Internal Audit Role in Cybersecurity

Carataș Maria Alina
"Andrei Saguna" University of Constanta
maria.caratas@gmail.com
Spătariu Elena Cerasela
Gheorghiu Gabriela
"Ovidius" University of Constanta
ebarbu2001@yahoo.com
gabrielag3110@gmail.com

Abstract

In a changing world, with a massive exposure to risks on all levels, from nature climate change to violent cyber war attempts, the business environment needs to adapt its instruments in mitigating and responding to cyber-security risks on different stages: prevention, detection, disposal, improvement.

Internal audit function has a key role in assessing cyber disruptions as part of strategic risks and identifying the operational control gaps on the business level, working with management at developing and maintaining an adaptive capacity to different types of risks building and improving business continuity.

Key words: cyber security, internal audit, cyber attacks, business continuity, cyber resilience
J.E.L. classification: F60, K24, M42, M48, O33.

1. Introduction

Technology surrounds us in every field and the risks on security got into a broader level. Therefore, apart from the existing risk exposure to global warming, nuclear war, political changes, terrorism, regulation changes, loss of well-prepared employees an important trigger consists in the cyber threats and security incidents.

Most of the big organizations have strong security protocols implemented to fulfil the cyber-security politics, like the three levels security, tunnel secure shell (SSH), telecom protocols, etc. This helps organizations develop appropriate tactics to determine how they can achieve continuity and recovery in the event of a data breach.

2. Current risk exposure

Deloitte (2015) conducted a study and the highest risks that can arise in a company disrupting the normal business are:

- cyber attacks, in terms of malware, denial of service, phishing,
- data breach (information theft, identity stealing, reputational damage, private/secure information public release)
- unplanned IT and telecom outages
- security incidents

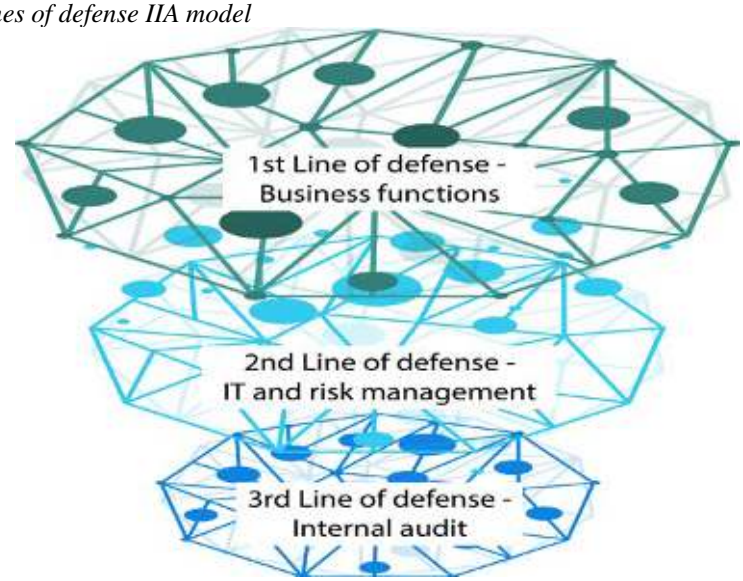
According to Business Continuity Institute (2017), Horizon Scan Survey, top three challenges in cyber-security are the use of the internet for malicious attacks, the influence of social media, and on third place, the loss of the key employees.

2. Three lines of defense model

Forwards, we'll present the IIA three lines of defense model and we will explain how a business can fight against the cyber security risks

Deloitte adapts the Institute of Internal Auditors *Three lines of defense model* with a view to cyber risks, as it follows:

Figure no.1 Three lines of defense IIA model



Source: Authors visual projection the IIA model

The first line of defense: Management control is the responsibility of the operational management, ensuring the identification and control of operational risks on the business processes level. There are three functions on this level:

- Owning and managing risks
- Anticipating risks
- Ensuring independence and security

Teamwork with IT department on cyber risks security and reaction. Internal audit will assure the effectiveness of the response actions on IT risk. On the first line of defense level, the business and IT function include cyber risk management in daily operations.

Promoting communication and collaboration using the extensive image that internal audit has it on the organization level.

The second line of defense is represented by:

- a risk management function and supervising the risk management and internal control system completed by the operational management; at this level, governance gets settled and also policies, standards, processes; eventual risky situations are reported to management;
- a conformity function providing consultation, verification, monitoring specific risks and reports to superior management and even on the governance structures;
- a financial control function supervising the financial risks and financial reporting problems. The independence on this level is limited.

The third line of defense is the internal audit function, which has higher independence, offering an objective opinion over the control carried by the operational management and the efficiency of the functions from the second line of defense.

The internal audit function reports to the executive management and governance responsibilities. Internal audit offers assurance over the risk management, internal controls, covering a large area of objectives. The result of the evaluation is further presented to top

management, to the Audit Committee and to the Board of Directors. Also, other stakeholders are interested in the evaluations of the internal audit, such as regulating authorities and the external auditor.

3. What should internal audit do in a proactive defense?

The Institute of Internal Auditor's CEO, Mr Chambers presented in several steps the role of internal audit in cyber security.

- He admits one of the roles of internal audit function is testing and providing assurances on the cybersecurity and the planning on business continuity and recovery strategies from different threats.
- Efficient communication between internal audit and executive management is essential to the cyber-security risks levels at the organization level and countervail or mitigate them.

Protect

- First of all, internal audit may provide help with developing adequate, IT governance program, including cybersecurity strategy and policy working together with the board of directors and management. Internal audit can also offer assurance on the IT governance.
- Furthermore, it needs to point out and evaluate the cybersecurity risks, assesses the tests and their effectiveness and works on diminishing them to a minimum by offering analysis reports and judgments on the execution plan.
- Getting the awareness that risks may occur both from outside and inside of the company, the internal audit function will carefully assess cybersecurity plans and work on mitigating risks.

Detect

- The internal audit needs to evaluate cyber risks, cybersecurity controls and inform the executive management and the Audit Committee about the vulnerabilities, threats, and effectiveness of the installed procedures and control systems solutions.
- The cybersecurity measures should be integrated into the internal audit plan. Also, the implemented organizational culture should support and encourage the cybersecurity endeavors.
- Should work on prevention in terms of cybersecurity, using sophisticated security and protocols, technology, and trained human resources. The internal audit can be externalized for an improved technical oriented audit aimed to widen the control over the cyber risks.
- With the use of data analysis and data mining IT security issues might be detected. Integrating data analysis in internal audit work leads to better risk monitoring and a wider control and fraud detection.

Business continuity

- Implementing a response program for cyber risks and a business continuity programme as a priority, in order to achieve cyber resilience.
- Cyber resilience can be a solution for the future, as cybersecurity without having implemented a business continuity program will not decrease too much the occurring risks.
- Companies need to pay greater importance and develop their own business continuity management (BCM) blueprint, by creating procedures on dealing and resolving different scenarios that might interrupt normal business activity, both on IT and physical security threats level.
- Business continuity brings value in organizations, as the existing risks tend to expand. Ex: terrorism, political moves, cybercrime, economic instability, climate change.
- It is a great strength for business to be able to foresight the darkest events that may occur and plan a strategy for managing to get out of it and continue their activity without being disrupted.

React

- Companies need to prepare a crisis management program, part of the BCM in case of incidence. The first important step is assessing the breach and finds a way to respond it. The entire organization needs to be aware of the crisis management program (so everybody in the company should be trained so they know their specific role in case of an incident), working in cohesiveness, so communication will be in a single voice and transparent.
- Internal audit will independently act in surveillance and assess the response.

Improve

- The internal audit function adds value to the business by expressing its opinions from the extensive activity.
- Security procedures, protocols, and strategies need to get continuous revising and improvements, to be always prepared for eventual attacks.

4. Conclusions

Organizations can create cyber resilience plans for their businesses, following the presented model protect – detect – business continuity, react – improve/re-evaluate.

Companies need to introduce in their organizational culture the cyber defensive behaviour and train the employees' rules of conduct and the internal audit will assess the conformity.

They should take advantage of the existing standards and framework on improving infrastructure on cybersecurity and adapt their policies and strategies accordingly.

Using a continuous monitoring program for cyber risks, as they are dynamic and prevalent; internal audit function should work aside from the IT in getting recurring updates and amendments on strategy cybersecurity program. This will lead to a change in internal audit function, in terms of expertness, talent, and leadership.

In case of risk emergence, a crisis management program, part of a business continuity management is fundamental. The first step will be discovering the reason for the attack and a way of response, and then ensuring a transparent and comprehensive communication, so every employee would know his role and responsibilities. Specific procedures (adopting ISO 22301 organization security - BCM) and defensive systems should be carried on an internal audit will assess the responsiveness and effectiveness of the strategies for future improvement opinions. A global collaboration and support between internal audit, executive management, IT and every single player in the company will lead to cyber resilience and greater protection on all level risks.

5. References

- Alcantara P., Riglietti G., 2017, *Horizon Scan Report 2017,* [online]. Business Continuity Institute, Available at: https://www.bsigroup.com/LocalFiles/en-AE/BCI%20Horizon%20Scan%20report%202017/BCI-BSI-Horizon-Scan-%20Business-%20Continuity.pdf [Accessed November 2017]
- Chambers R., The Institute of Internal Auditors, 2017, *Internal Audit's Critical Role in Cybersecurity*, Available at: https://www.accountingweb.com/aa/auditing/internal-audits-critical-role-in-cybersecurity [Accessed November 2017]
- MetricStream, 2017, *Top eight priorities for cyber security and BCM Leaders in 2017,* https://www.metricstream.com/
- Pundmann S., Doctor P., Adams S., White N., Deloitte Development LLC., 2016, *Internal audit insights High - impact areas of focus 2017*, Available at: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-internal-audit-insights-high-impact-focus-areas.pdf [Accessed November 2017]
- Pundmann S., Young C., Juergens M., 2015, Deloitte Development LLC., *Cybersecurity - The role of Internal Audit*, Available at: https://www2.deloitte.com/us/en.html [Accessed November 2017]