RESILIENCE IN CYBERSPACE WITH DATA ANALYTICS FOSTERED KNOWLEDGE MANAGEMENT CAPABILITIES: A DISCOURSE FOR SUSTAINABLE IMPLEMENTATION STRATEGY

Prof. Pradnya Kashikar
Research Scholar – MIT ADT University, Loni-Kalbhor, Pune- India
pradnyakashikar@gmail.com

Dr. Rachana Shikhare
Coach, Consultant and Associate – Samshodhan Trust, Pune-India
rachana.savita@gmail.com

Dr. Vinod Mohite
Assistant Professor, MM's IMERT, Pune-India
vinodbmohite@gmail.com

ABSTRACT
In the Cyber world today managing threats dynamically, is challenging, moreover generation of knowledge and enhancing knowledge management (KM) capabilities is becoming crucial due to the dynamics of technological advancements. In this context a regulatory mechanism is essential; this resilience required is achieved through data analytics which bridges the gaps between the challenges faced in cyber space and implementable realistic solutions.
Along-with the technological advancements it becomes imperative to optimally utilize and align knowledge management capabilities. A need was foreseen to reconsider KM capabilities in the fields of computer security, data management, also legal and risk management. The researchers have attempted to work on the aspect of sustainability, in handling challenges and solutions in implementing effective cyber security and in building better KM infrastructures; through innovative enabler such as Data analytics. In the proposed effort to elaborate this review study, assessment and quantitative analysis is recommended.
Keywords: Knowledge Management Capabilities, Cyber Security, cyber threat management, Data Analytics.

Introduction

In today's highly competitive world, IT infrastructures are preferred to be equipped with Cyber security mechanisms to curtail down the cyber threats. Protecting sensitive data, computer systems, networks and software applications from cyber attacks generates a large amount of data which can be analyzed substantially to form information security resources for better knowledge management around cyber security. Such protecting mechanisms are used by individuals and enterprises to deal with the challenges such as tampering and/or unauthorized access to vital resources and other computerized systems. Every organization has these important resources which are called as intellectual assets that include hardware, software, and data. With the continuous increase in the number of cyber threats and its effects on the organization due to the complexity of the cyber attacks; organizations are struggling to protect the information in an upcoming highly dynamic business environment. It has become essential and important to secure the intellectual assets including digital processes, information and IT systems from tampering systems and data stored within, exploitation of resources via attacks. These intellectual assets should be legally protected to achieve security of confidential information of an organization such as source code, solution manual, executable, live databases of clients, passwords and other confidential information stored on servers, financial data, and employee details etc.

The security of organization's data has become inevitable for the effective management and utilization of information generated by an organization as all organizations are driven by technology and technology is evolving very dynamically. The systems that are not aligned in coordination with information security mechanisms and policies may result into challenges such as unauthorized access, user authentication concerns, hacking, virus and worm dissemination, intrusion into company's private network and so on. People and group of people, that is employees and teams; work for an organization using intranet and extranet. Intranet is a type of network in which data and information is shared and is circulated within the organizations confined area. Extranet is nothing but company's private network at different locations where in data transfer and information sharing happens from one location to the other using virtual private networks.

Gap Analysis and Problem Description

With the rapid advancements in the technology and possibility of successful yet undetected cyber-attacks, organizations must adopt innovative methods, to derive dynamic strategies to manage threats effectively. This can be done seamlessly without loss of credibility, value and security of information which is managed by the

organization and used in several ways and formats. Managing upcoming threats dynamically have become extremely challenging, wherein data analytics and algorithms enabled in generating knowledge and enhancing knowledge management capabilities thereby propagating a need of a resilient solution.

Cyber threats are one of the key areas where concerns related to ransomware attacks, crimes related to upcoming technologies such as Artificial Intelligence (AI), Internet of Things (IoT), Robotics, blockchain etc., electronic commerce and mobile commerce related cybercrimes, financial frauds, etc. should be addressed. To improve the privacy and security when the information is in transit or the information is stored on hardware devices is becoming very crucial for the organizations. While analyzing the access mechanism and information during transmission; authorization becomes necessary and important in context to the security breaches, through openly accessible lines and with the help of ever-growing cyber attacking tools. It is seen that corporate networks can become vulnerable to cyber threats at larger extent. There are potential perpetrators at several points of penetration making the data at various levels of confidentiality vulnerable to intruders compromising the integrity of data. Email security and security of information stored on cloud and other networks is becoming more susceptible to attacks and companies need to be geared up with processes in placed to address cyber-attacks. The prevalence of ransomware attacks and increased use of internet enabled applications is leading to the risk to networks and information stored at servers.

Literature Review and Objective of the Research Study

(Masike, 2023)Security in all aspects of hardware, software and data are crucial for the management of policies, mechanisms at an enterprise level. (Samtani, Zhao, and Krishnan, 2023) To produce secure environment in the organizations, development in technologies like AI is beneficial for the implementation of secure knowledge management. Furthermore, in context with cyber security related tasks such as anomaly detection, vulnerability detection, bitcoin fraud detection, as well it is valuable.

(Ciasullo, Montera and Douglas, 2022) Big data analytics capabilities are fostering the opportunities for SME to identify tangible and intangible resources and infrastructure and ways and mechanisms to protect them from cyber-attacks.

(Zwilling, Klien, Lesjak, Wiechetek and Sklodowska, 2022) For effective cyber security controls awareness must be incorporated and should increase in the developing countries to avoid data loss and information retrieval challenges.

(Sandor and Tonţ,2021) To deal faster with the information security issues at the business enterprise level, the KM capabilities address the cyber security issues regarding organizational processes. The implementation of cyber security from KM perspective will help better identify risks, threats, and vulnerabilities and to create and maintain secure environment.

(Kapur,2020) For every individual, it is important to enhance knowledge in terms of augmenting the abilities consciously. Providing right information at the right time securely is nothing but a knowledge management.
Cyber security ventures (2020) powered by reviews for business by Finance Online, the computer ransomware i.e., hacking had been causing havoc to businesses and people worldwide. Organizations are considering ransomware as a biggest threat and a challenge to be addressed on highest priority, as it is fast growing, with damages predicted to be 57 times higher by 2021.

(Cyber edge 2020 cyber threat defense report, 2020) the frequency of successful cyber-attacks (at least one successful attack) is increasing year by year giving heads up for designing a framework. this can be implemented for aligning knowledge management capabilities with the help of data analytics as a tool. the technological advancements in attacking strategies have also been impacting continuously which is resulting into successful attacks as shown in the figure below.

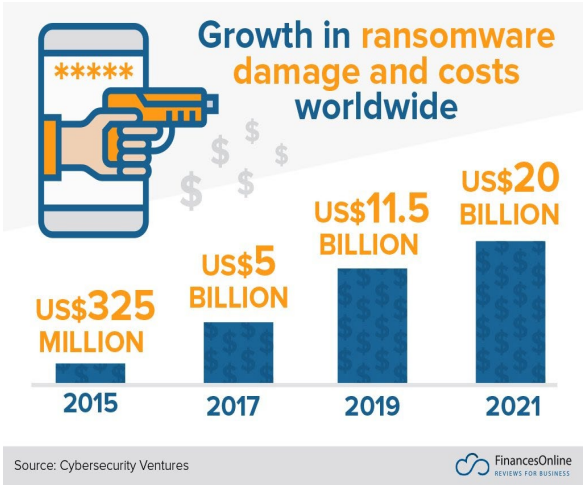

Figure 1: Growth in ransomware damage and costs worldwide
(Source: Cybersecurity Ventures; FinanceOnline, 2020)

This initial study aimed in fostering the knowledge management capabilities, in context of cyber threat management through data analytics; thereby bridged the gaps between challenges faced in cyber space and implementable resilient solutions. The strategic level capabilities of every organization are highly based on its domain specific environment.

(Obitade, 2019) The link between the KM capabilities and superior cyber protection is nothing but a data analytics which is important for the success of every organization.

(Jenab and Moslehpour, 2016). The cyber-attacks are growing day by day causing corporate espionage, threats to intellectual assets of every organization as well as it is impacting at an individual level.

Wang and Wang (2016); stated the differences between traditional enterprise information systems and KMS stating the data analytics methods and models that facilitates the knowledge management implementation. From the various studies carried out; it became imperative to address the everchanging cyber security challenges in context of the business environment as well as technological advancements. To optimally utilize and align knowledge management capabilities in these perspectives, there was a need to consider knowledge management and its relevant tools and techniques; in the context of computer security, data management, also legal and risk management.

The researchers have further attempted to explore how data analytics can be an enabler in identifying challenges and solutions in implementing effective cyber security and in building better knowledge management infrastructures. To sustain in this hyper competitive and data sensitive digital era, securing wealth of data gets vital precedence, using KM Capabilities through advanced proven analytics have acknowledged the case. Further assessment and supportive quantitative analysis are recommended in the proposed effort to elaborate this review study to the next level.

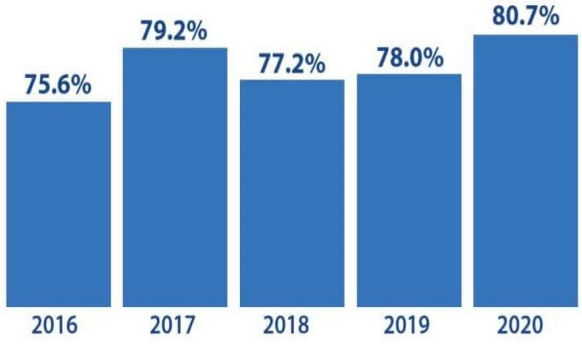

Figure 2: Percentage compromised by at least one successful attack by year.
(Source: CyberEdge 2020 Threat Defense Report)
In order to enhance the Knowledge Management [KM] capabilities of an organization, a holistic consideration of technical, structural, social, and cultural aspects of any infrastructure of a business enterprise is inevitable. Cyber threat management leads to a specialized organizational structure to follow best practices across the

interorganizational tiers. To address these concerns from multidisciplinary perspective, a thrust for some strategic model as alternative solutions becomes imperative supplementing it with innovation.

The flow of information in business organizations comprises of various knowledge forms that needs to be modelled to emphasize its relevance and context due to its ever-evolving nature. Thus, the elicitation process that stores, manages, and transforms knowledge in a cyclic manner is understood as Knowledge Management which is central focal point. Moreover, KM for cybersecurity domain should have well defined objectives and measures to assess the effectiveness of KM capabilities. Almost all large organizations invest considerably in digital and IT solutions, and specifically in analyzing challenges and risks that can be faced by any organization. The data analytics can be an enabler of superior performance and act as a facilitator to leverage these capabilities. This study will also help in finding practical solutions in implementing effective cyber security and in building better knowledge management infrastructures.

Considering Significance of Knowledge in a Cyber Space Scenario

The digitized world today, which is established on network of internet-enabled systems, is vulnerable to the risk of losing data integrity in the cyberspace. As a strong protective shield, Cyber threat management demands an integrated cyber risk identification and management approach to address and mitigate the cyber security risks and threats in the cyber space. Configuring an effective threat defense mechanism also deals with data acquisition and leveraging automation. Also, depending on the domain in which organization is working, relevant analytics and cross correlation across the vast domains of Cyber security can be analyzed in context to technological advancements.

Considering illustration in this given diagram (Figure 3); the progressing learning evolution shows transition of raw data into the most critical form of evolved data as wisdom. We realize evidently through this info-graphic representation that wisdom is the knowledge applied in action.

The transformation is resulting in better version of data after iteration of the depicted steps, with context and relevance that can be applied using innovative approaches to manage the knowledge intensive environment.

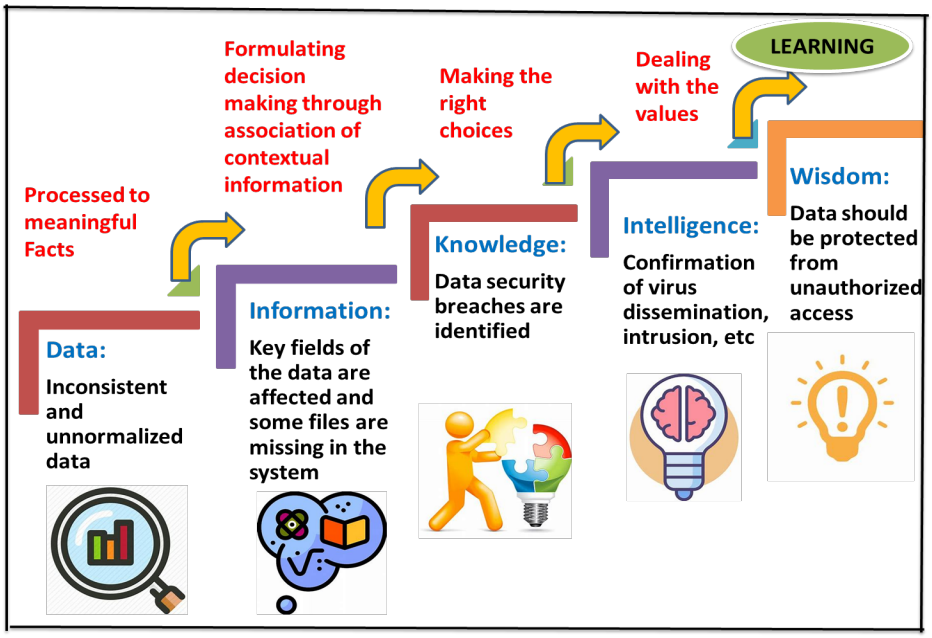

Figure 3: Model of Learning Evolution and Locus of The Knowledge
(Figure Template Adapted from Shikhare, 2013)

Data, information, and knowledge are comprehensively used interchangeably, although they differ in their context and nature of usage that gets it a different form rising its relevance and utility. The researchers attempted to comprehend the progressive data with reference to the cyber wisdom which is evolved being depicted in this info-graphic representation with intuitive illustration in the above diagram (Figure 3) Model of learning evolution and Locus of the knowledge.

A framework is often used by cyber security teams in any organization to manage the life cycle of a threat to identify and respond to it with speed and accuracy. A smooth integration between people, process and technology in the cyber threat management is an important aspect to continuously identify the risks beforehand and stay ahead of potential threats. The under researched areas include: faster threat detection with lower risks to intellectual assets and reliable investigations at regular intervals with optimal response time. On one side, ongoing digitization of business processes is giving many benefits, at the same time it is posing cyber threats and challenges in the digital world on the later part. To secure the confidential assets and to maintain the integrity of data, appropriate security policies and mechanisms should be implemented and refined from time to time to address upcoming new types of cyber threats and challenges effectively. An effective Cyber threat management has the potential for continuous improvement. This can be achieved through a built-in strategic plan with innovation and process measurement with the help of data analytics and reporting mechanism in the emphasized KM environment.

Cyber threat management is important to organizations to understand, aggregate and resolve the potential cyber security challenges that need closer attention in context to new emerging data risks. Nevertheless, it demands the collaboration between employees, business process and technological advancements, giving organizations the valid opportunity to detect threats in early stage and respond immediately with the aid of certain analytical tools.

Exploring Data Analytics as a Tool in Enhancing the KM Capabilities

In the fast-paced world today, several organizations desire to use the available and evolving data for gaining strategic advantage and they are geared up for competing by making best use of analytics. Past two decades has witnessed Knowledge Management term being coined and widely used in the highly data-oriented environment, wherein huge data is evolved and disseminated. Moreover, businesses are highly evolved based on knowledge-based economy, which is so dynamically affected by several factors within and outside a business enterprise. As we can see the Covid19 pandemic today has completely ruined the global economies, across all the sectors; cyber threats have emerged as additional challenges that is further hampering the broken systems. The churning of knowledge that is the core of the organization has tremendous potential to either elevate or collapse any system (if not configured and managed); and thereby threaten an empire of business in the context of this competitive realm of business ecosystems.

Recent studies (Moon and Lee, 2014) have concluded that culture and knowledge sharing processes contribute to knowledge management (KM) effectiveness. Business organizations view knowledge as their most valuable and strategic resource for achieving sustainable competitive advantage (Davenport and Prusak, 2000). There have been inhibitions to share knowledge due to the behavioral factors on various levels of knowledge elicitation; causing hindrances in utilizing its fullest potential of KM capabilities for the growth, business development and sustainability.

Understanding Knowledge Management Capabilities

To compete effectively, firms must leverage their existing knowledge and create new knowledge that favorably positions them in their chosen markets. In order to accomplish this, firms must develop an ‘absorptive capacity’—the ability to use prior knowledge to recognize the value of dynamic information, assimilate it, and to apply it to create new knowledge and capabilities.

(Gold, Malhotra and Segars, 2001) have developed a model of km based on the capability’s perspective. They referred to knowledge infrastructure capabilities and knowledge process capability to achieve organization excellence. Wherein, further knowledge infrastructure capabilities can be considered from three key infrastructure capabilities—technical, structural, and cultural—that enable the maximization of social capital (intangible capital). The researchers have taken the traces from this model and attempted to put forward adaptive model of km capabilities adding innovation as another strategic capability; based on the strong deliberation of cyber threats and challenges. The km cyclic process model itself is mapped with the second part of the proposal relating to knowledge process capability.

Furthermore, in this paper the researchers have also thought of data analytics as a probable tool to address the challenges stated so far in this paper; as it is observed that huge data is being churned worldwide in this digital era. The classic reference would be the drives in Indian context such as Digital India, Make in India, Atmanirbhar Bharat which is enabled on the pillars of digitization literacy among the citizen. Here we cannot ignore that while being part of these drives, common man has now realized about the inevitable need for; both cognizance as well as usage of digital technologies. Nevertheless, the common man is now recognizing the need and importance of being part of the cyber space with more wisdom and caution in this world of connecting people with internet enabled organizations.

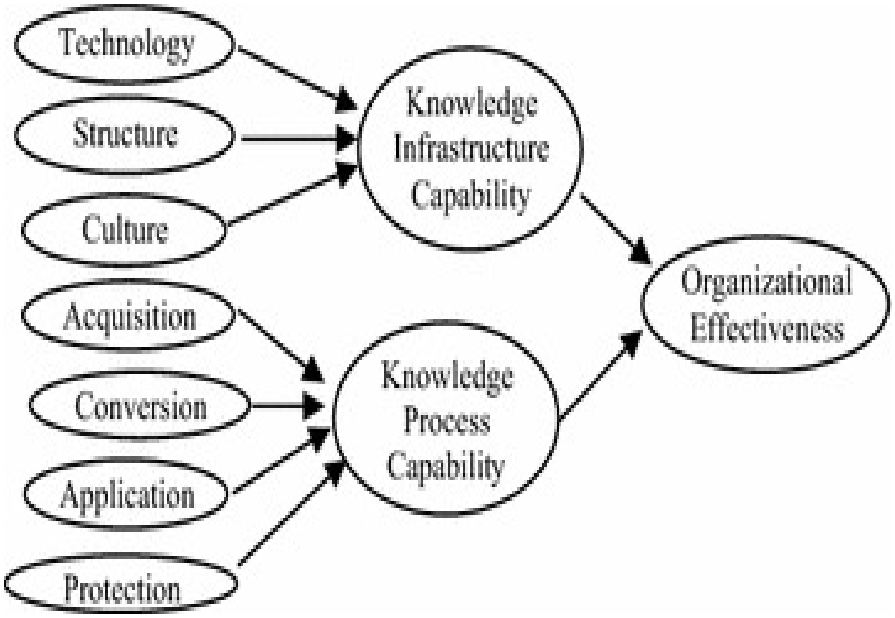

Figure 4: Model of Knowledge Management based on Capability's Perspective
(Source: Knowledge management capabilities and organizational effectiveness; Gold, Malhotra and Segars, 2001)

In context to Indian scenarios, the self-reliant India [Atmanirbhar Bharat], Digital India and Make in India are the drives envisioned to support India innovators and business leaders including startups and big organizations. To make India a global technology superpower, digital literacy has been introduced to a citizen that includes awareness about electronic commerce, electronic governance, mobile commerce, and use of technology for services and business management. If we take a closer look at the progress, current status and challenges of these initiatives, a common man has been benefitted bringing a measure of digitization in every aspect of life; right from education, finance, trading, marketing, managing resources to commerce and governance. These initiatives were meant for reviving the infrastructure for the sustainable self-reliant growth and for identifying the challenges faced by business leaders and organizations.

The need and importance of being a part of a cyberspace gave rise to being more cautious and aware about the cyber threats and challenges while using digital technologies. The number of internet subscribers is increasing day any day worldwide and it is a clearly identifiable and visible indicator of digital transformation happening across the globe. As a result of increased usage of smart phones and internet enabled devices, huge data is at the disposal of cyber offenders, resulting in cyber threats are also emerging at a huge speed. The role of social media platforms, wireless technologies with high bandwidth, internet service providers, and private sector companies like Google, Facebook, Reliance Jio, etc. cannot be ignored in the worldwide digital evolution.

In order to manage the dynamic data and the cyber threats and challenges the new component proposed by researchers as Innovation, can play significant role. It can be noted that this innovation in the form of strategic capabilities of Knowledge management can be used to mitigate the risks of cyber threats and deal effectively with the challenges at all the levels of organization. The analysis of data flowing from and into the organization should be studied in an innovative way, so that a strategy can be built for the sustainable growth of an organization in this highly competitive and fast-growing technology driven cyber space.

With this rapid growth of both Internet and digital world around, traditional Knowledge management systems and its capabilities may fall short to manage the real time highly volatile data churning, as there would be newer lethal cyber attacks that can as well keep on rising. Advancing internet connectivity and competition across market players, high speed network dependencies, mobility of information is happening at rapid pace. In parallel, we see remarkable growth of various social media platforms, data capturing technologies, etc. giving a tenacity to propose improved capabilities of techniques, tools, technologies, and methodologies.

Big data and data analytics these days have come a long way proving effective in managing both data storage utility, security, and the data integrity requirements in the real time. To elevate the business performance among the several factors to seize the upcoming opportunities and curtailing the threats; moreover, deal it strategically in the real world becomes the stepping stone of all the levels of organization. The small and medium size companies

are also using business analytics today as a business decision making tool not only to enhance business operations and managerial efficiencies but also to improve the customer experience in the competitive marketplace (Rajagopal and Ramesh Behl, 2016). May it be micro or small startup or a well-established matured techno giant, flourishing their business on the planet; every enterprise should be built up on a framework strengthened by Knowledge Management capabilities.

In the given current scenarios, we find data in several variants extensively used and progressively transformed within business systems and heterogeneous environment. It becomes need of the hour to cater the customized requirements and transmitting constraints over World Wide Web (WWW); making it a strong case to apply the data analytical abilities strategically. This foundation gives a thrust to basis the decision-making process elevates business performance and thereby achieves business excellence in a long way. It is obviously necessary to be proactive in our approach rather than reactive whenever there is a concern of data security infringement and many such breaches. Better approach that is more agile and preemptive in nature, would at the same time demand better and stronger support systems for back end complimented with better tool kit to fetch it as and when it is used. Massive data usage with emergence of better technological advancement and secured storage demand is seen; and these systems overall would be more prone to the risk of cyber attacks.

We all see today that Internet is anchoring decision making process in core business activities. More mature and strategic decision-making tools would act as a catalyst to leverage the data creation, elicitation, assimilation, and various other processing and managing needs; in the dynamic environment. Not limited to just IT sector but almost every other non-IT sector as well is having data intensive and data critical processes that demands a new framework of enhancing the existing KM capabilities and blending them with innovative strategic moves. This will facilitate in taking policy decisions that are pragmatic and applying them to gain control over the business with such well thought of architecture, supporting the data security aspect as well. These solutions need to be full proof, agile as well as cost effective and easily integrated in the existing systems in every industry which is nowadays technology driven. And technological advancements are continuous and never-ending phenomenon in the cyber world so is their demand and utility. Such proposals have been put forth by many researchers as to how big data addresses these concerns to improve the cyber security in an information technology enabled environment on a greater extent, by supporting the KM capabilities. Business Analytics and Cyber Security Management in organizations compiles innovative research from international professionals discussing the opportunities and challenges of the new era of online business. (Rajagopal and Ramesh Behl). Business analytics techniques, strategies for data storage, and encryption in emerging markets that are identified and highlighted by the professionals and experts needs to be boosted by further more innovative ideas and value adding frameworks that are more technology driven. Above all, the components of such frameworks need to be measured against the effectiveness of the digital world and thereafter the holistic evolved model be validated for further work and research.

The classic example of measuring effectiveness of digital transformation is work culture adopted worldwide by different sectors for their business continuity during lock down period due to pandemic situation of COVID19. Many organizations are opting for work from home, working remotely partially or in a full-fledged manner. Connecting over online business meetings and taking strategic level decisions using a technology mode at an operational level and increasing productivity by working from home is becoming a new normal. But this has also led to uncertainty of jobs and unemployment, leading to inclination towards committing financial frauds and serious cybercrimes like hacking and intrusions into the corporate companies' private and confidential information.

The increasing cyber threats have given an indication to the organization to really focus on protection of their assets by implanting suitable strategies with the help of innovative policies and mechanisms.

Contribution to the Body of Knowledge [CBOK]

To excel knowledge management capabilities, there is a need to acquire knowledge and skills in the fields of cyber security, data management and strategically managed risk management. Knowledge management capability (KMC) is an organizational mechanism to create knowledge continually and intentionally in organizations (Von, Nonaka and Aben, 2001). In addition, (Gold, Malhotra and Segars, 2001) proposed knowledge management (KM) infrastructural capabilities and process capabilities as direct determinants of organizational effectiveness (Figure 4); they argued that an organization must leverage its existing knowledge management capabilities and apply the knowledge in its operations to sustain competitiveness. Taking clue from this basic work done, the researchers are proposing additional vital components of Innovation comprising Strategy and Policy perspectives to the model of Knowledge Management capability; complimenting the Knowledge Management cycle comprising the cyclic processes powered with data analytics; in context to the research scope of this paper. They intend to take it further

validating the model and considering this effort for their empirical studies in the same area of research study. Here apart from Physical infrastructure and organizational hierarchy the other aspect which is the crucial interface is the technological framework that helps to mobilize the social capital in the process of knowledge elicitation. Information technology is often cited in the literature as an important KM infrastructural capability, enabling or supporting core knowledge activities such as knowledge creation, knowledge distribution and knowledge application. (Gold, Malhotra and Segars, 2001). Considering the research focus on management of the cyber challenges and threats it becomes imperative to have its impetus; both with the outcome perspective on the study undertaken and its influence on the overall Knowledge Management environment considered here in the study. Thus, another important aspect as per the researchers along with Culture, Organization structure and Infrastructure is Innovation which forms the newly introduced fourth component as one more pillar shown in the diagram (Figure 5). This innovation has its scope encompassing the policy and strategic perspectives that may be required to apply as per the framework of Cyber space and as per unanticipated threats that may occur in real time. This results in putting the system into more challenging circumstances, directly compromising the security and integrity of intellectual assets of an organization or at individual level.

Outcome of the research study

The researchers have proposed a conceptual framework, in which they have taken efforts to foresee how data analytics can be an enabler in identifying cyber threats and challenges. To overcome these challenges, exploring solutions in implementing effective cyber security and in building better knowledge management infrastructures is another area where the researchers have been working. The Knowledge Management capabilities namely: [organizational structure (comprising people/teams)] as one pillar; other pillars proposed in the model (refer figure 5) are [infrastructure (comprising physical/technological)], [innovation (comprising strategy/policy span of scope)] and [culture (comprising techno-socio aspects)].

As deliberated (2013) in research study; any Knowledge Management enabled Systems (KMS) implemented within an organization it requires a systematized framework to enrich information management; wherein Knowledge Management acts as a multidimensional mechanism that works at all levels of the business pyramid. This includes self-growth and performance elevation at individual level, peer-to-peer knowledge sharing at group level and diffusing best practices at workplace level which promotes better organization at every functional level. In this context cyber security becomes significantly complex and essential for managing challenges such as loss of data, preventing intentional sabotage, hacking, unauthorized access, intrusions, etc.

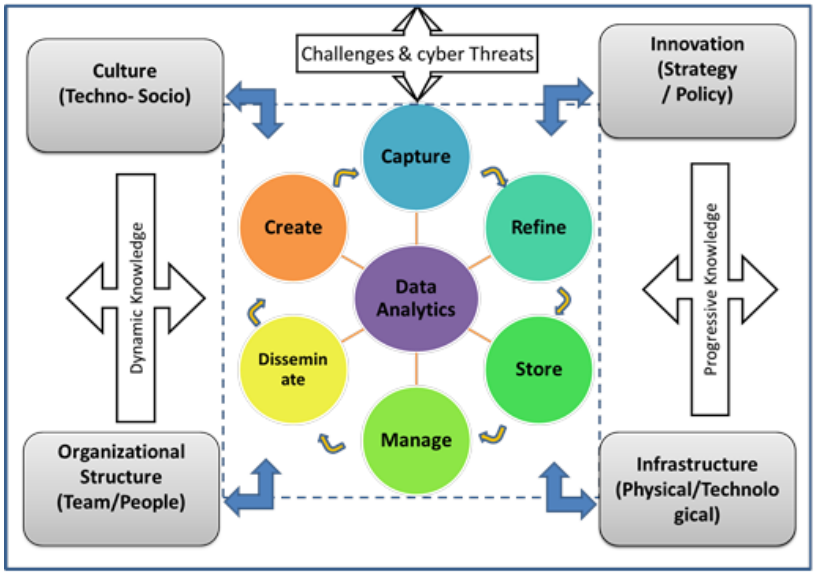

Figure5: Proposed Model: Enhancing KM Capabilities driven by Data Analytics to manage Cyber security challenges and threats (The researchers' original contribution to the body of knowledge)

Utility of the Research Study

A step-by-step systematized effort with innovative approach in applying certain business strategies and polices is recommended. This may prove to be illustrative model for successful integration of the knowledge forms and processes at different levels within an organization. Data Analytical abilities managing the core KM cycle, under the purview of KM capabilities proposed; can be a model not limited to the elicitation process of progressive and dynamic knowledge. This model as well can be a supportive advanced mechanism in dealing the cyber challenges and protecting from cyber threats as it is empowered by Data analytics. Moreover, to sustain competitive

advantage that is affected due to rapid technological advancements, it is becoming crucial for the organizations to empower KM capabilities with data analytical approach. The very nature of knowledge being vibrant, this proposed model addresses the knowledge elicitation process considering cyber threats and challenges and also to regulate progressive knowledge with disciplined data analytics. The data analytics can as well be an enabler of superior performance and to leverage these capabilities, almost all large organizations are seen investing considerably in IT solutions. This data analytics driven approach has given a thrust in analyzing challenges in regulating effective cyber security and in building better knowledge management infrastructures.

Concluding Reflections

World is going to keep advancing and so are the new challenges that threaten the precious knowledge. Thus, such vulnerable data and networks (including extranet and intranet) would need stringent mechanism to address and resolve not only the anomalies but as well defend the cyber attacks. Traditional model may form a basis of any resilient solution that is being proposed. Newer and better routes need to be evaluated and verified complimenting the legacy systems; to address the invading threats to knowledge in the cyber space. Data analytics fostered KM environment, comprising the major pillars of KM capabilities; having strategic innovative support; will keep the KM Cycle in equilibrium.

Techno-socio culture being vital part of corporate environment along with innovation with respect to KM capabilities proposed in this research paper, has a great influence in the cyber space giving impetus to align systems with proper analytics. This has inspired the researchers for the suggestive model that addresses fostering the KM capabilities there by managing the cyber security challenges and threats effectively by virtue of data analytics. This review study formulates the basic building block as initial step, to instigate elaborative research work. This may include validation of the model proposed here; with quantitative analysis and well-defined scope of the further study.

References

Carvalho, Baroni De R. and Ferreira, Tavares M. (2001) "Using Information Technology to Support Knowledge Conversion Processes" Information Research, 7(1).

Chiu, C., Chen, H. The study of knowledge management capability and organizational effectiveness in Taiwanese public utility: the mediator role of organizational commitment; Springer plus 5, 1520(2016).

Ciasullo, V, Montera R., Douglas A. (2022), Building SMEs' resilience in times of uncertainty: the role of big data analytics capability and co-innovation, March 2022

Davenport, H., and Prusak, L. (2000) Working knowledge: How organizations manage what they know. Boston, MA: Harvard Business Press.

Gold, H., Malhotra, A. and Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. Journal of Management Information Systems, 18(1), 185–214.

Jenab, K., Moslehpour, S., Cyber Security Management: A Review, May 2016

Kapur, R.; Knowledge Management, January 2020

Masike, M., Management of enterprise cyber security: A review of ISO/IEC 27001:2022 2023 International Conference on Cyber Management and Engineering (CyMaEn); January 2023

Mittal, Y., (2010) Role of Knowledge Management in Enhancing Information Security IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, ISSN (Online): 16940814.

Moon, H., and Lee, C. (2014). The mediating effect of knowledge sharing processes on organizational cultural factors and knowledge management effectiveness. Performance Improvement Quarterly, 26(4), 25–52.

Obitade, P.O., Journal of Big Data 6(1) August 2019

Rajagopal,(Mexico and Boston University, USA) and Behl R. (International Management Institute Bhubaneswar, India) (2016), Business Analytics and Cyber Security Management in Organizations.

Sandor, A., Tonţ, G. (2016); Considerations Regarding the Inclusion of Cyber security in Knowledge Management June 2021 International conference knowledge-based organization 27(1):231-236

Shikhare, R. (2013) Ph.D. Thesis– "Application of enterprise knowledge management in HRD: A Comparative analysis of the selected companies in IT sector in and around Pune, Savitribai Phule Pune University, November 2013.

Samtani, S., Zhao, Z., Krishnan, R. (2023); Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence, Information Systems Frontiers, February 2023.

Von, G. Nonaka, I, Aben, M. (2001); Making the most of your company's knowledge: a strategic framework. Long Range Plan 34:421–439.

Wang, C., Integrating Data Analytics and Knowledge Management: A Conceptual Model, Issues in Information Systems Volume 19, Issue 2, pp. 208216, 2018.

Wang, Y. and Wang, Y. (2016) Determinants of firms' knowledge management system implementation: An empirical study. Journal of Computers in Human Behavior, 64, 829-842, November 2016.

Zwilling, M. Klien, G. Lesjak, D and Wiechetek, L. (2022) Sklodowska M., Cyber Security Awareness, Knowledge, and Behavior: A Comparative Study Journal of Computer Information Systems 62(1):82-97; January 2022.

