CYBERSECURITY:CHALLENGES FROM A SYSTEMS, COMPLEXITY,KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE

[1]Dr.M.padmavathi , Assoc..prof , CSE,macherlapadmavathi@gmail.com

Swarna Bharathi Institute of Science and Technology

[2] I.Ramesh babu ,Asst prof, CSE, inapala.ramesh35@gmail.com

Swarna Bharathi Institute of Science and Technology

[3]S. Nagamani, Associate Prof, CSE, nagamanikunchipudi@gmail.com

Swarna Bharathi Institute of Science and Technology

ABSTRACT

Cybersecurity breaches persist as a major threat to information systems. Concerns about economic interests, national and local security, and intellectual property are among the many areas impacted by these more sophisticated and severe intrusions. There are a lot of answers that deal with IT security and the technology themselves. Cybersecurity from a corporate, societal, and IT standpoint may be better understood with a systems, holistic, approach. The interplay and complexity of the organization's many stakeholders at the strategic, managerial, and operational levels are also taken into account. All of these things need to coordinate well and quickly. To find and handle the massive volumes of data needed to make suitable, prompt cybersecurity choices to avoid or reduce these breaches, Business Intelligence and Analytics offers a suite of approaches and technologies. Information technology, cybersecurity, knowledge management, business analytics, and business intelligence are all related terms.

INTRODUCTION

The Ponemon Institute released its eleventh report on data breach costs in May of this year. The overall cost of data breaches rose from $3.5 million in 2014 to $3.79 million in 2015, according to the research [15]. North Korean spies or an evil insider may have breached Sony Pictures' computer systems in November 2014, releasing humiliating personal emails and commercial secrets. Home Depot and Target, two of the biggest retailers in the world, lost millions of dollars in sales and customer trust in 2013 and 2014, respectively, due to massive breaches of consumer credit card information. Cyberattacks have repercussions beyond only the economy. The conventional wisdom is that cybersecurity issues are best studied via an IT-centric lens. A more recent body of work emphasizes the need for an all-encompassing strategy that takes into account not just organizational psychology and other elements like those outlined in the Clinger-Cohen Act, but also corporate goals, governance, and risk management. All levels and parts of an organization should work together to solve problems, according to Systems and Complexity Theory. Cybersecurity poses unique challenges to knowledge management due to the sheer volume of data, the transient nature of that data, the rapid pace of technological change, and the sheer number of parties and pieces of

information involved. Methodologies and tools for dealing with these issues are available in business analytics and BI. From these vantage points, this study analyzes cybersecurity.Pros and Cons of a Holistic Cybersecurity Strategy New evidence suggests a more comprehensive strategy is required to resolve cybersecurity gaps. A comprehensive strategy is required for cyber defense, according to research by Atoum, Ottom, and Abu Ali (2014). Cybersecurity frameworks are also inconsistent in their efficacy. Cost, operational considerations, and adversaries' capacity to adapt to vulnerabilities were not taken into account by most technological cybersecurity solutions, according to Hughes and Cybenko [11]. The Orange Book and other long-standing security rules are struggling to keep up with the increasing complexity of systems and new methods of procurement [11]. "Information security is a part of information risk management, which in turn has a place in business risk management," says Jirasek as stated in his work [12]. The model that the author lays forth takes into account

stakeholders, security drivers, and security management. Organizational compliance with applicable rules and regulations, the need to safeguard company goals and information, and potential security risks all constitute security drivers. Whoever receives or is responsible for safeguarding the data included in the company's goals is considered a stakeholder. Among the many artifacts, including system designs, that make up security management are policies and standards for cybersecurity control. Risk analysis and exposure quantification to risk and security risks posed by attackers are part of this [12]. According to Klaus, considering "technology, economics, usability, and psychology" is essential in cybersecurity, which is an interdisciplinary field (Klaus, 2013, p. 6).Security must be considered in all IT endeavors, according to Bunker, but this consideration must be tailored to the specific demands of the company [5]. "Strategic controls, such as business alignment and governance; risk and compliance; operational controls, including physical security; backup and incident handling and response; and tactical controls, such as secure builds, anti-virus and intrusion prevention," he explains, dividing the controls into many categories. [5]. A new academic field known as "economics and cyber security" has formed in the modern era. Cybercrime expenses are broken down into three categories: direct, indirect, and defensive costs (Anderson et al., [1]). Theft in the abstract, income lost because customers don't trust a business, and the price of conventional cyber protections like firewalls and antivirus software all fall into this category. Models and frameworks that took repair and recovery costs into account were studied by Thomas, Antkiewicz, Florer, Widup, and Woodyard [17]. A review of the literature on economics and information security by Anderson and Moore [2] reveals that cybersecurity should focus on three areas:(1) identifying and eliminating risky behavior; (2) developing systems that take into account human psychology, criminal behavior, and warfare; and(3) identifying the kind of institutions capable of managing intricate, interdependent systems.From these many perspectives, we may infer that cybersecurity management should take a comprehensive approach, taking into account not just technology but also corporate goals and alignment, governance, rules and regulations, economics, risk management, technology, psychology, and criminology, among many other fields. Systems theory is the bedrock of holistic methods. Cybersecurity management might benefit from Complexity Theory and Complexity Leadership Theory in light of the rapidly evolving cyber landscape of the twenty-first century. Theory of Complex Systems and Leadership As a meta-theory that cuts across disciplines, systems theory is well regarded. The foundations of the theory were laid forth by Joseph Litterer (1969) and Ludwig von Bertalanffy (1955).One definition of holism is the "interrelationship and interdependence of objects and their attributes" [16]. It also encompasses the following: (1) goal-achieving system interaction; (2) goal-achieving system transformation; (3) impact of environmental and other disorderly factors on systems; (4) impact of regulations on systems; (5) impact of system hierarchies and subsystems on the system; (6) differentiation among subsystems; and (7) multiple/alternative ways to achieve system objectives (Skyttner, 2005). The "problems of identifying, reconstructing, optimizing and controlling an organization, while taking into account multiple objectives, constraints and resources...possible courses of action, together with their risks, costs and benefits" [16] are considered in systems analysis, which is applicable to complex organizations. In response to the ever-changing nature of the global economy and the pressures on businesses and their leadership to keep up with the times, Complexity Leadership Theory has gained traction in recent years. Complexity theory was expanded by Schneider and Sommers (2006) to include non-linear dynamics, adaptation, evolution, and the impact of chaos theory. To maximize organizational performance, new dynamics are required, and the old theories of leadership and management that treated the flow of information between leaders and followers as simple cannot offer them [4]. A complex web of many interacting factors is entrenched in leadership, not just the influential act of one or more persons [19]. Additionally, Uhl-Bien, Marion, and McKelvey discovered the "entanglement of two roles:" when studying management under the Complexity Leadership Theory.(1) establishing the right organizational environment (or enabling factors) to encourage adaptive leadership in areas that need innovation and flexibility, and (2) making it easier for information and ideas to move from adaptive to administrative organizations. Everyone in a company (and in the adaptive dynamic) plays a part in enabling leadership, but the specifics of that function will change depending on where you sit in the organizational chart. [19]. According to Clarke [7], leaders should think about how they influence structures, context, and cultures, and that leadership is an autocatalytic process. According to these two schools of thought, cybersecurity is a complex, dynamic, multi-dimensional, and multi-disciplinary problem. Systems.

DISCUSSION

Thus far, this paper has brought attention to the seriousness and increasing worry surrounding cybersecurity breaches, the importance of taking a comprehensive and multi-faceted view of cybersecurity, and the need for methods and tools to organize, analyze, and share the massive

amounts of data required to manage cybersecurity among all parties involved.To begin with, who are the elements and stakeholders in this organization? In 1996, Congress passed the Clinger-Cohen Act, which was an early systemic approach to IT management. Following the mandates of the Clinger-Cohen Core Competencies and Learning Objectives from 2012, the US Government Federal Chief Information Officer's Council [9] established a collection of best practices in response to the Clinger-Cohen Act of 1996. First, policy and organization; second, leadership and human capital management; third, organizational development; fourth, information resources strategy and planning; fifth, models and methods for assessing the performance of information technology; sixth, management of project scope and requirements; seventh, control over capital planning and investments; eighth, acquisition; ninth, management of information and knowledge; ten, cybersecurity and information assurance; eleven, enterprise architecture; and twelve, management and assessment of technology systems. Cybersecurity, according to Systems Theory, may be seen from all these angles, even if these skills deal with IT administration.A taxonomy revealing the stakeholders and elements starts to take shape as a result of using the aforementioned notions. You may see this taxonomy in Figure 1 down below. You can see the mutually beneficial relationship between them by looking at the two-way arrows.

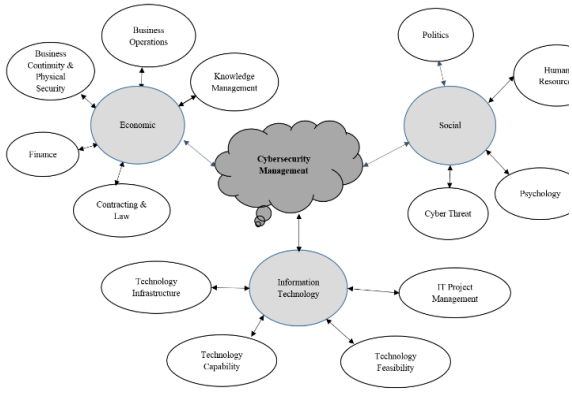

Figure 1. Cybersecurity Management Taxonomy

Volume 16, Issue III, pages 191–198, 2015, Issues in Information Systems 194 Following the mandates of the Clinger-Cohen Core Competencies and Learning Objectives from 2012, the US Government Federal Chief Information Officer's Council [9] established a collection of best practices in response to the Clinger-Cohen Act of 1996. First, policy and organization; second, leadership and human capital management; third, organizational development; fourth, information resources strategy and planning; fifth, models and methods for assessing the performance of information technology; sixth, management of project scope and requirements; seventh, control over capital planning and investments; eighth, acquisition; ninth, management of information and knowledge; ten, cybersecurity and information assurance; eleven, enterprise architecture; and twelve, management and assessment of technology systems. Cybersecurity, according to Systems Theory, may be seen from all these angles, even if these skills deal with IT administration. A taxonomy revealing the stakeholders and elements starts to take shape as a result of using the aforementioned notions. You may see this taxonomy in Figure 1 down below. You can see the mutually beneficial relationship between them by looking at the two-way arrows. Cybersecurity Management Taxonomy (Figure 1) Governmental programs, processes, and policies are all a component of policy and organization, as are the goals, functions, structure, rules, procedures, decision-making mechanisms, and interrelationships within and across agencies. Leadership and human resource management include a wide range of topics, such as developing and preparing for one's career, managing one's performance and employees, and keeping a skilled IT staff. Development of organizations, management of processes, enhancement of quality, reengineering of business processes, and cooperation across boundaries are all components of process and change management. Baseline assessments, interdependency analyses, IT planning, contingency plans, evaluation methods, and monitoring are all part of an information resource strategy and planning process.Compliance with the Government Performance and Results Act, decision-making, and the measurement of IT success are the primary foci of models and methodologies for assessing IT performance.The management of requirements, integration, time, money, performance, quality, risk, and lifecycles is an important part of IT program and project management. Other aspects include software development and testing, vendor management, and program management leadership. Portfolio management, business case analysis, cost-benefit analysis, and risk assessment are all topics covered in Capital Planning and Investment Control. Management of contracts, supply chains, best practices, techniques, and strategies are all part of acquisition.Data privacy and accessibility, records and information management, knowledge management, social media, online planning and maintenance, information collecting, and open government efforts are all parts of information and knowledge management.Information assurance and cybersecurity cover topics such as administration, plans and strategies, dangers and weaknesses, management of risks and security controls, reporting of incidents, enterprise management, and disaster recovery and protection of critical infrastructure. Among the many components that

make up enterprise architecture are guiding frameworks, functions, and ideas; development and maintenance; data management; performance assessment; and the application of architectures to investment decision making. Finally, when it comes to managing and assessing technology, there are a lot of factors to think about. These include mobile devices, networks, spectrum, computers, the web, data management, software development, cloud computing, data storage, and developing technologies. Outsourcing technology and the associated management challenges fall under this category as well. Everyone from top executives to contract and finance managers to lawyers to HR experts to IT specialists to law enforcement to organizational psychologists to stakeholders from outside the company are all considered stakeholders. Professionally and personally, each of these groups and people brings their own language, culture, and set of experiences to the table. Because of political factors, cybersecurity is an issue on a regional, national, and international scale.Stakeholders and factors (Systems Theory), the necessary complex and dynamic interaction (Complexity Theory), and the tools and techniques (Knowledge Management and Business Intelligence) to bring them all together (Cybersecurity Management Framework) are difficult to characterize. Consideration of the fact that every level of an organization is important is essential to all of this. These correlations are tried to be shown in Figure 2. In systems theory, there are three vantage points from which to view an organization: the economic (operations, continuity of operations, finance, legal, etc.), the social (human resources, organizational dynamics, politics, threats, etc.), and the information technology (technical infrastructure, capabilities, etc.). According to complexity theory, there are three tiers to every given system: strategic, managerial, and operational. The degree to which different levels inform one another varies with the specifics of the situation. The variables and levels are interconnected and not in a linear fashion, as proposed by the System and Complexity Theories. Uncertainty and chaos might set the stage for their occurrence. Technology and information exchange are moving at a rapid pace, making perishability a vital factor.

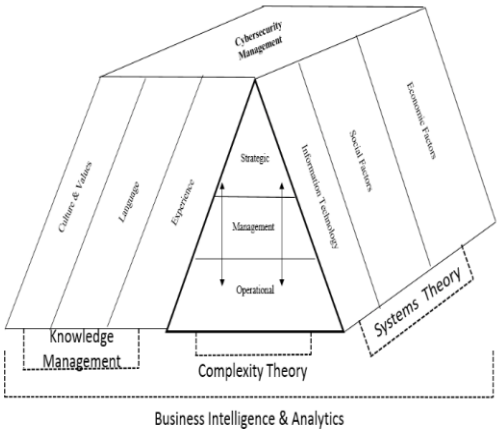

Figure 2. A Cybersecurity Management Framework

When leaders interact with the right information at the right time with the right resources, they are better able to handle the knowledge. At the right point in the business or operational lifecycle, for instance, the budgeting, contracting, and program management processes may connect important financial and project data. At the right moment, databases and incident responses may connect the dots between susceptible business processes and information systems, threat intelligence, and security mitigation tactics. Figure 2 has arrows pointing in both directions. This is to stress that all levels contribute to the whole and that any one level of an organization may take the lead in making a decision at any given moment. For instance, in the event of a security breach, fixing a significant vulnerability may take priority over day-to-day work or strategic choices, notwithstanding the impact on schedule or budget. Understanding and interpreting information in a timely manner is tough for managers under the best of conditions due to rapid technology and information turnover. Data accuracy and related business processes and systems provide a problem, particularly in big, complicated, and dispersed enterprises, even if Business Intelligence and Analytics gives the methodology and tools to aid with this task. Despite appearances, the work at hand is anything from easy or straightforward. Business roles, particularly in multinational corporations, may vary by region and by organizational level. Logistics at the corporate level may focus on long-term goals and objectives, whereas at the operator level the focus is on day-to-day resource acquisition. Securing the supply chain is of utmost importance for cyber and mission assurance. There is a time- and function-specific information demand for every level and function. It could be overwhelming to try to prioritize and map out all of these functions to the relevant data and system. Advice on creating knowledge systems may be found in Davenport and Prusak [8].They propose incorporating technological, organizational, and cultural factors while beginning with the business challenge and

identifying information of high value to the firm in order to construct the repository. On the other hand, if the company is big and complicated, managing knowledge systems in a constantly changing environment could become too expensive and time-consuming. Before all of the information is properly recorded, it can become obsolete.

CONCLUSIONS

Knowledge is at the heart of many organizational challenges. A lack of understanding is a problem in the field of cybersecurity. Decisions need rapid comprehension of voluminous amounts of information. It incorporates a wide range of people and organizations, each with its own set of norms, languages, and customs. Because of its complexity and the requirement for a comprehensive strategy, most companies would benefit from using Business Intelligence and Analytical procedures and tools. This might be because to a lack of understanding, an unwillingness to communicate what is known, an inability to articulate how to do so, or just divergent viewpoints on the subject matter. Some people or organizations could be blissfully unaware that an issue exists.To improve cybersecurity management, it is important to keep in mind the following points:(1) cybersecurity from a technological perspective is insufficient; (2) organizations should be seen as complex systems; (3) all employees, regardless of rank, should be involved in creating and sharing information as part of the information management process; (4) organizations could benefit from having a cybersecurity knowledge manager on staff who is skilled in multiple areas of the organization; and (5) cybersecurity functions and systems can be identified by beginning with the business problem to identify information, its priority, and related information systems.The extensive and complicated nature of cybersecurity management, as well as the best ways to safeguard information systems, need more study on these areas.

REFERENCES

1.Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013).Measuring the cost of cybercrime. WEIS, 2012, 265-200, retrieved from weis2012.econinfosec.org/program.html.

2. Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613.

3. Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. Information Management & Computer Security, 22(3), 251-264.

4. Avolio, B., Walumbwa, F., & Weber, T. (2009). Leadership: current theories, research, and future directions. Annual Review of Psychology. 60, 421-49. doi: 10.1146/annurev.psych.60.110707.163621.

5. Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. Elsevier Information Security Technical Report 17, 19-25, retrieved from www.compeseconline.com/publications/prodinf.htm. doi:http://dx.doi.org/ 10.1016/j.istr.2011.12.002.

6. Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big
impact. MIS quarterly, 36(4), 1165-1188.

7. Clarke, N. (2013). Model of complexity leadership development. Human Resource Development International, 16(2), 135-150.

8. Davenport, T.H., & Prusak, L. (2000). Working knowledge: how organizations manage what they know.
Boston MA: Harvard Business School Press.

9. Federal CIO Council. (2012). 2012 Clinger-Cohen core competencies & learning objectives. Retrieved from:
https://cio.gov/wp-content/uploads/downloads/2013/02/2012-Learning-Objectives-Final.pdf

10. Hofstede, G., G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind. New York:
McGraw.

11. Hughes, J., & Cybenko, G. (2013). Quantitative metrics and risk assessment: The three tenets model of
cybersecurity. Technology Innovation Management Review, 3(8).

12. Jirasek, V. (2012). Practical application of information security models. Elsevier Information Security
Technical Report 17, 1-8. doi:http://dx.doi.org/10.1016/j.istr.2011.12.004.