MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

Emerging Global Cyber Security Trends in Sustainable Business Practices

Dr. Saroj Rani, Dr. Sonal Babbar and Dr. Jyotsna

Abstract

Newton's law can be adopted in a fitting manner when it comes to cyberspace. The reaction from adverse groups who are a source of cybercrime seems to use the internet faster than the productive groups such as business firms, governments and Netizens. The e- way of life across continents said to be IT revolutions which lead to great boom of business and relations among nations. Besides the applications of business analytics in assessing the market trends and forecasting, use of Internet in business has enhanced the cyber threats despite the opportunity of being omnipresent on the global platform. Hackers use frequently the global network to steal vital business information and bow companies to compromise on various businesses issue. Thus, organizations today have to rethink their defenses and move from reaction to anticipation. Managing information security is a more complex issue than the technical challenges. The information management is built on the critical infrastructures, organization, and technology. Security lapses are management failures more than technical failures. Recent research shows that corporations worldwide are losing hundreds of billions of dollars annually from the loss of Intellectual Property, trading algorithms, destroyed or altered financial and consumer data, diminished reputations, as well as risking increased regulatory and legal exposure. And, the situation is getting much worse. Finally, the economics of cyber security favors the attackers. Cyber attacks are relatively cheap and easy to access. The attackers' business plans are expansive with extremely generous profit margins. Meanwhile, defense tends to be a generation behind the attackers. There legal instruments punishing the cyber criminals seem to have forum non-convenes and there is complex situation across jurisdictions in penalizing and containing the cybercrime. This paper is an attempt to examine the risk posed by cyber threats to business. The necessity of business firms to face up to the threats of cybercrime? And also to find out mechanisms to improve cyber security and create awareness; Efforts to improve cyber security must be able to adapt rapidly to emerging threats, technologies, and business models. There is a need for cyber security as e- business booms across the globe because of not only conducting the business affairs but also to protect the state and people of the globe.

Keywords: ***Cyber laws, Sustainable business, Intellectual property.***

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

Introduction:

There are numerous cyber threats plaguing global organizations. Commercial and personal data are increasingly migrating to global, interconnected technology platforms. The usage of access data and systems increases through interconnected ecosystems which expands cyber threats risks proportionately. We do not know the scale and impact of cyber threats paralysis. To make structure for cyber resilience decisions and investments by Organizations struggle. There is a lack of measuring the quantity of cyber threats, curtailing the ability to make clear strategic decisions concerning optimal access and investment levels. Cyber risks due to uncertainty reduce global scale technical and economic development. Now there is an unsteady ecosystem which lacks collaborative controls and safeguards emerging surrounding proliferating digital access and also lack of proper guidance and delay of adoption of new technological innovations due to limited understandings of required action taken to counteract a danger or threat. Systematic lack of resilience required substantial actions from stakeholders across the shared digital ecosystem. A shared context for cyber resilience needs to be clarified for organizations to adapt to and counter continually evolving threats.

Cyber security tends to emphasize the type of attacker and the methods used in the attacks. A shift in business relevance and response effectiveness can come from adding a focus on assets (both digital and physical) and building cyber use cases at the intersection of all attackers, type of action (attacks) and assets at risk.“Cyberspace has grown phenomenally and interconnected global digital infrastructure. It includes the Internet, computer systems, hardware, software and services, and digital information.” Collectively, cyberspace has brought unprecedented economic growth, opportunity, and prosperity. It is the nervous system of today’s economy - most of our major economic institutions would not operate without it but it enables e-commerce, e-government, information sharing, and trade. The commercial Internet of the annual global economic benefits equal to $1.5 trillion. Cyberspace’s underlying information technologies (IT) have automated entire economic sectors such as finance and manufacturing and continue to create whole new industries and markets. Today’s cyberspace technologically the connectivity , devices and uses of today’s cyberspace includes computing tables, home networks, smart meters, cloud computing and social networks. Young generations view social networking and online collaboration as parts of their daily lives.

As a new crime opportunities through the interconnected, global, and digital nature of the cyber infrastructure has presented bad actors. Cyber- based transactions and activities have to occur

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

these security practices to counter these opportunities but industry and governments are aligned in this area. The secure digital infrastructure is wanted across all industry sectors for commercial transactions, therefore all IT companies are now making new hardwares, software and services to enable a secure infrastructure and recognize the need for trust in their technologies and services. Cyber security is a board-level risk management issue. A loss of intellectual property or a breach of systems resulting in a loss of consumer, partner or supplier data, or the failure of the provision of a core service of the company can cause significant reputational, brand, monetary and/or regulatory loss. It is a risk that needs to be managed. Besides the applications of business analytics in assessing the market trends and forecasting, use of the Internet in business has enhanced the cyber threats despite the opportunity of being omnipresent on the global platform. Hackers frequently use the global network to steal vital business information and bow companies to compromise on various business issues. Thus, organizations today have to rethink their defenses and move from reaction to anticipation. Managing information security is a more complex issue than the technical challenges.

This paper examines why unconscious compliance poses a risk to business and how to facilitate an innovative and constructive discussion on how governments, businesses and society can prepare themselves for the ever increasing integration of the digital economy in the physical world.

The tripartite relations between state, firms and consumers are in different phases. The online contract is completely different from the contract which has been ruled by *Lex Mercatoria* principle. The UCC model of the USA and the UN or UCP model followed by the Commonwealth and other nations are in different position to deal with the cyber related issues in their jurisdiction.

The following questions are outcomes of prima facie problems arise in cyber space:

1) Who “owns” cyberspaces which are netted with company? Is there a cross-functional team in place for risk management, enforcement and response?

2) Has the company identified its “crown jewels,” and what IP deserves priority protection?

3) Are there security and privacy policies in place, and are they updated and enforced?

4.) Has the company experienced cyber threats in the past? What is the history of nontrivial cyber threats?

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

5.) What about employee training, communications and enforcement? Does the company prioritize cyber?

6.) Does the company have cyber insurance? What's covered, and is it sufficient?

7.) Is the company using existing best practices like the NIST Framework, ISO or some hybrid—if not, why not?

8.) Are business unit leaders responsible (and accountable) for cyber in their departments? When they plan new services or products or infrastructure, do they account for cyber risk? What are its current and past possible liabilities for cyber incidents?

9.) Does the company participate in public-private partnerships for cyber in their industry? What is its relationship with cyber law enforcement?

10.) Does the company understand cyber threats and their consequences on current and planned businesses?

To Address the ever-growing issues that arise out of cyber space/cybercrime, the global consensus is important. The bad actors in every nation who produce cyber threats make global threats because of the complex business relations. The sovereign power of the nations is under attack. But at the same time there is a huge responsibility of the global community to fight against cyber threats.

Literature Review:

The cyberspace is vulnerable to threat and attack. It is space less and e -prone issues such as loss of sovereignty and erosion of jurisdiction is rampant.

The Internet is an almost organic mix of actors and their machines, a wide ranging scheme of government and process of making decisions of private, nonprofits and for-profits. One of such example is "Zombie PC Army Responsible for Big-Name Web Blackout" sounds like a headline from a bad Hollywood B movie when instead it means that computer users could not access the websites of Apple, Google, Microsoft and Yahoo because a Trojan horse program – which belongs and placed secretively on thousands of personal computers these machines under the control of their cybermaster of zombie computers, – launched and attack at a same time on a key piece of the domain name system infrastructure (*Lemos and Hu 2004*).

The cyberspace where traditional law enforcement techniques to crime and wealth- transferring activities are difficult to apply therefore Private security expenditures are important given the

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

decentralized nature of the Internet. There are certain difficulties related to cyber attack such as to identify who is responsible for cybercrimes, arising difficulties from large volumes and inchoate nature of cybercrimes and also associated with punishing judgment- proof individuals.As a consequence low probability of punishment, small size of the sanction of punishment occurs and also low penalty and less fear of consequences. **(*Becker 1968*).**

The issue of optimal openness has become newly important as the Internet and related technologies have made it seem inevitable that information will leak out. Sun Microsystems CEO Scott McNealy received considerable press attention a few years ago when he said, "You have zero privacy. Get over it" (*Froomkin 2000*).

80 percent spam may arised or estimates from zombie machines by taking prominent websites. Those spam are the best way for a malicious computer programmer to seek fame , but these spam in which the day-to-day computer experience is degraded by our shared network decisions. **(*Sandvine Inc. 2004*).**

The cyber space activities that mostly depend on communication which can be done through cyberspace infrastructure gives rise of terrorism as one type of asymmetric and distributed warfare has one of the threats for gains derived from cyberspace. To reap benefits from cyberspace Individuals and governments wish to ensure that cyberspace controls will not be turned against them because their enemies see cyberspace as a high-value target. A one of the example is Al Qaeda's reign in Afghanistan as it developed one of the academy of cyber terrorism so that they can attack the cyberspace infrastructure of the West **(*Gellman 2002*)**

Objectives:

1.) To study why every company needs to face up to the treats of cybercrime?

2.) To assess why unconscious compliance of cyber security poses a risk to business?

3**.)** To examine why private sector often limits its involvement on cyber issues to government-initiated workshops and discussions?

4.) To analyze Economic and social collaboration between the public and private sectors is lacking for cyber issues?

5.) To facilitate an innovative and constructive discussion on how governments, businesses and society can prepare themselves for the ever increasing integration of the digital economy in the physical world.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

Hypothesis:

H1: Cyber security must properly reflect the borderless, interconnected, and global nature of today's cyber environment.

H2: Companies that have unconscious compliance with cyber security pose a risk to business.

H3: Cyber security must focus more on Threats and bad actors directly.

H4: Cyber security must focus on awareness.

Findings:

1.) Cyber security must properly reflect the borderless, interconnected, and global nature of today's cyber environment.

Cyberspace is a global and interconnected domain that spans geographic borders and national jurisdictions. To support the growth, operation, maintenance, and security of this domain, information technology (IT) companies continually innovate and invest in the development of globally deployable products and services. Cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - seek a consistent, secure experience in cyberspace.

Efforts to improve cyber security should reflect cyberspace's borderless nature and be based on globally accepted standards, best practices, and international assurance programs. This approach will improve security, because nationally focused efforts may not have the benefit of the best peer-review processes traditionally found in global standards bodies, because proven and effective security measures must be deployed across the entire global digital infrastructure, and because the need to meet multiple, conflicting security requirements in multiple jurisdictions raises enterprises' costs, demanding valuable security resources. This approach will also: 1) improve interoperability of the digital infrastructure, because security practices and technologies can be better aligned across borders; 2) permit more private-sector resources to be used for investment and innovation to address future security challenges; 3) increase international trade in cyber security products and services that can be sold in multiple markets; and 4) allow countries to comply with their international commitments, such as the World Trade Organization (WTO)'s Technical Barriers to Trade Agreement (TBT), which calls for non-discrimination in the preparation, adoption, and application of technical regulations, standards, and conformity assessment procedures; avoiding unnecessary obstacles to trade;

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

harmonizing specifications and procedures with international standards as far as possible; and the transparency of these measures.

The IT industry is actively involved in developing globally accepted cyber security standards, best practices, and international assurance programs. Some key examples follow: U.S. IT companies contribute to global cyber security standards development through the International Organization for Standardization (ISO), Organization for the Advancement of Structured Information Standards (OASIS), Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and numerous other organizations. The U.S. Government, and foreign governments work to implement, improve, and expand the Common Criteria for Information Technology Security Evaluation (CC), the international standard (ISO 15408) for computer product assurance security certification. The CC is both the ISO standard and a multi-lateral agreement - Common Criteria Recognition Arrangement (CCRA) - among 26 countries including the U.S., Japan, the UK, Australia, Germany, Korea, and India. The governments of different countries participate in bilateral and multilateral efforts to facilitate international government-industry cooperation on global cyber security best practices. Examples include bilateral critical infrastructure protection (CIP) forums between the U.S. Government and our trading partners including Japan and the EU, and the Congressionally mandated biennial Cyber Storm exercise series run by the Department of Homeland Security (DHS), which is designed to test and improve communications, policies, and procedures in response to various cyber threats.

2.) Companies that have unconscious compliance with cyber security pose a risk to business.

Experts explored how legal and regulatory frameworks for protecting personal data and privacy could enhance trust in the use of the Internet and combat cybercrime. UNCTAD had conducted a mapping exercise that had found that 107 countries, including 51 developing countries, had in place data protection and privacy legislation, while 117 countries, of which 82 were developing and transition economies, had enacted cybercrime laws. One of the main challenges in developing cyber legislation was to strike a balance between data protection, and ease of data flow and freedom of information. There were new complex issues to contend with, including some alleged outsourcing of security functions aimed at circumventing data privacy restrictions in certain jurisdictions. Data protection laws were sorely needed in many developing countries. To ensure data protection, cyber security measures should adhere to the

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

"does no harm" principle. One panelist proposed that Government and private sector stakeholders should apply the principle to achieve a just balance between government surveillance of data for cyber security reasons and data privacy. Without such safeguards, countries risked defeating the purpose of cyber security by undermining encryption standards, exploiting back-door vulnerabilities in infrastructure and applications. Some positive initiatives to enhance cyber security were already under way, in the form of public–private partnerships and the harmonization of legal instruments. One expert noted that business organizations were increasingly falling victim to cybercrime. Cross-border cybercrime affected international trade and was difficult to investigate and prosecute. The United Nations Office on Drugs and Crime (UNODC) cybercrime repository had recently been set up to enhance international cooperation on cybercrime by compiling case law and lessons learned relevant to data protection. Identity and data theft, phishing, hacking of personal e-mail accounts and cyber fraud undermined the adoption of e-commerce and consumer trust in digital finance and mobile money. While some African Governments had put in place cyber security policies, data protection and electronic transaction legislation, and had set up computer emergency response teams, they faced significant implementation obstacles. These included a limited understanding of cybercrime and ineffective coordination among stakeholders and enforcement. In addition, cybercrime was increasingly linked to other transnational crimes, such as terrorism, human trafficking and money laundering. Other countries provided for extraterritorial jurisdiction in cases of cybercrime, but had in practice been unable to obtain electronic evidence from outside its national borders. Several experts recognized the difficulty of investigating and prosecuting cybercrimes. Some noted that law enforcement agencies needed more training to deal with cybercrime and appealed to relevant international organizations to consider this when supporting e-commerce and law reform. To strengthen enforcement, the UNODC cybercrime repository would benefit from contributions from multiple stakeholders to improve its scope and coverage. To this end, UNODC was encouraged to increase its presence in multi-stakeholder meetings that discussed cyber law and cyber security. Where critical ICT infrastructure was privately owned, Governments faced an additional challenge in ensuring its safety. The private sector had a level of responsibility that could be defined in the context of public-private partnerships. Such partnerships were particularly important when countries set up computer emergency response teams.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

3.) Cyber security must more directly focus on bad actors and their threats.

Cyber security means understanding and mitigating threats in addition to vulnerabilities and consequences. Cyberspace, with its global connectivity, poses considerable challenges to those tasked with protecting it. The breadth of criminal activity and number of bad actors make getting ahead of the actors and crafting responses to incidents difficult. At the same time, we must acknowledge the analogies between the off-line and on-line worlds. These are traditional actors and crimes - the difference is the medium - and there are traditional laws and government bodies that have long been tasked with dealing with them.

4.) Efforts to improve cyber security must focus on awareness.

Cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - need to know how to reduce risks to their property, reputations, and operations. However, many stakeholders are not aware of and also do not adequately utilize the range of tools available to them to do so, such as information sharing, risk management models, technology, training, and globally accepted security standards, guidelines, and best practices. Raising awareness so that cyberspace's stakeholders can use these tools is critical to improving cyber security.

There are a variety of effective information technology (IT) industry and government efforts to raise cyber security awareness. Some key examples follow.

1.) U.S. IT companies founded the National Cyber Security Alliance (NCSA), a non-profit organization focused on conducting cyber security education and awareness programs. NCSA has become the premier cross-sector umbrella organization for public-private collaboration to increase cyber security awareness at home, school, and work. NCSA is also a lead partner, with the Anti-Phishing Working Group (APWG), in the "Stop Think Connect" national awareness campaign with the Department of Homeland Security (DHS). The Federal Trade Commission (FTC)'s On Guard Online program provides practical tips from the federal government and the technology industry to help citizens to guard against Internet fraud, secure their computers, and protect their personal information. EDUCAUSE, a nonprofit association formed to promote use of IT to promote advanced higher education, provides extensive information and resources on cyber security for the higher education community.

2.) In 2007, Estonia became the first country to face cyber attacks on its critical infrastructure that warranted NATO's help to protect Estonia. Estonia has now evolved its own cyber

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

security strategy, which has made considerable progress in addressing its security. The Estonian Information System Authority (RiigiInfosüsteemiAme) (RIA) has been assigned to lead its major security policy work with the Department of Critical Information Infrastructure Protection (hereinafter CIIP), Critical Information Infrastructure (CII), the Police and Border Guard Board (PBGB), the Estonian Defence League's Cyber Unit (EDL CU), and finally the Information Technology Foundation for Education (HITSA). Along with these domestic bodies, Estonia is actively engaged with regional and international cyber security policy making.

3.)The Japanese cyber security can be referred to as the one, which is trying to find a balance between all stakeholders 'without creating excessive state control'.x Japan has internationally promoted its own initiatives, such as PRACTICE (Proactive Response against Cyber-attacks through International Collaborative Exchange) and TSUBAME (International Network Traffic Monitoring Project).

4.) India's cyber security policy must respond to multiple challenges that it faces in the cyber world. India's economic growth, as important as cyber security, is dependent on popular access to the ICTs. Second, India's e-Governance, though these are developing extraordinarily, are still limited within a small community of net users, thanks to many reasons including the non responsive e-Governance. Third, India's ever increasing number of internet users is largely untrained and unaware of cyber threats and security responses.

Conclusion:

Governments need a secure global digital infrastructure for similar reasons – economic growth, prosperity, efficiency, and protection - all of which provide tremendous value to their nations' businesses, citizens, and economies. The security guide is required for cyberspace growth that will continue with openness, stability, interoperability, resiliency, economic growth and risk mitigated for its development. In the right policy environment, we can increase security while maintaining cyberspace's overall benefits. A host of tools and approaches are available to consumers, businesses, governments, infrastructure owners and operators, and the IT industry to meet our shared security challenges and goals. the globally accepted security standards, guidelines, and best practices that required tools which include information sharing, risk management models, technology, training and the development.Public policy will play an important role in encouraging the use and improvement of these tools and helping to shape the expectations and actions of stakeholders on cyber security.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

Organizations can provide a focused approach to managing your particular cyber risks, and, in conjunction with technical and audit partners, provide a range of compliance solutions. They should offer training for managers and employees on how to comply with privacy and data protection rules, including counseling related to the cross-border exchange of data and international privacy protection laws. Organizations work directly with executive teams, boards, audit committees and risk management committees to provide timely, real-world guidance on compliance and potential liability issues related to the production, collection, processing, use, distribution, storage and disposal of electronic data; information management policies regarding customer and employee personal information; establishment of cyber security, privacy and data protection protocols; theft, loss and unauthorized use of confidential or personal information; and industry-specific privacy regulations. They also can assist you with allocating oversight responsibility, determining Internet Service Provider responsibilities and addressing insurance coverage matters. Public awareness and basic cyber hygiene efforts need to be improved. With a large population new to the digital space, people are often the weakest link in the Asia–Pacific; therefore a strong public education push is needed. The private sector is a useful vehicle to help improve public cyber hygiene, especially where government efforts are lacking. Partnerships across academia, the private sector, civil society, and government can help pool best practice and address a wide range of common cyber issues.

1.

References:

1. Anas, Omair (2015),"In search of India's Cyber Security Doctrine " Indian council of world affairs
2. Becker (1965),"Crime and Punishment: An Economic Approach", Journal of Political Economy, The University of Chicago Press, Vol. 76 No.2, PP- 169-217.
3. Chen Hsinchun, Roger H. L. Chiang Veda C. Storey(2012), *"Business Intelligence and Analytics: From big data to big impact "*MIS Quarterly Vol. 36 No. 4, pp. 1165-1188
4. Flegel .Ulrich, Flegel. Florian, Miseldine. Philip, Monakova. Ganna, Wacker .Richard, and Leymann .Frank, "Legally Sustainable Solutions for Privacy Issues in Collaborative Fraud Detection" Springer Science+Business Media, LLC 2010

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 33 Issue 1, June – 2023, Pages: 109-120

5. Gellman, Bartom (2002) "Cyber-Attacks by Al Qaeda Feared," Washingtonpost.com, Available from http://www.wahsingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; Accessed 12 Apr 04.
6. Global cyber security and Privacy (2014),"Protecting and promoting cyberspace"
7. Golodner Harold Umberger (2011), "Cyber security: Threat Identification, risk and vulnerability assessment" Springer Science+Business Media B.V. 2011
8. Golodner M .Adam (2014), "The Need for a Holistic Approach to Global Cyber Issues" M&A and Corporate Governance Newsletter.
9. Lemos.R and Hu. J (2004), "Zombie PC army responsible for big name web blackout," CNET News.com (available at http://software.silicon.com/malware/0,3800003100,39121439,00.htm).
10. Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. (2020) Review and insight on the behavioral aspects of cybersecurity. *Cybersecure* 3, 10.https://doi.org/10.1186/s42400-020-00050-w
11. Randel .C. Picker (2004),"Cyber Security: Of Heterogeneity and Autarky", John M. Olin Program in Law and Economics working Paper No. 223.
12. Robert. D. Atkinson, Stephen. Ezell, Scott. M.Andes and Daniel. Castro (2010),"The Internet Economy 25 Years After .Com: Transforming Life and Commerce," Washington DC.
13. Sandvine Incorporated. Trend analysis: Spam trojans and their impact on broadband service providers, June 2004.
14. Information technology industry council (2011),"The IT Industry's Cyber security Principles for Industry and Government" . washington. Version 3.0
15. United Nation Conference on Trade and Development (2015) "Report of the Multi-year Expert Meeting on Cyber Laws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned".
16. United Nations (2023),"Fifty- Two People lost their lives to homicide globally every hour in 2021, says new report from UNODC, Office on Drugs and crime.
17. World Economic Forum (2014),"Partnership for Cyber Resilience towards the Quantification of Cyber Threats" Switzerland.
18. Zadelhoff.Van.M (2016),"The biggest Cybersecurity threats are inside your company", Technology and Analytics, Harvard Business Review.