HOW TO INCREASE THE INFORMATION ASSURANCE IN THE INFORMATION AGE

LTC Artur SOSIN*

*Ministry of Defence/Republic of Moldova

The competitive world we live in today is characterized by an environment where the advancement of technology has increased the number of complex vulnerabilities and sophisticated attacks. Organizations around the globe are facing now the same challenges of implementing data protection and securing information assurance. The purpose of this paper is to prove that Information Assurance has become one of the most important tools in creating and maintaining a competitive advantage in today's competitive and global marketplace. This paper also presents the relationship between information assurance and cybersecurity, and their connection with confidentiality, integrity, availability (CIA) triad. Furthermore, assuring information and providing security is a life cycle process which needs a comprehensive understanding, skills, and experience in order to protect today's risk management challenges. The author concludes the paper with the importance of information assurance policies which are the fundamental guidelines for protecting information assets and fulfilling information assurance objectives of an organization.

Key words: *Information Assurance, Cybersecurity, Confidentiality, Integrity, Availability, Risk Management, Policies.*

1. INTRODUCTION

The competitive world we live in today is characterized by an environment where the information is progressively interconnected and at the same time more independent. Globalization has become part of every domain in which the world operates such as economic, social, and technological infrastructure. Behind the globalization is the transformation of information technology which has become an important part of an organization's global business strategy. Today's interconnected world is full of uncertainty which allows transferring the information across the borders through cyberspace.

At this moment, we are in a phase of transition, a world which is moving from the Industrial Age to the Information Age. In other words, we are changing from 3D hyper-integration technology architecture such as future technology research in computer, nanotech and biotech to a 3C (connected, contested and complex) hyper world. Unfortunately, today's sophisticated environment and electronic war give us less expected and more unexpected.

In short, the transformation from industrial to information is a test for all of us, and even if we pass it, this does not mean that we have been well prepared. This is the reason why, nowadays, people are more concerned about new threats such as data security and information assurance. It is difficult sometimes to make a distinction between information security and information assurance.

2. INFORMATION ASSURANCE CONCEPTS AND PRINCIPLES

2.1. What is Information Assurance?

Information assurance has many definitions or interpretations. According to Department of Defense Information Assurance Certification and Accreditation Program (DIACAP) *Information Assurance* is defined as "measures that protect and defend information and information systems by

ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." [1] Information Assurance Handbook has the following definition; "*Information Assurance* is the overarching approach for identifying, understanding, and managing risk through an organization's use of information and information systems." [2]. The Maconachy-Schou-Ragsdale (MSR) model of information assurance characterized three states of information (storage, transmission, and processing); three essential countermeasures (technology, policy, and people); and five basic services (availability, integrity, authentication, confidentiality, and nonrepudiation), as shown in **Fig. 1**. [3]

According to these definitions, information assurance has a much broader view than only secure the information because encompasses all the components of information security under the integration of protection information based on confidentiality, integrity, availability, non-repudiation, and authentication which are the five main components of information assurance. Furthermore, information assurance includes all information an organization can transmit, store, and process.

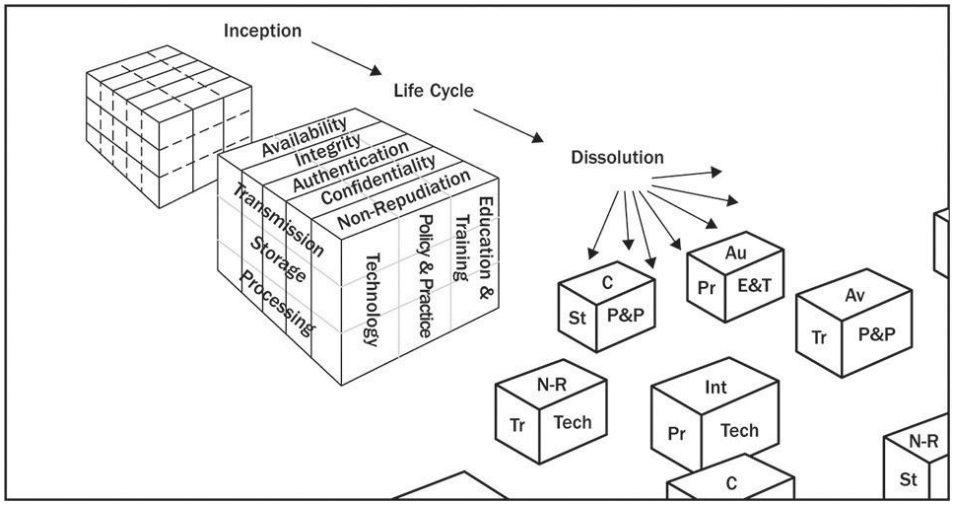

Fig.1 MSR Model

2.2. Information Assurance and Subdomains

In addition, there are three main subdomains of information assurance; information security, information protection, and cybersecurity. Information security is a subdomain of information assurance and focuses on the CIA triad: confidentiality, integrity, and availability, as shown in **Fig. 2.**

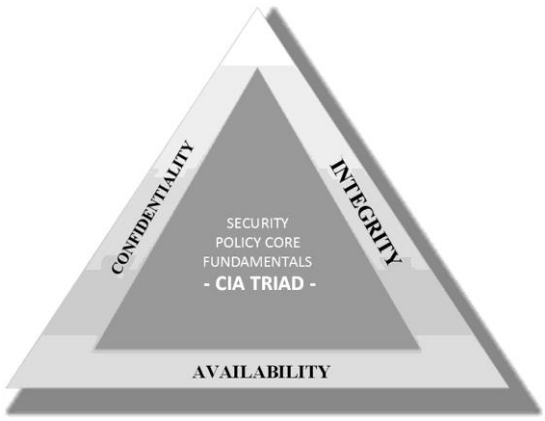

Fig.2 CIA Triad

In the same context, information security is responsible for all information an organization is storing and transmitting, electronic or paper format. As information assurance, information security is responsible for both domains: information protection and cybersecurity. Information protection has the role of protecting the integrity and confidentiality of information by using a diversity of means such as monitoring information classification, information categorization, and all the strategies. [4] Moreover, from other point of view, information protection has to be in charge of sensitive information such as personal information and information related to person's health.

For example, Central Intelligence Agency (CIA) of the United States is focusing on this "triad" when it needs to put into place a new security control policy into computer environment. [5] This triad facilitate the understanding of Information Technology (IT) Governance to ensure the efficiency and effectiveness of information technology in making possible that the organizations achieve their goals and produce measurable results toward accomplishing their strategies. The Figure 2 shows how CIA is represented by these three pylons that are the security policy core fundamentals.

Every component has its own significance, because an organization cannot achieve success if one of these is not fully integrated. Confidentiality is very important nowadays because it is very easy for hackers to obtain private data and information such as birth date, social security number, and other types of data if there is no encryption of information. This is why only authorized people who have the equivalent level of secrecy must have access to folders, and permission to access this type of information.

Furthermore, in order to protect data and information every organization has to have all the information about the administrators who are in charge of their security control and must be monitored also. Information must always be accessed by the correct users in order to be secure. However, even if the information is well secured but there is no authenticity that can create another problem.

Another fundamental component of information security is integrity. It is about making sure that data has not been modified or changed. Authentication comes with "trust" because it is very important to trust the person with whom you are interacting with. In other words, only by joining together integrity and authentication we will get to the level of authenticity. For example, if a database follows rules such data integrity, the database will increase performance, stability, accuracy, and will not allow entering data in an incorrect format in database.

The last part of the triangle is availability. This part describes the restriction and limitation of using data, and the access to the device must be available only with the given permission by the authorized administrators. The access to the information must be restricted, or available only with the permission and approval of the authorized people. These attacks can easily damage the whole system by shutting down the system. This is why security policies must be put into place in order to remediate these unwanted attacks before the event happens to help keep information safe and secure.

2.3. Information Assurance and Cybersecurity

The twenty-first century has become an interconnected corporate IT system for managing and distributed computing which provided the possibility to work from anywhere around the globe, and has created a

new era of vulnerabilities. [6] This is the reason why cyber crimes cannot be controlled and the cyber risk is the newest indicator of an out of control world. [7] Despite the fact that big companies around the globe spend every year millions of dollars in order to secure their information assurance, the next generation of cyber risk has the potential to have a negative impact on their data base and network systems. The main goal of cybersecurity is to protect electronic information systems and networks from being attacked by threats and vulnerabilities. Organizations start paying more attention to cybersecurity domain because both public and private sectors are not sufficiently protected against sophisticated attacks, and they need to develop defensive actions in order to be ready to secure the information.

The efficiency and effectiveness of cybersecurity requires that governments, private companies and non-governmental organizations must concentrate their efforts to understand the threats from a common point of view and to share the information and resources in order to mitigate them. [8] As our world is more interconnected at the same time is more insecure. Cyber domain is an environment where there are many actors involved that may affect the security network at the national and international level. Numerous companies have been victims of cybercrime, by losing their integrity and confidentiality. It is very important for the companies to assure themselves that only the right and authorized individuals have access to data and information, otherwise the information will not be secured. [9] For example, in the healthcare scenario, the doctor who sends the information to the laboratory needs to be sure that the orders can be read only by technicians in order to perform the test, and should not be accessed by the receptionist. [10]

For this reason information assurance becomes one of the most important issues and must be encrypted before transmission from end-to-end. Today anyone can start a computer and can access all the files from the hard drive. Furthermore, after gaining access many attackers will try to escalate the system in order to become the administrator of the computer. For example, in September 2014 Home Depot was one of the targets of such an attack which give the attackers the advantage to discover ~~of~~ 53 million customer e-mail addresses, and also 56 million credit cards accounts. [11] This is another example that shows the importance of information assurance, and what happens when the attackers break the network system of an organization only by compromising the username and password. There are many areas the companies have to focus on when they speak in terms of protecting confidentiality, but not all the time they succeed on doing so.

Today, many organizations do not want to pay attention to cyber threats or often they try to neglect the area of information security without investment in this domain. These situations bring to the conclusion that big companies spend a colossal amount of money to this domain. Cybersecurity is an area where nations need to continuously take actions in order to raise the level of information security, and to sustain their competitiveness on the business global market. Figure 3 illustrates the connection between information assurance and its relationship with subdomains such as information security, information protection, cybersecurity, and their relationship with confidentiality, integrity, availability, authentication, and nonrepudiation. [12]

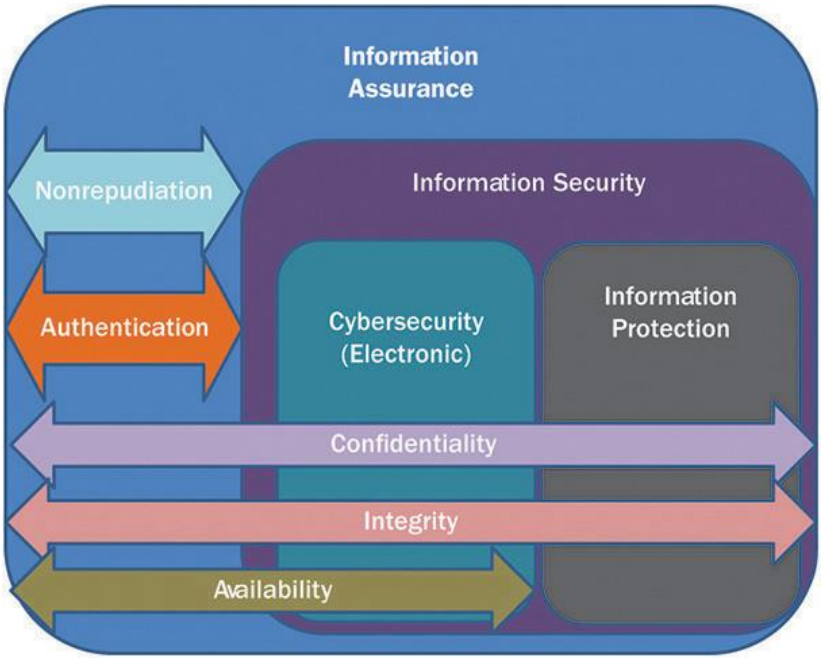

Fig. 3 Information assurance and subdomains

3. INFORMATION ASSURANCE RISK MANAGEMENT

3.1. Risk Management Concept

For an organization's management is very hard to be successful without implementing a risk management strategy for defending the risks. A well-executed management plan can reduce risk and increase economic efficiency. However, organizations must identify risk in order to manage it. The objective of risk management is to identify, analyze, evaluate, and continue to progress ~~it~~ every day. In addition, risk management is a whole process that includes policies, theories, and practices for identifying, managing, and controlling risk actions. Companies must take into consideration that ignoring the risk may cause unwanted outcomes. For this reason is important for organizations to have a good management risk practices in order to be ready and prepared for unwanted surprises.

Information assurance risk management is very important for an organization in order to face uncertainty, which can be one of two: a risk or an opportunity. This is a challenge for many organizations because they have to decide how much ~~it~~ they can accept in order not to fail to manage the risk. One of the areas which can bring success to an organization is the integration of protection of the infrastructure of communication technology by requiring identification, authentication and ensure the continuity of the companies by mitigating the risk management. [13] The risk management is a key element in the organization's information security program and contributes to the organization with the most effective framework for selecting the appropriate measures for an information system in order to secure and protect individuals and assets of the organization. [14] One of the most important functions of risk management is to select protective measures to guarantee the ability of the organization to fulfill its mission. [15] A holistic approach must be integrated for protecting an information system. Furthermore, it is important to know the most vulnerable parts that should be protected and the security measures which must be taken. Nevertheless, for security is not enough to have techniques and skills because the most critical point in any information system are the human beings. [16] To have the entire framework of security network we must take into consideration both

technical and human factors. Moreover, as the technological and societal backgrounds are progressively evolving, threats also transform and evolve.

The information system has a strong connection with threats and has to be both monitored and managed at the same time. There are many definitions related to risk. One of the most recent provided by the International Organization for Standardization is "the effect on uncertainty on objectives." [17] The older definition is "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization." [18] As we can see both definitions have something in common, because the effect on uncertainty means the terms *threat*, *vulnerability*, and *asset* can produce harm to an organization by challenging its way of operating, and damaging the resources that maintain the value of the organization and its mission. Research has shown that in theory information security risk is easy to calculate by using different types of formula. In contrast, reality has shown that, in order to measure the risk within an organization it is necessary not only to take into consideration a combination of theoretical measures but also an organization must be prepared for unknown situations by adopting the best practices.

Another way of measuring risk is by adopting fundamental principles, analyzing and evaluating the factors that are connected to the event, particularly the threats and the vulnerabilities. In addition, risk can be reduced by applying security measures that are translate from a methodology. A methodology that should include a security approach defined by effectiveness and efficiency applicable to directives, executive orders, policies, standards and regulations. [19] These documents must be part of Risk Management Framework, in order to make an information security program more effective, and organizations need not to apply only to the enterprise architecture but also to the new information system within the context of the system development life cycle. [20]

4. Risk Management Process

Risk management consists of many processes that are related to the information security. There is no a single process which can be used by every organization because every organization applies its unique process. Organizations should choose their management methods or approaches that are more relevant to their environment where business is taken place. Risk management process should have a continuous cycle and this cycle have to be always monitored, as shown in **Fig. 4.** [21]

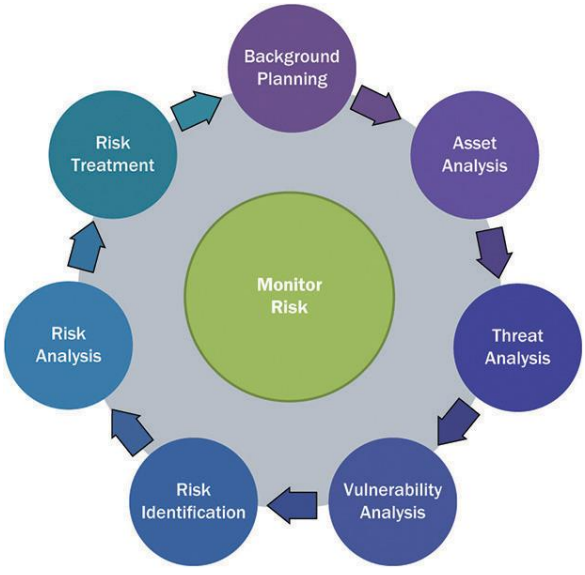

Fig. 4 Risk management process

The three main processes that risk management is focused on are: risk assessment, risk mitigation and evaluation and assessment, as shown in **Fig. 5.** [22]

Fig. 5 Risk management components

It is a very complicated course of action for an organization to be able to evaluate the impact of the risk on the business information process without having risk evaluation criteria. The criteria should indicate both: the level of damage caused by an information event and the estimate cost for eliminating it. Research has shown that there are no organizations in the world that are completely secure and do not acknowledge risk acceptance. Every organization must have a strategy that should include the goals and objectives related to developing risk acceptance criteria such as business criteria, finance aspects, and social and humanitarian aspects.

First and foremost, in order to assess the risk within an organization, it is imperative to define the scope and make sure that all the measures are taken into consideration ensuring risk assessment. Furthermore, the scope is not the only factor that should be taken into account when we want to assess the risk, because we have to be aware of limitations and constrains. By identifying the boundaries, organizations might figure the risks arise inside these boundaries. Only after identifying the scope and boundaries, the organization needs to analyze its whole approach to risk management such as strategic objectives, strategies, and information security policy. As abovementioned, every organization needs to identify its limitations and constrains. Risk analysis should be done from both perspectives: quantitatively and qualitatively. Both types of analyses must have the same common goal to analyze the risk in order to obtain a general scale of the risk level, and most importantly to consider the major risks identified. The risk evaluation process includes a complex risk assessment in order to make decisions for the next actions, and prioritize risks in accordance with risk evaluation criteria. Taking into consideration that risk management is an ongoing and never-ending process, maintenance of security measures should be planned and permanently performed on a regular scheduled basis. [23]

The implementation of security measures must be done by the organization in order to organize and develop risk assessment exercises within the organization by involving all the factors that have a connection with risk such as new types of business objectives and functions, and we must follow how effectively and efficiently are put into practice the security measures to respond to the new more sophisticated threats or vulnerabilities. Only after all the necessary adjustments and transformations had been taken into consideration, the risk might be reevaluated and security measures could be identified.

Risk assessment is the first phase of risk management process and includes all organizational resources such as information, people, processes and technologies. In addition, based on these resources an organization can make an estimation of the value they add in achieving the organization mission, estimating the vulnerabilities that have a direct impact on the resources, and assessing the likelihood or probability that each threat will have a connection with an equivalent vulnerability. [24]

From a practical point of view, a risk matrix approach is the best option for an organization to measure its risk because shows both the likelihood and the impact of a risk event happening. This graph demonstrates that even though the risk is not completely eliminated, it can be partially reduced, as shown in **Fig. 6**. [25] The highest risk is the more sophisticated one and requires more resources and time. In contrast, the medium and low risks need less effort and can be fully eliminated. However, all the organizations must keep in mind to be responsive to all types of risks, and they have to daily monitor and periodically review them to make sure that organizations are secure.

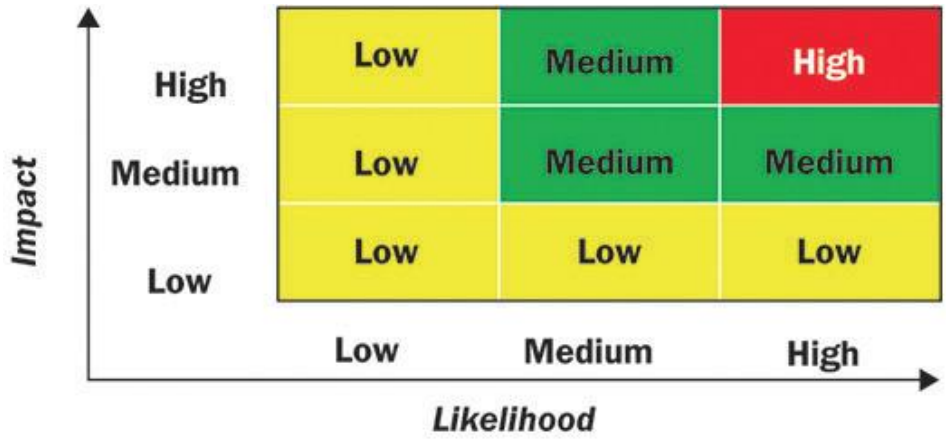

Fig. 6 Example of risk level matrix

5. INFORMATION ASSURANCE POLICIES

5.1. Security Policies and Plans Development

Information assurance policy is unquestionably the essential element for any successful organizations and without having these policies it is very hard for an organization to operate properly. Every organization must have a comprehensive information assurance documents that guarantee their security policies against potential threats. Today, there are no organizations in the world who can assure their information without a strong secure policy and security plans and methodologies that must be used in contemporary assessment and information technology infrastructure. For example, in order to build a resistant and solid house we need a strong foundation at the base, because without having this house might be destroyed at the first big flood. The same analogy we can use for an organization. For this reason it is imperative for any organization to have a security policy implementation foundation to be put in place and to have well-organized senior management support, as shown in **Fig. 7**. [26]

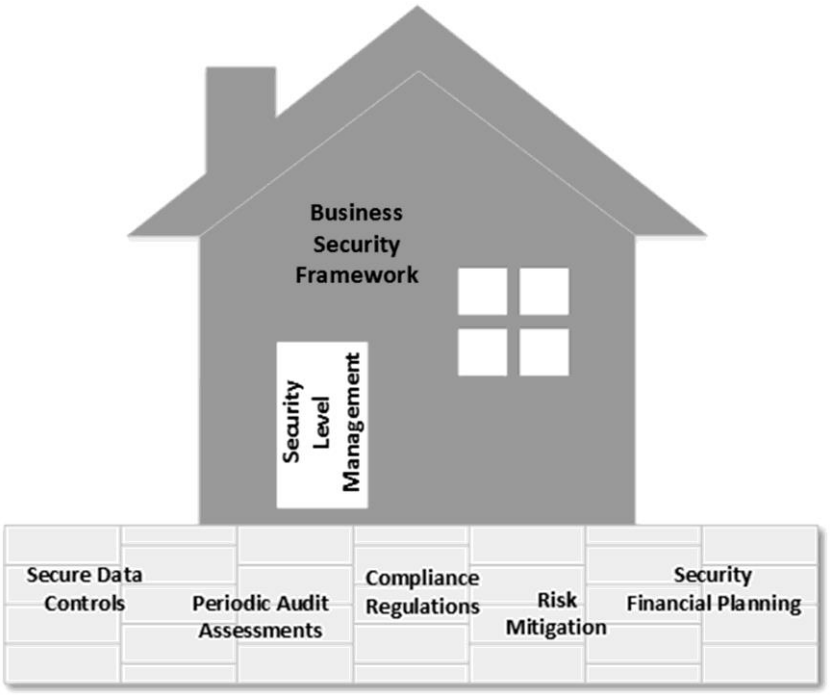

Fig. 7 Business security framework

By using this analogy, every organization can spend less time and resources for identifying solutions without reinventing something when events will happen. Another secure example that could be used by an organization is called "BRICK" that also emphasizes the biggest challenges that most of the organizations have to regularly work on, in order to keep protecting their security environment by defending confidential data and information as renewed as possible, as shown in **Fig. 8.** [27] Nowadays, in the field of computing is almost impossible to control the storage and the use of information due to innovative cybercriminals who are taking advantage of security gaps that are present in the unprepared organizations.

Cybersecurity strategist Matthew Gardiner pointed out very well saying that "the sophisticated hacker of today is not so much a hacker by trade but more entrepreneurial" and "They are leaders on the bad side of the economy, but they have the same skills that happen in the good side. They can assemble the people and processes needed to run a business." [27] This saying demonstrates that these types of criminals are more orientated toward money, and they can easily start a business because they have a technology background and this knowledge help them to assemble everything in order to run a business. Based on "BRICK" model, all five phases need to be fully integrated each other in order to ensure the life cycle for security policy and to correlate the policies with the needs that must be updated to help secure the environment and identify the measures that must be taken to accomplish the whole process.

Fig. 8 BRICK

5.2. Information Assurance Priciples and Strategy

The information assurance strategy should be a living document of every organization because its principles accomplish the necessities and objectives that organizations need in order to develop their long-term business plans. The most important principles that an organization must be based on are the following; comprehensive, independent, legal and regulatory requirements, living document long life span, customizable and pragmatic, risk-based approach, organizationally significant, strategic, tactical, and operational, concise well-structured, and extensible – see **Fig. 9**. [28] Each principle has its unique contribution to the grand information assurance strategy.

The future organization should have in place a non-classic model and more comprehensive type of strategy such as defence-in-depth strategy, which will cover all the management programs and domains.

Fig. 9 Information assurance strategy principles

The defence-in-depth strategy is not only an information assurance concept which uses the multiple countermeasures to protect the integrity of the information assets in an

organization but also offers the best practices taking into account the three main important elements for an organization such as people, technologies, and operations. The 19th century military strategist Helmuth von Moltke said that "No plan survives contact with the enemy." [29] We should not underestimate the enemy, because they know what is their strategy and how to react once engaged. The same concept hackers and attackers apply when they want to damage the software and network systems. Even though organizations have already developed plans, there is no guarantee that their information is secured. The defence-in-strategy is the most effective approach because is composed of numerous countermeasures that can be applied to various types of risks which have different level of complexity and rigidity. Furthermore, defense-in-depth offers the best tools for information assurance.

However, this type of defense must always be planned in advance because it has to be responsive to the most sophisticated attacks and unpredicted events. Former U.S. Defense Secretary Donald H. Rumsfeld stated very well by saying, "You go to war with the army you have, not the army you might want or wish to have at a later time." [30] There is no well-developed strategy in the world that can respond to unknown situations. However, having a strategy can minimize the impact of the risk. Organizations must take appropriate actions according with their laws and regulations to survive when sophisticated attacks are happening. An information assurance strategy is the essential pylon for protecting an organization.

6. CONCLUSION

Organizations and their resources are always under risk pressure, which create them a lot of problems in the areas where they are more vulnerable. Seniors and managers have to conduct a comprehensive risk assessment within organizations in order to evaluate their level of risk and to identify the most sensitive parts. The advanced technology has brought new types of risks that are more complex and sophisticated. In today's information age a country which is isolated from the rest of the world cannot survive alone. This is why it is necessary that all the countries combine their efforts and establish a common joint research to exchange experience in the field of technological training. In addition, organizations should increase the level of security and draft plans against cyber attacks. A globalized world makes the products to be developed outside the country. This development has invented a new "Open innovation" or "Open doors" which becomes more a new way of collaborate with other companies and a new imperative of competition in global markets, but lees a secure system and control access of integrity among competitors. [31]

It is very important for organizations to make *right* and *secure* decisions and to properly address enough methods for securing information assurance. However, in order to make right and secure decisions, organizations have to have a comprehensive approach, because cyber domain includes threats that are more sophisticated and dynamic. These complicated threats most of the time are created by individuals such as customers or competitors with extensive knowledge and who have the authorized permission. Organizations should maintain their level of information assurance by developing and implementing defensive policies that may keep their infrastructure technology secure. If companies do not take measures against threats today, they will never have a greater chance of success in future cyber environment. There is no magic formula which can be applied in today's turbulent environment. Companies should be flexible and to adapt easily to this environment, meanwhile, to be strong, more efficient and more integrated with partners around the globe in order to secure their information and to remain operational. Nowadays, measures should be taken at the international level in order to share information according to some criteria which are accepted by private companies and non-governmental organizations. There is no country in the world that can defend alone against cyber threats. For this reason, the internal network security cannot be effective

anymore, and it is necessary to have a common knowledge management and a defense approach at the international level. By adopting a set of defensive strategies, the management of information assurance will be increased, and organizations will be secured from being attacked. Organizations must have a comprehensive defense policy in order to ensure the protection of critical infrastructure of their security network. Not all the time the advanced measures can neutralize the unexpected risks. Organizations have to invent new solutions based on their evaluation criteria from the risk analysis perspective.

A secure organization is not only about equipment and antivirus programs. It is very important to understand that no program or combination of programs will make a secure organization by itself. Securing information assurance is an entire process which requires critical and innovation thinking, a lot of time, money, and application of new IT technology to maintain the organization operational. However, many organizations do not want to pay much attention to information assurance domain, or they do not want to spend much money on it, and as a result they end up with unwanted outcomes. This is why creating a secure infrastructure is compulsory for every organization at national or international level, because we never know when an organization might be under attacked by very sophisticated hackers.

ENDNOTES

[1] Department of Defence Directive, Information Assurance, October 24, 2002.
[2] Corey Schou, Steven Hernandez, *"Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"*, Published by McGraw-Hill Osborne Media, 2015, p.14.
[3] Ibid.
[4] Ibid.
[5] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017, p.567.
[6] Kewin Walby and Randy K. Lippert, *"Corporate Security in the 21st Century: Theory and Practice in International Perspective*", p.248.
[7] Ibid.
[8] Maria Manuela Cruz-Cunha, Irene Portela, *"Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance"*, Published by IGI Global, 2015, p.317.
[9] Glen Sagers, Bryan Hosack *"Information Technology Security Fundamentals"*, Business Expert Press, LLC, 2016.
[10] Glen Sagers, Bryan Hosack *"Information Technology Security Fundamentals"*, Business Expert Press, LLC, 2016.
[11] Glen Sagers, Bryan Hosack *"Information Technology Security Fundamentals"*, Business Expert Press, LLC, 2016.
[12] Corey Schou, Steven Hernandez, *"Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"*, Published by McGraw-Hill Osborne Media, 2015, p.16.
[13] Maria Manuela Cruz-Cunha, Irene Portela, *"Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance"*, Published by IGI Global, 2015, p.273.
[14] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017, p.497.
[15] Kenneth J. Knapp, *"Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions"* Published by IGI Global, April 2009, p.56.
[16] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017, p.3.
[17] Ibid p.508.
[18] Ibid.
[19] Ibid. p.511.
[20] Ibid. p.516.
[21] Corey Schou, Steven Hernandez, *"Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"*, Published by McGraw-Hill Osborne Media, 2015, p.57.
[22] Kenneth J. Knapp, *"Cyber Security and Global Information Assurance: Threat*

Analysis and Response Solutions" Published by IGI Global, April 2009, p.56.

[23] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017, p.515.

[24] Kenneth J. Knapp, *"Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions"* Published by IGI Global, April 2009, p.58.

[25] Corey Schou, Steven Hernandez, *"Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"*, Published by McGraw-Hill Osborne Media, 2015, p.119.

[26] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017, p.565.

[27] Ibid. p.566.

[28] Corey Schou, Steven Hernandez, *"Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"*, Published by McGraw-Hill Osborne Media, 2015, p.5.

[29] Ibid. p.25.

[30] Ibid.

[31] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017, p.5.

REFERENCES

[1] Department of Defence Directive, Information Assurance, October 24, 2002.

[2] Corey Schou, Steven Hernandez, *"Information Assurance Handbook: Effective Computer Security and Risk Management Strategies"*, Published by McGraw-Hill Osborne Media, 2015.

[3] John R. Vacca, *"Computer and Information Security Handbook, 3rd Edition"*, Library and Cataloging-in-Publishing Data, July 2017.

[4] Kewin Walby and Randy K. Lippert, *"Corporate Security in the 21st Century: Theory and Practice in International Perspective*".

[5] Maria Manuela Cruz-Cunha, Irene Portela, *"Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance"*, Published by IGI Global, 2015.

[6] Glen Sagers, Bryan Hosack *"Information Technology Security Fundamentals"*, Business Expert Press, LLC, 2016.

[7] Kenneth J. Knapp, *"Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions"* Published by IGI Global, April 2009.