Archives of Business Research – Vol.6, No.5
Publication Date: May. 25, 2018
DOI: 10.14738/abr.65.4657.
Nowduri, S. (2018). An Attempt to Understand Cyber Security Management Proces. *Archives of Business Research,* 6*(5),* 309-327.

An Attempt to Understand Cyber Security Management Process

Srinivas Nowduri Ph.D.
Department of Management, US Coast Guard Academy,
26 Mohegan Avenue, New London CT 06320

ABSTRACT

Modern businesses are still thriving to achieve to a security level opting for cybersecurity, in the form of a cybersecurity management process (CMP), is detail at three levels. The first level focuses on the architectural and components of this CMP. The second level details the comprehensive view, and finally presents systems and complexity view. This work also proposes a cybersecurity management model, along with some challenging issues.

Key Words: Cyber security management process (CMP), Cyber security management (CM), Risk management, Business intelligence (BI)

INTRODUCTION

The invention of computers and information system (IS), move the world in to a dynamic path, through an automation process, coupled with advancements in communication and networking. ISs were born as technology by products, slowly become integral parts of the business process; impacting the business budgets and finally become decision makers (through decision support systems (DSS)) for organizations, while guiding through profit paths. The influence of IS on businesses is not only through productivity/quality improvements but also make business unique; thus making them secured, becomes mandatory and challenge for modern businesses. A business progress was initially proportional to the number of products/service it has produced, now it is directly proportional to the number of secured IS it has. Thus, technology and its security, has become a driving force behind every successful organization.

At the same time, the design, development, implementation IS has become the bottle neck issue for modern corporate world from two different angels; maintenance and security. Businesses composed of several departments, with several ISs for each, starts communicate and exchange data/information every second online. Cybersecurity is all about securing organization's digital assets like: data, information, processes, ISs, databases and many more. Securing them through a specific cybersecurity management process (CMP) becomes a real challenge, realized to be a step much beyond information technology (IT) management. CMP is defined to be combination of technologies, practices and policies that address threats or vulnerabilities in network, computers, program and data [1][5]. These threats and vulnerabilities expected to flow from or enable by connection to digital infrastructure, information systems, or industrial control systems, including but not limited to, information. Securing organization wide digital assets becomes main agenda in both scientific and business organizations; to remain competitive and in improving the leadership qualities. Therefore for modern businesses, first managing IS's risk became the basis for corporate cybersecurity. Management being initially responsible for people, process and resources, has now took an additional component "cybersecurity".

Modern IS designers starts implementing authentication, authorization and nonrepudiation tools as the basic software to maintain their system's security with respect to confidentiality, integrity and availability. The seminal relationship among these six intra-dependent

components, (with respect to their functionality) entails the IS security. In every organization, technology being ubiquitous, being used by employee on a daily basis becomes an integral part of our society as well; throwing more light and need towards its security. Unfortunately, at the same time, it also given a huge scope for IS designers and cyber attackers alike. These cyberattacks, involves risk not only through external people but also due to few internal employees. Thus management has a moral responsibility in installing a CMP, to make business viable.

Risk management visualizes the scope of cybersecurity being the responsibility for everyone, within the organization, comprising of management, people and processes. Initially, the Information technology management (ITM) was a subject of interest to both academicians as well as industrialists in view of its different ways of managing IT resources, databases and their upgradation. Since it was not throwing enough light on the security aspects, IT departments cannot conduct proper risk management and mitigations on their own. In view of their vulnerability modern businesses start focus towards securing their digital asserts like data, ISs, processes and methodologies, leaving a huge scope for cybersecurity.

In the past several researchers viewed this cybersecurity management from different perspectives such as enterprise orientation [5] [9]. As a persistent management process, its ability lies in its adaptation continuously to a changing environment. This research throws light in establishing precautionary measure needed, against hacking or sabotage activities; without much emphasis towards establishing a CMP or its improvement. At the same time, risk management has been in lime light by several researchers for betterment through its framework and management. Aim of this research is based on historical information perspective [10] [11].

Hacking these days is multidimensional exists in different forms as well as shapes, emerged and grow as computing became easier. Managing cybersecurity through CMP has become a bottleneck issue. As a consistent process, CMP is expected to ensure not only secures all digital assets but also playing a role in organizational technology innovation. Unfortunately CMP cannot be made unique across all businesses, due to difference in input, process, output and functionalities. This research throws light on CMP and its different components/functionalities. CMP is analyzed from three different perspectives: (A) Business driver guidance towards different cybersecurity activities (as part of risk management and information assurance process) (B) Upgradation of technology and its needed support and (C) Technology awareness and education among the employees across the organization.

This research work is organized in the following way. First it presents an architectural and component view of CMP. It then describes the nature and scope of cybercrimes and rectification through CMP. Later it details cybersecurity management model as part of the organizational innovation process. Finally it concludes with four dimensions of CMP, and its associated challenging issues.

AN ARCHITECTURAL AND COMPONENT VIEW OF CMP

A management process is a unique process or methodology in producing, cost effective, quality products and services. Each division within organization, such as human resources, marketing, accounting, IT, have their own IS and processes. Cybersecurity is a way of securing all the business digital assets, managing these against their abuse, misuse and theft, is the responsibility of the management. It is realized that: An organizational cybersecurity is invariably interlinked and intertwined with all business ISs within. The by CMP is also

responsible for their periodical creating, updating and maintenance. A business organization being a non-linear combination of people from various capabilities and skills, with different academic and work experiences, involves a wide scope for several cultural and social issues. CMP is a unique combination of socio, technical, and economic issues, relating to people, processes and products.

Finally the cybersecurity is designated to be one among several management sub processes such as: Procurement, Transport, Warehouse management, Human resource, Marketing etc. Each of these department involves various ISs to function, in variably tied up with CMP, across the organization. All department ISs are interlinked and reports to top management through CMP, on a weekly/monthly basis. Thus cybersecurity management is precisely about securing, preventing, and correcting any threats to all its departmental digital assets, through CMP. The following section attempts to visualize a broad view of CSM based on its basic roles and functionalities; useful for both system designers as well as management people.

CMP as a Modern Business Driver

In this era, an organizational business is directly proportional to their processes and IS involved; giving more emphasis on prevailing technology and its dominance. Security for each of these IS and processes, is the responsibility of cybersecurity, is vital for today's market.

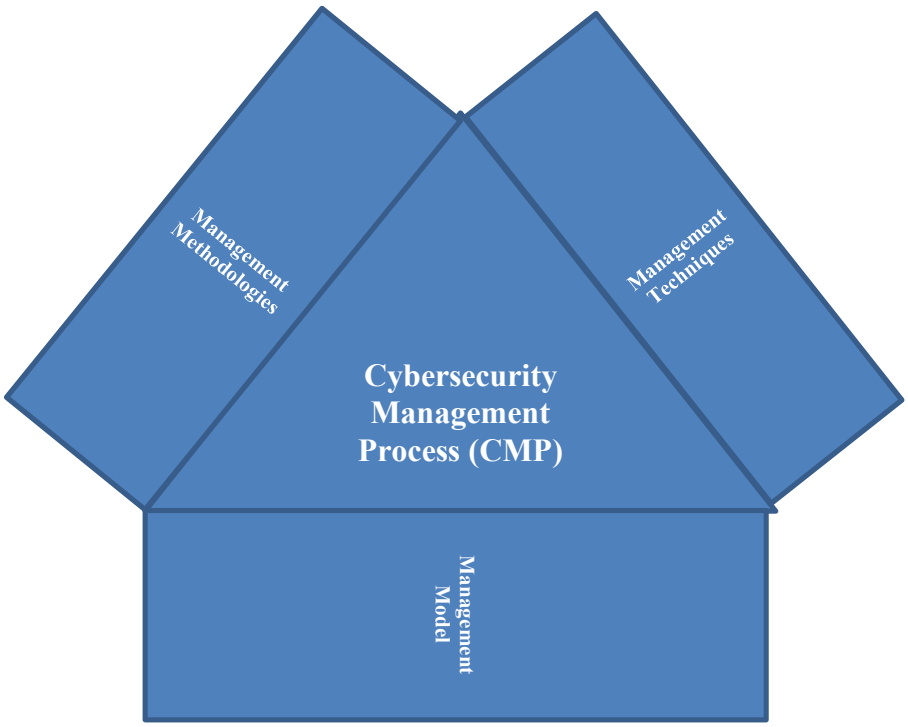

Figure 01: An Architectural View of CMP

As a real time software system and a kernel 24/7, CMP reports to management, for any possible digital thefts and any vulnerability issues across the organization. The architecture of CMP is based on three prominent pillars viz., Methodologies, Techniques and Management Model; each visualizes data or information in their own angel as shown above in Figure 01.

A. Management Methodologies: A management methodology is uniquely designed on its existing business processes and products. This methodology varies according to the nature of the business and processes involved, across the organization. CMP in particular encompasses many processes such as databases, networking, information management, which are all inter-twinned and tightly secured. From the cybersecurity perspective, these processes and products

function differently while processing, altering, and deleting digital information. Involvement of any external interference, during this automation process raises red flag. In fact, these methodologies are continuous, sometimes encrypted and more of information centric by default. Also these methodologies are applicable and exclusively designed around all organizational ISs; possibly for information sharing, intelligence gathering and surveillance. Therefore the security of these methodologies is of high priority task. Furthermore, the privacy of these methodologies and ISs also includes individuals if any, who access it. These methodologies of CMP are a continuous evolution of five primary steps as defined below in Figure 02.

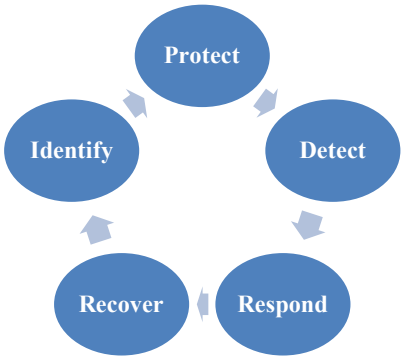

Figure 02: Evolution of CMP

Every methodology here has a unique hierarchical structure representing its business vision and goal.

A cyberattack or crime can be due to an internal employee or an external hacker; in either case, the management needs to "protect" cyberattacks called "information assurance". In the past two decades, this field is quickly developed establishing strict rules, policies and standards for the organizations and their employees' usage of any digital assets. Some employees inevitably override/undermine these policies and standards, giving scope for the second step, "detect". This necessitates management to look after, data loss or information leak or a post incident analysis. The fields exclusively dedicated for this step includes digital forensics, crime mapping, etc. A person is not a "suspect", until his/her crime is technically or procedurally established.

Completion of this step, leads to third step "respond", supported by fields like cyber laws, to retain, questioning and extract information from a suspect. This requires a set of respond team members, established procedures coupled with cyber legal procedures. One need more attention during the "recover" step, which is based on search and seizure techniques, involve court orders, without violating human/employee rights. During the final step "identify" the organizations estimate on information loss, digital damage and its impact on overall business productivity and business sustainability in the competitive markets. The entire procedures being continuous and cyclic go through a number of iterations, subject to the nature of the cyber theft.

B. Management Techniques: Organizational management techniques are the set of high levels decisions, which are secretive and highly confidential. In general they are strategic by nature, not freely predictable, by any one. Cybersecurity management (CM) is relatively a new technique, might have started one to two decades from now, yet managing it is a real challenge. As of today, there is no consistent and complete CM for managing cyber threats and crimes. The two primary reasons for this includes: Cyber threats and crimes are of business specific, categorized as: Preventive, Detective and Productive, described below. Second management

technique in handling these is not entirely technical, but involves social science theory, organizational psychology and business needs [4] [6].

Business related 'preventive' techniques do exists, fall under information assurance (IA). These will be familiarized to all employees through mandatory trainings. They shed light on ethics related to work and business, with an undertaking from every individual. An organization is conglomerations of different personalities vary in academic as well as experience backgrounds. Some joins organization with good working knowledge and improve further; others come with fewer working knowledge, but improve their working skills through trainings. In either case the management should make sure that they are adequately skilled; cybersecurity treats all alike.

The question remains unanswered to today's corporate world is with third category viz., people with join organization with fewer working skills but have no motivation to improve [5][7]. There is rich possibility of these becoming cyber thieves, through white collar thefts. There are some techniques in social science and organizational psychology addresses these issues, which are beyond the scope of this research.

By default, 'detective' techniques are the most difficult to handle and are specific type, sheds more light in estimating digital loss and its impact. Digital loss can also include a small hardware component like integrated circuit chips (ICs), processors etc. The main issue in this regard is to identify the person who initiated, processed and implemented such a theft. Short circuit cameras may not be of much help in this regard; usually referred to as white collar theft. All modern ISs have several inbuilt features, in detecting personal identity, through fingerprints, tomography, Iris etc., but often hackers can go much beyond these.

The 'productive' techniques are useful in projecting, modifying and improving cybersecurity, and push organization towards market leadership. These are the standards each organization to follow in order to protect their digital assets. Department of energy (DOE's) cyber security capability maturity model is a good example in this regard [12]. This basically helps pushing the organization towards higher cybersecurity capability and higher security management standards, and is vital in procuring and managing all the digital assets.

C. Management Model: Management model is very vital for organizational growth, basically represents, establishes and demarks an organization and its strength/significance within in the competitive markets. For example, a software company, with capability maturity model (CMM) level 5 company attracts more projects, progress very fast in the competitive markets, does not mean it is more productive or quality oriented; instead one should realize that this is built on a standard business model. Therefore any business flourishes on a standard management model. We propose a general view of an organizational management with their decision making capabilities, to give an idea of management model, as shown below in Figure 03.

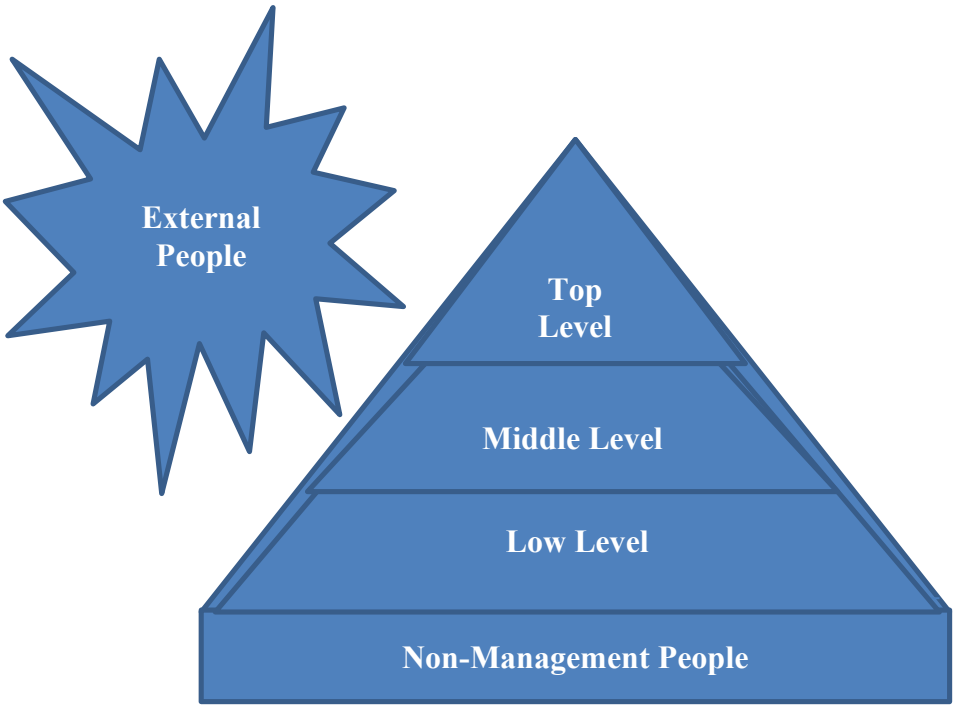

Figure 03: Organizational Management Levels

***Top Level Management*:** A high level set of executives and strategic decision makers for the entire organization create organizational long term plans. These people are expected to poses high levels of leadership qualities and commitment to business/organization. Major organization functions are directly based on these peoples' vison and mission. As dynamic drivers and path finders of the organization, in general includes: Chief Information Officers, Chief Executive Officers, Board of Directors, etc.

***Middle Level Management*:** These are supervising category, tactical decision makers, monitor day-to-day, activities of the organization and its associated business activities. For better productivity and quality this team controls all business processes and products. As supervisors, these are very good in getting the work done for the day/week/month, includes: Vice Presidents, Deans, Assistant Provosts and Assistant Directors; reports directly to top level management.

***Low Level Management*:** These are the actual working class of the organization, work in groups and teams, reporting to their supervisors. Since these are more in number, and as operational decision makers, do the actual work for the organization, with time limits.

***Non-Management Workers*:** There people work for a short time period, on an hourly or day-to-day basis, across the organization. Being a temporary or contractual workers, designated for certain specific work profiles, possess job specific knowledge.

***External People*:** These people, stays externally to the organization and its business units, yet influence and impact its overall progress and success of the organization; include the customers, stake holders and raw material suppliers. These peoples are the creators of the organizational image within the society where it physically exists.

These different levels of people will have direct (or indirect) impact on the overall productivity and quality of the organizational products and services. The first three levels of management (from top), must be familiar with the competitive technological trends in the market. These are

the real players for the organizational technology change management. Cybersecurity and its management are very much tied-up with these. Over all the technology upgradation is always subject to economic viability and budget constraints of the organization.

Technology Upgradation and its Impact

Technology is a non-volatile entity to human society; perceive it through products or process. From an organizational perspective, its upgradation can be visualized from two different schools of thought: As a competitive driving force and as an innovation task. In 21st century, every business organization is intertwined with technology as part of their business process, input, process and output. Modern business organizations are forced to allocate funds exclusively towards technology and its upgradation [2] [8]. Technology always thrive businesses towards market leadership; staying up to date with technology only can makes it possible.

At the same time, new technological products coming to the market on daily basis, making world more and more competitive. This has also given scope for technology innovation, where new products or process development, which is time and cost effective. Therefore every business organization has realized its existence and sustainability, by striving towards technology innovation as part of their core business improvement. This has become the driving force to businesses and strategic management of technology, part of research and development (R & D) wing's responsibility. Technology innovation is a spinning ball in modern market, its support and improvement become mandatory and the responsibility of every business management; in order to remain competitive in the market. Thus the age of creativity and innovation has become two challenging tasks for the modern corporate world.

Cybersecurity and its off spins like CMP and its management, assures corporate digital assets. Finally building technology-based distinct competencies and technology leadership has become modern business trend. For example, big data analytics and internet of things (IoT) also playing a vital role, as a technology off spins, in the modern corporate world in this regard. The inventions of IPv6 protocol, in fact, is a technology response to cybercrimes, that has built-in authentication, integration, confidentiality and control capabilities at the IP layer level. For todays' society, computing slowly becomes easier and less expensive in one side, making it as an easy task for hackers, on the other side, of the same coin. Though the technological upgradation is done from several spheres within the organization, it is also a mandatory step, for its awareness throughout the organization. Through every employee may not be aware of micro details, but should be familiar with goals of such a technological innovation [9] [10].

Technology Awareness across the Organization

The modern society has clearly witnessed one seminal fact: Technology and cooperate world's dependency on it, is becoming inevitable, in fact start growing exponentially. Therefore in order to coop-up with this rocket fast industrialization phase, the current society needs to evolve accordingly. For that one seminal factor that needs to be geared up is technology education and technology awareness among the public; especially in view of fast growing cyber thefts and cybercrimes.

All along technology has been a logical mix of purposeful application of human knowledge, skills and experiences. It has shaped the world for better utilizing the resources to create products or systems to meet human needs. Off late this human knowledge is misused by some set of groups and teams, pushing the world in backward direction. For that cybersecurity needs to be understood and address, in human mind from its positive spirit, of protecting corporate digital assets. All along the corporate world is looking at technology as an important asset for

their business expansion. Thereby the technology awareness has become an important agenda for all employees across the organizations. Once employees aware off technology and its usage, and security importance; one can control the internal white collar thieves, which in turn sends a positive note to external hackers.

Most of the businesses across the world started inter-twining the technology with their main stream business processes. Technology slowly starts influencing (and influenced by) different cultures of people, has become part of our daily life. These days, technology awareness and familiarity to its employees, has become a major concern to top management. To some extent this comes as a helping hand in minimizing/eradicating cyber thefts. As most of the cyber thefts works in groups, it is necessary for every employee to be familiar with prevailing technology. To that effect, most organizational management periodically conducts technology workshops, among its employees. In this era, during such technology workshops, cybersecurity aspects are taking a front bench.

It is worth noticing that: Cybersecurity is everybody's concern within the organization. Except to a small portion of employees, rest is invariably uses the organizational information systems for their day-to-day work. On the basis of work ethics, every employee is invariably responsible for their system's security; need to safe guard their departmental software systems. There by making familiarity of the existing computer systems and their possible threats, is a mandatory for everyone.

Having discussed CMP, from its architectural and components view; rest of the two sections focus CMP from two different perspectives viz., comprehensive and system complexity view as detailed below.

COMPREHENSIVE VIEW OF CMP

Based on the technical details of CMP it can be visualized as a comprehensive service source to the entire organization. The upgradation of CMP in a timely manner addresses the other business governing issues like business intelligence, business objectives and risk management [11]. Here we briefly detail each of these issues and their connectivity to CMP. It is possible to achieve these business governing issues to each of these tasks, through different modules within CMP. This is beyond the scope of this work. However we review some of these aspects from CMP perspective as shown in Figure 04 below.

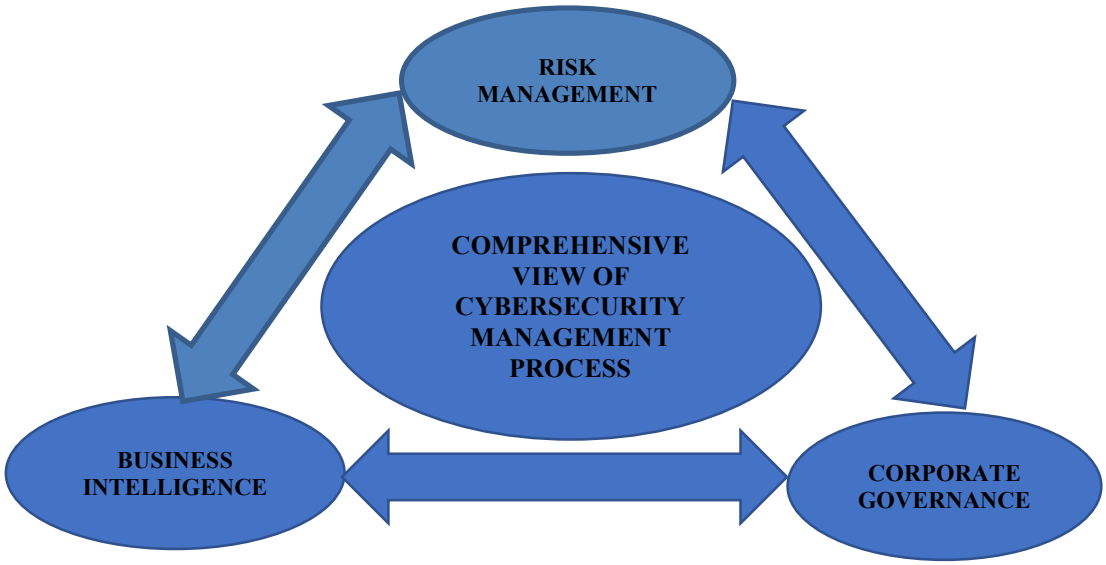

Figure 04: Comprehensive view of CRM

Risk Management: This is a process for identifying, assessing, and controlling threats to organization's capital and earnings. In this era, it includes more business processes exclusively for identifying and controlling threats to all company assets such as corporate data, supply chain data, customer data, and intellectual data. From the CMP perspective one narrow down this set of assets limited to digital assets, such as confidential data, ISs, Databases, etc. Further to each of these modules we can define a separate firewall with two level personal identification password system.

Business Intelligence: Business intelligence (BI) is a computer based technique in spotting, digging-out, and analyzing business data. In the course of such an analysis the system should be in a process to identify useful and corrupted data and eliminate accordingly. Intrinsically CMP is intertwined with BI in the following ways: intelligent decision making, data warehouse management and Web trafficking. On the other hand, BI is a collection of several techniques in which CMP certainly play a major role, due to its connectivity with business data and its security. BI also uses several special techniques such as data mining, machine learning and statistical; their connectivity to CMP is beyond the scope of this research. Therefore CMP basically provide a comprehensive data, used by all these BI techniques.

Corporate Governance: These are a set of techniques by which companies are directed and managed. These are the sole responsibility of top level management people. It is worth noticing several similarities between the CMP and corporate governance. CMP is very much linked with its corporate strategic direction and governance is about its implementation. Both corporate governance as well as CMP ensures a good strong and balanced economic growth. At the same time, both governance as well as CMP lowers the capital cost needed for the company. A good governance and CMP ensures customers confidence and help minimizing the wastages, corruption, risk and mismanagement.

SYSTEM AND COMPLEXITY VIEW OF CMP

In this digital era, world is coming closer day by day due to rapid usage of Internet and variety of communication devices. This looks very interesting and fascinating, but on the other hand, there exists a serious problem: People spending long hours of browsing the cyber world, indirectly giving an opportunity to someone else to peep into it, steal or hack the data – cybercrimes [1][3]. Since everything is in digital form on a cyber space, it is very difficult to identify the cyber criminals, going beyond the scope of any law enforcement agency. Though it is far reaching task of identifying the hacker, but with few precautionary measures one can safe guard their computer systems.

The systems and complexity view of CMP sheds light on some of these issues from management perspective. Please remember, every top level manager may not be a cyber expert to visualize and analyze all the cybercrimes and theft, yet he/she needs to be familiar with certain vulnerabilities with all digital data. Before we go into the details of those cyber measures, first let us have a look at the types of cyber-crimes, which are prevailing in our society. Systems and complexity view can be further sub divided into two broad angels' viz., threat driven approach and cyber activities and their impact on businesses.

The Threat Driven Approach

Threat is basically an idea initially triggers in human mind, to do a particular task in a specific way, which makes panic in and around a particular situation. Neither the person invoking nor the person witnessing/receiving this treat is unaware of its full consequences. Computer threats are not a new phenomenon, have been around since several decades. These are basically a possible danger that might exploit a vulnerability to breach security and therefore

cause possible harm [3] [2]. Only in recent days people start looking it seriously in view of its consequences. There are some IS in the market, which can predict, correct and delete threats, across networks, databases and servers. The hackers' knowledge level is going much beyond the scope of these ISs, causing anguish among the business owners and management professionals.

By default these threats are relentlessly inventive by nature, constantly evolve to find new ways to annoy, steal and harm. A threat is like a painless injection into our human body, goes in to the body, in a way that, it is very difficult for patient to realize its immediate consequences. However, there are several public sector and private sector companies developing several vaccination software, capable of predicting, controlling the deterrent computer systems. Threats come in a variety of ways, so it is very difficult to enumerate and categorize the types of threats; however here we provide a broad spectrum of threats:

Virus: This is a computer program/software, capable of altering the way the computer operates, without the permission or knowledge of the user. Thereby the fixed instructions given to the computer are now contradicted, results in damage to the computer.

Spyware: This is also a program/software sit in your computers and monitors your activities or installs programs without users

Hackers & Predators: This refers to a group/set of programmers, who are capable of writing computer programs, to victimize others by breaking into their computers, to exclusively steal or change or destroy their information. We refer to this as cyber-terrorism.

Phishing: This is a person; need not be always a programmer or a system administrator, who is masquerading as a trust worthy person or business, attempting to steal sensitive financial or personal information through fraudulent email or instant messages. This makes user to confuse between a legitimate message and a phishing scam.

Computer (or a computer system), a human made machine is useful in several ways, solves day to day real life problems, has now become threat (called cyber threat) to our society. This clearly reflects how human are unethical and insecure in terms of their thinking capabilities? Thus "human thinking", is the most common underlying aspect of these threats; especially so, at work places and/or in decision making, known to be organizational psychology.

Organizational Psychology and CMP

An organization is built on three prominent components viz., people, processes and products. People are rated (or judged) for their thinking (or working) capabilities, processes are chosen according to their strict adherence to company policies and procedures and quality decides the products. An organizational growth depends on two clear visible concepts: Productivity (due to products) and Quality (due to processes). This product and process depends on people and their workmanship. Further, people are the most important assets to organization, in starting and maintaining its business processes and methodologies. On the other way round, these people's (employees) understanding about the organization, in terms of its policies, guidelines, vision and mission, is also of equally importance. Therefore most of the business objectives are achievable only through employees understanding about the organizational psychology (OP). The following is an outlines OP in a nutshell, shown below in Figure 05 below.

Figure 05: Organizational Psychology

In OP, "thinking capabilities" broadly includes an in depth understanding about the organization and its business policies; can be improved only through environment and society. This is also influenced and intertwined by factors such as work-related attitude, leadership, decision making and stress. The "workmanship" can be improved through organizational trainings and practices. Workmanship is also influenced by factors, socialization, group dynamics and communication.

Therefore the impact of OP on every employer is phenomenon, in improving several invisible factors on human thinking capabilities and in improving the workmanship. Therefore the organizational psychology (OP) is an overall study about employees' understanding about their organization, in terms of its business processes, policies and methodologies.

Cybersecurity is relatively new subject when compared to OP, is fast influencing today's digital world. It can be visualized as combination of hardware, software and processes, tied up in a compact way as shown below in Figure xyz. The invisible activities here includes thinking capabilities and workmanship is deterministic, can be improved through supplement of certain logic, data structures and programing skills, through organizational training and workshops. Tracking and monitoring the "hacking" activity is becoming a challenging day by day. There are some developed techniques, but inadequate for today needs.

Cybersecurity is witnessed to have close link with organizational psychology, from three different perspectives: Human attitude, Thinking Capabilities and Workmanship; unfortunately which cannot be altered through any common software processes and products, across organizations as shown below in Figure 06.

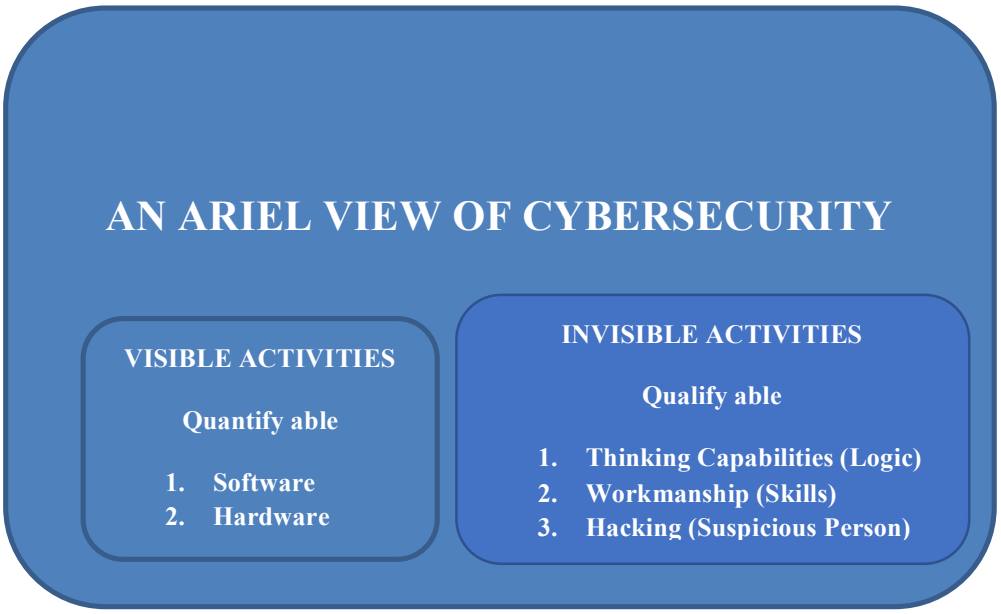

Figure 06: An Ariel View of Cybersecurity

Business Intelligence Life Cycle and Societal Impact

We know that a typical business intelligence (BI) is not just a set of software tools to analyze raw data to help make strategic and operational decisions. Typically, BI is a framework, which offers guidelines in understanding what to look in the volumes of disparate data. Therefore as a framework, BI is a continuous cycle of analysis, insight, action and measurement as shown below Figure 7 [13]:

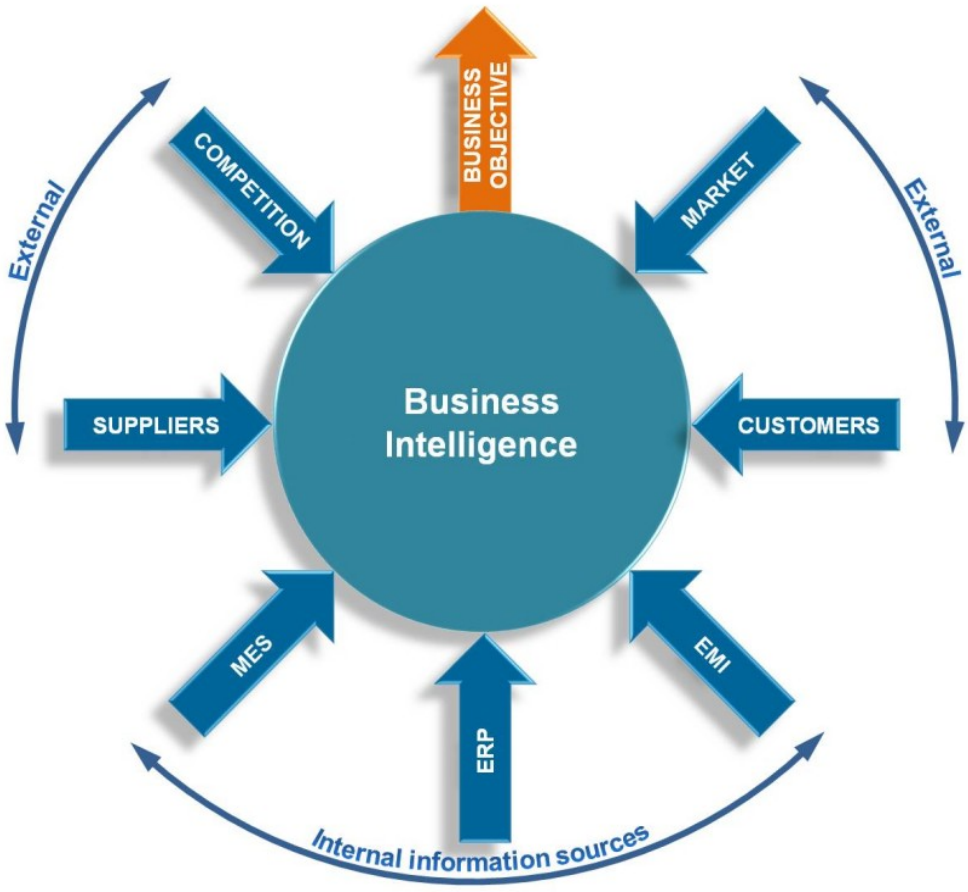

Figure 07: Business Intelligence as a Cyclic Process

BI derives its data from seven directions aiming in one particular direction viz., "business objective". In particular, as shown above, its main digital data/information come from several internal information resources like EMI, ERP and MES; which sustains the organization and useful for its survival in competitive markets. Each of these information resources go through a sub-cyclic process, as shown below, help towards intelligent decision-making process, while improving their products and services.

In any business organization, the work nature goes through a particular cyclic path, depends on the products or services it offer. BI in cybersecurity is defined as action cycle (as defined below), with reference to organizational digital assets. Every computer process data in to some useful information, then human mind converts information into some useful knowledge; finally, this knowledge is used for (intelligent) decision-making (or sometimes by alters or readjust the data). Therefore, the final decision-making (by top-level management) is precisely the crust of the corporate BI.

The logical connectivity among Data, Information, Knowledge and Decision Making with reference to business, is always cyclic (by nature) supported by several ISs, as shown below in Figure 07 below.

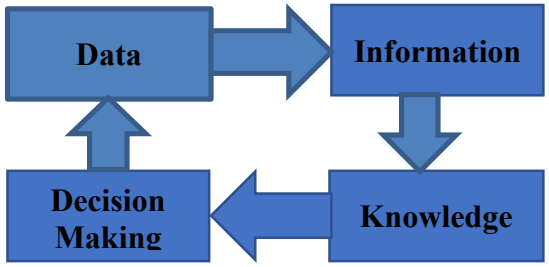

Figure 08: Business Intelligence as a part of Cybersecurity Process

Each of these components has several subdivisions such as raw data, processed data, Process Specific and Product Specific data/information, Expert knowledge, Organizational knowledge, intelligent decision making. Business intelligence (BI) is the new technology for understanding the past and predicting the future. For example, the company sales data in the past few years, taken as input, and predicting the sales of the company, in coming years. We briefly present few ideas of BI with reference to modern businesses and their cybersecurity as following:

1. *Data*: It can be employees and/or resources IDs, sometimes even the IDs of some business software. This is not specific to a particular department or unit, but needs to be at a low level of security; level 1.
2. *Information*: This is surely more of a department or business unit specific. Human resources IS, is different from that of marketing IS, sometimes, one IS can be shared by few business units. The security and upgradation of these ISs is precisely cybersecurity, fall under the control of cybersecurity infrastructure. This needs a medium level security; level 2, as some information might be a shared value for more than one business unit or department.
3. *Knowledge*: This is more of organization specific, though it generate in one specific business unit or department, called intellectual property; thus demands additional level of security, level 3. This knowledge is useful not only in that business units progress but also helps in moving the business to the next level. Cybersecurity has larger responsibility; especially while passing through, intra/inter departmental communications networks. Therefore needs a double layer network security, while transmitting.
4. *Decision Making*: This is a very crucial and cost effective process by its structure, needs

highest level of security, level 4. This has impact on many aspects of the business such as market leadership, sustainability, organizational merging, business process improvements, etc.

The impact of above defined BI cycle on CMP can be visualized in the following directions:

- Process improvement
- Impact on productivity and quality
- Creation of intellectual knowledge
- Over all control over the business ISs
- Avoid several cyber threats and crimes

Employees bring different level of skills, education and experience to the organization, yet they are part of the same cybersecurity infrastructure. Therefore the social and cultural values are clearly visible in work places. In fact CMP has many views towards societal impact; it believes them to be root cause for several types of cyber thefts and cybercrimes. Furthermore the urban and rural education system also impacts the individuals' behavior at work places. The following are some possible places and situations at work place, where employees are influenced by the society and environment.

- Working in groups, with reference to group coordination and communications.
- Organizational meeting places, with reference to yes-men groups
- Organizational dining and canteen areas, with reference to food choices
- During the division of labor, with reference to skills/experience coupled with favoritism

The implementation of CMP is more strategic by nature allows flexibility with reference to time and space complexity. BI being a part of CMP, for every task/goal, it gives an opportunity to re-think in a cyclic manner, before arriving at intelligent decisions.

Cyber Activities and their Influence on CMP

It is very difficult to define possible places for cybercrime; it can be online, computer network, databases, etc. Cybercrimes are invisible by nature, uses special techniques and processes, not covered in literature. At the same time, the consequences and impact of them is very huge and difficult to quantify. These days, most businesses being online, necessitate research and focus in this direction. Before we go further, let us look at the types of cybercrimes.

Types of Cyber Crimes

A cybercrime is mostly invisible before and during its operation, but by the time, one realize, the damage might have already occurred. Therefore cybercrime is a malicious activity, by known or unknown person within or outside our community. Majority of cybercrimes are due to internal employees of the organization, leaving scope for suspicion on everyone. The proposed CMP and model of CMP are just attempt to ensure that they were either prevented or will not occur again. It is humanly impossible to enumerate all types of cybercrimes, detail here a broad spectrum of cybercrimes:

Hacking: This crime occurs when peeping (entering) into some else computer without his/her permission, to access his personal and sensitive information. In some organizations, in order to check their internet security protection, the administrator arbitrarily login into some ones computer – called ethical hacking.

Theft: This crime occurs when violate the copyright act, such as downloading music, games, and online messages. Nowadays, there are few laws which prevent people from illegal downloading.

Cyber Stalking: This crime occurs, when someone is giving unsolicited emails and messages online, using Internet as stalk.

Identity Theft: This crime occurs, when criminal uses victim's personal data online, such as bank account, credit cards, social security, to siphons money or to buy things online in the victim's name. This results not only financial loss to victim but also spoil his credit history.

Malicious Code: This crime occurs, when someone writes a malicious code online, which disrupts not only the network but also its clients.

Child Soliciting and Abuse: This crime occurs, when criminal solicits minors via online chat rooms for the purpose of child pornography. There are some measures taking by government to prevent this type of crime, which leads to child abuse.

Computer Vandalism: This is a type of cybercrime, that damage or destroys data rather than stealing; it basically transmits virus.

Each of these crime types occurs according to nature of digital source used such as network, database, server, etc. One thing is for sure, the hacker attempts one type of crime, failing which he/she shifts to other. The same hacker's psychology also applied for his/her attempt on different digital sources as well. At the same time, one thing which is not sure: How long hacker will do these silly attempts of different types of cybercrimes?

Analysis of Cyber Activities

In this technological era, hacking comes in different forms and shapes. Each crime comes with a wide range of actors and methods, yet difficult to find their trace. Forensics throws some light on this cybercrime analysis, through some sophisticated software such as ProDiscover, Encase and FTK; but the procedures associate with are more cost/time effective. This field also gives excellent techniques and methods of protecting your networks, databases and servers. Sometimes the pattern of crime on a digital source gives us a clue on next possible upcoming crime.

Sophisticated attacks possess a greater damage potential to both ISs and networks. Hacker groups start breaking the pentagon network to steal military software and threats to sell the software terrorists if their demands are not met are on a rise. This clearly shows hackers are no longer enthusiastic cyber-geeky profiled teenagers, but are monsters with bad intentions having monetary interests and selfish motives. Slowly we see a strong link between attackers and terrorist organizations who envision cyber-crime as a potential mode to carry out their motives.

The increased difficulty in protecting data comes as the value of intellectual property is sky rocking for companies. At the same time, in view of proliferation of devices, the number of locations and devices that information can be stored makes the of keeping track of this more challenging and difficult for an organization, giving scope for establishing a CMP. The analysis of cybercrimes needs to be analyzed from two different directions: Estimate the knowledge unit it has impacted, and the ways of improving (or modifying) the aspects of risk management (towards information assurance aspects) of the business. The invention of IPv6 protocol is an

attempt to address cyber-crimes, as it supports built-in authentication, integration and confidentiality and access control at the IP layer.

CYBERSECURITY MANAGEMENT MODEL

In general, management model is a set of well-defined practices with high level of abstraction, with which individual organizations interpret their various structures and sizes [12]. Management model demonstrate the uniqueness of the organizational process and positions the organization in the competitive market. It represents organization's image from three unique perspectives viz., process capability, service capability and business strategy. In the past several researchers study the management models and their impact. The standard three step approach includes: First business management must undertake a risk analysis for their organization and prioritize their assets that require the most protection. Second, leadership is necessary to take necessary action and ensure information security best practices are employed by the enterprise. Third, organizations must be prepared to detect and respond – internally and externally – to cyber events via institutionalize organizational processes [7].

Cyber security management model is a linear combination of existing cybersecurity frameworks, standards, programs and initiatives. This proposed model is supposed to provide guidance to help organizations develop and improve their cybersecurity capabilities. Corporate managers act in accordance with their mental model of the situation, and this model is highly subjected to situations and conditions. Corporate management models will reveal and help simplify many complex realities that one needs to recognize and interpret. This model is expected to outlook all the possible cyber threats and crimes, consists of four primitive variables, form as cyclic process, as shown in Figure 09 below.

Cyber Variables: One need to identify cyber variables, which are the driving force for the CMP. These variables include,

1. Culture: A way of thinking, behaving and then working. Every digital asset is sensitive and part of organization's intellectual property, its protection and security is every ones' responsibility.
2. Processes: Intelligent and short cut methods at the work place. Every information system is proprietary software, their copyright is not allowed.
3. Objectives: Organizational business objectives are the employees' work objective. Employees' work progress is proportional to organizational business progress.

Cyber relationship among those variables: The relation among these variables should be secured and limited to only working group/team. The digital input data, is to be related to the existing process, finally linked with the output information. This output information to be related to databases and decision making activity, across the organization.

Illuminate the Cybersecurity context: Every cyber variable and their relation is a program or system concept, so it needs to be illuminated only in organizational business context, without misusing or releasing to others.

Offer a range of perspectives: The range of organizational perspectives is an OP concept every organization expected to visualize them in their respective business way. Once cyber variable, relationships and business context is established, then the range of business perspectives to be established from three angels:

1. Unitary Perspective: This is based on the assumption that organization is an integrated group of people with single authority/loyalty structure and set of common values, interests and objectives shared by all members of the organization.
2. Pluralistic Perspective: Pluralistic perspectives is made up of powerful and divergent sub-groups, each with its own legitimate loyalties and with their own set of objectives and leaders, such as management and trade unions
3. Critical Perspective: The critical perspective is to develop employees' power as critical creative and active thinkers. Some employees' intellectual contribution and ideas are more powerful than management (being passive) views.

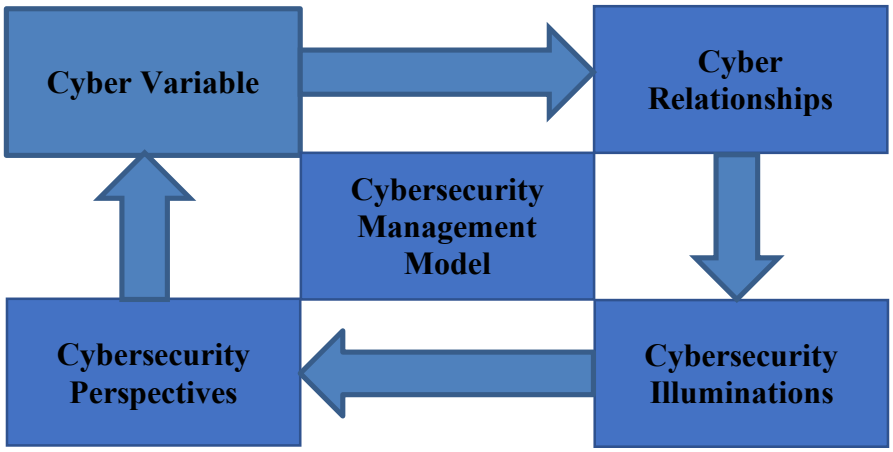

Figure 09: Cybersecurity Management Model

This model also throws light on set of choices made by top management (executives) about how the work of management gets done. Therefore every management member should be aware of certain market and technological innovations, in order to sustain in the competitive market. This model also needed for better business quality and productivity. Finally this model reflects choices made by top executives regarding how they define objectives, motivations efforts, coordinate activities and allocate resources. The other management models like strategic management models, capable of allowing new as well as existing businesses to build new strategies that help the organization responds quietly and quickly to new technological challenges.

In essence, all the existing management models stick to a specific management process in choosing and defining organizational purpose and its functional objectives; then finally formulating and implementing a viable long term plan (strategy) for that specific business.

LESSONS AND CHALLENGES DERIVED FROM OF CMP

Most of the modern businesses are doing their business both in traditional way as well as online, due to immense customer support and market demand. Cybersecurity is more in tune with online businesses, impacting e-commerce businesses. In spite of several third party venders, come in between the customer and online businesses, no one can stop customer accessing the online businesses direct selling site. Therefore for a criminal accessing online sensitive information and data using it means a rich harvest of returns; but unfortunately catching such criminal is not that easy task.

We do not have a consistent, complete and correct CMP, yet there are many techniques exists through information assurance; coupled with some seminal methods of preserving our digital assets given by forensics. Overall cybersecurity management has been a fascinating field, both

to academicians and industrialists from two different viewpoints: As a continuous management aspect and more rewarding field to attain the market leadership. The following are some of the (may not be exhaustive) challenging and lesson learned issues with CMP

1. Integrate the cybersecurity as part of the business process/plan.
2. Make sure to encrypt every employee's cell phones, personal laptops, business computers are properly encrypted.
3. Even the best programs, if they are hacked, will experience failures, and expose some sensitive information. Therefore best organizational ISs and programs need to be under the control of top level management.
4. Establishing a cyber group across all departments within organization, make them responsible for all cyber activities, might reduce number of cybercrimes.
5. Cybersecurity management looks like a top-down approach, but may not be. As most of the cybercrimes are bottom –up approach. In either case, first every top level manager should be aware and familiar with existing technology and IT 100%.
6. The protection of critical company and customer information is a business requirement to protect the company's reputation and enterprise value.
7. How do we ensure the enterprise risk management process through CMP and based on few hacking incidents?
8. How to categorize threats that have immediate, medium and longest effects/consequences on the organizational business processes?
9. What are the different ways of detecting, analyzing and correcting, the longest consequences of cyber threats?
10. What is the impact of CMP on business IT management its procurement process?

CONCLUSIONS AND FUTURE POSSIBILITIES

It is concluded that, every business organization should have a strong CMP, as part of every management process, to secure their digital assets. It is clear that instead of attempting to find the hacker details, educate the employees for the prevailing and using technology across the organization. All employees are the organization's assets, so is their awareness to current technology. One need to develop a security measure/method and a security process, to our customer databases on a high priority basis. Designing certain cyber security principles and ethics as part of the curriculum at high school level entails good ethical employees for future.

References

Salim M. Hamid and Madnick E Stuart (2016), Cyber Safety: A Systems Thinking and System Theory Approach to Managing Cyber Security Risks, Working Paper, Cybersecurity Interdisciplinary Systems Laboratory (CISL), MIT, Cambridge MA 2016.

Ramanosky S and Acquisti (2014), Privacy Costs and Personal Data Protection: Economic and Legal Perspectives, Berkely Technology Law Journal, Vol. 24, No. 3. May 2014.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February, 2014.

Draft Version of Maritime Cybersecurity Project, Maritime Security Center, American Bureau of Shipping (ABS), August 2017.

Tomasz C, et al, (2014) Enterprise-oriented Cybersecurity Management, Proceedings of Federated Conference on Computer Science & Information Systems, ACSIS Vol. 2. 2014.

Susan M.Tisdale (2015), Cybersecurity: Challenging From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective, Issues in Information Systems, Vol. 16, Issue III, June 2015.

ICC Cyber Security Guide for Business (2015), ICC Publication No. 450/1081-5, 2015

Eric A. Fischer (2016), Cybersecurity Issues and Challenges: In Brief, Congressional Research Service Report 7-5700, August 2016.

J. Barateiro et al (2012)., Manage Risks through the Enterprise Architecture, in Proc. 45th Hawaii International Conference on Systems Sciences HICSS-45, Hawaii, Jan 2012.

Y.Y. Haimes (2008), Models for Risk Management of Systems of Systems, International Journal of Systems of Systems Engineering , Vol., 1, No. 1.2, 2008

J. Araujo Wickboldt et al (2011)., A Framework for Risk Assessment base on Analysis of Historical Information of Workflow Execution in IT Systems, Computer Networks Vol., 55, No. 13, September 2011

DOE's Cybersecurity Capability Maturity Model (C2M2) Version 1.1, February 2014

Web Source: http://intellidsi.com/the-business-intelligence-cycle

