unfamiliar decisions.

Recognize the Potential Advantages of Having the Strategic Security Leadership

Within IT

The potential advantages are:

- Proximity to the IT infrastructure, where most, if not all, information is manifested at some stage of its life cycle.
- Proximity to the constantly changing technology environment and threat landscape.
- Closer alignment and working relationships between strategic, tactical and operational security functions.

Understand the Potential Disadvantages of Having the Strategic Security

Leadership Within IT

The potential disadvantages are:

- It inhibits the CISO's understanding of business processes, which impedes the security leadership's ability to focus on business-centric security projects.
- The security staff retains a technology-centric perspective and language, hampering communication and relationships with the rest of the business.
- It reinforces the perception that security is a back-office function as well as an IT problem.
- It risks lack of authority and influence outside of the IT organization.
- There is a potential conflict of interest between the CISO and CIO when the CIO accepts too much risk on behalf of the IT organization.

4. CONCLUSION

There are a number of reasons why the subject of the CISO roles and responsibilities is becoming an interesting issue within enterprises. The increase in data breaches, the ramifications of breaches, the compliance dictated by regulations, the multinational aspects of information traveling across borders, emerging information technology architecture and services, and the external auditor demand for attestation all have elevated the CISO position to be a topic of discussion among the BoD and senior executives. The importance of SoD highlights the fact that the CISO should neither be part of the IT organization structure nor report to the CIO.

Since the CISO position is being promoted to report higher in the organization chart, a greater emphasis is being placed on the CISO role and expected skill level of those filling the role. It has moved the skill of the CISO from technical implementer of technology to one of business focus and the ability to oversee digital security as a vital business unit to justify its relevance and demonstrate the ROI to the enterprise bottom line.

Additionally, enterprises are evolving to become risk-based organizations. This requires transformation of the enterprise culture to a risk-based culture, where digital security is the responsibility of all the employees of the enterprise.

However, such cultural transformation has put greater pressure on the CISO to be a trusted advisor who operates as the integrator of the enterprise business units and a relationship builder. Digital security is becoming the bridge to integrate the enterprise products and services with the enterprise business functions.

ACKNOWLEDGEMENT

This publication was realized with support of the Operational Programme Integrated Infrastructure in frame of the project: Intelligent systems for UAV real-time operation and data processing, code ITMS2014+: 313011V422 and co-financed by the Europen Regional Development Found.

REFERENCES

[1] Boney*Hayslip*Stamper, 2016. CISO desk reference guide. A practical guide for CISOs. Joint Venture Publishing, ISBN 978-0-9977441-1-8

[2] Tom Scholz, 2020. Determining whether the CISO should report outside of IT. Gartner, ID G00263700

[3] Robert Putrus, 2019. The role of the CISO and the Digital security landscape. ISACA Journal 2019

[4] Bethany Deeds, 2019. Who should to the CISO report to? It depends. ISACA now blog 2019.

[5] Mike Loginov, 2018. CISO Defenders of the Cyber Realm: Dirty Deeds, Hackers & Heroes. CreateSpace Independent Publishing Platform 2018

[6] Todd Fitzgerald, 2008. CISO Leadership: Essential Principles for Success. Auerbach Publications; 1st edition 2008

[7] Scott Ellis,2016. The CSO Guide: The Chief Information Security Officer (CISO) Handbook. Independently published (22 Nov. 2016), ISBN 978-1519090348

Jaroslav REMEN, Ing.
Milan KUBINA, prof. Ing., PhD.
Department of Management Theories, Faculty of Management Science and Informatics, University of Zilina
Univerzitná 8215/1, 010 26 Zilina, Slovak Republic
e-mail: jaroslav.remen@gmail.com, milan.kubina@fri.uniza.sk