THREAT FOR "CYBER WORLD WAR", EMERGENCY FOR ESTABLISHMENT OF UNIFIED INTERNATIONAL CYBER LAWS (A STUDY WITH SPECIAL REFERENCE TO WORLD'S HIGH RISK POPULATION)

*Written by **Amarendar Reddy Addula***

Pursuing PG Diploma in Cyber Laws from NALSAR, Hyderabad

Statement of the Problem:

Cyberspace is occupying global common place more than that of land, water, air, space etc. World development is parallel with much advancement in Information Technology consisting web technology, e-commerce, social networking etc. Information Technology has played and playing vital role Globalization. Recent surveys revealed that 40% of world's market are occupied by Online Market witnessing greater share of Cyber Technologies in World Development in reaching faster and easier. Cyber attacks rapidly emerging as one of the most alarming international security threats of global concern. We know that, world cyber technology has widely expanded and playing more than expected role in strengthening respective fields yielded to unbounded businesses ex: Space, Defense, Science, Research, Software, Communications, Banking, Marketing, Shopping, Education, Entertainment, Gaming, Social Networking etc. This has great potential impact on global economy failing international cyber security of almost all nations. Such a top widely used Cyber Technology is dead in means of it's security and it's adverse effects victimizing many innocent international cyber users. This is because, Cyber Technologies having great loop holes in designing, programming and functioning and more particularly utterly failing as neither it could prevent users from breach nor catch such breachers. It is shocking to know that world's best 10 software are under the list of this categorized victims US Department of Justice, Linkedin, Democratic National Convention, Yahoo, World Anti-Doping Agency, Dyn, Adultfriendfinder together puts 2000 million victimization suffering from their personal, private, official and

confidential information. Then thinking about other millions of software, count of victims is behind imaginary. Peace, harmony, security, privacy and justice in cyberspace should be protected by international law and such serious crimes must be established under international law irrespective of state laws. One has to take the responsibility.

"Computer or Cyber crimes are considered as illegal, unethical or unauthorized behavior of people relating to the automatic processing and transmission of data, use of Computer Systems and Networks".

Massive cyber security breaches have become almost commonplace, regularly grabbing headlines that alarm consumers. But for all of the attention such incidents have attracted in recent years, many organizations worldwide still struggle to comprehend and manage emerging cyber risks in an increasingly complex digital society. As our reliance on data and interconnectivity swells, developing resilience to withstand cyber shocks—that is, large-scale events with cascading disruptive consequences—has never been more important. In the 2018 Global State of Information Security® Survey (GSISS), 40% of survey respondents from organizations using robotics or automation say the disruption of operations would be the most critical consequence of a cyber-attack on those systems. Despite an awareness of disruptive cyber risks, companies often remain unprepared to deal with them.

Common types of Cyber Crimes may be broadly classified in the following groups:-

1. Against Individuals:

a. Against Person: i. Harassment through e-mails. ii. Cyber-stalking. iii. Dissemination of obscene material on the Internet. iv. Defamation. v. Hacking/cracking. vi. Indecent exposure.

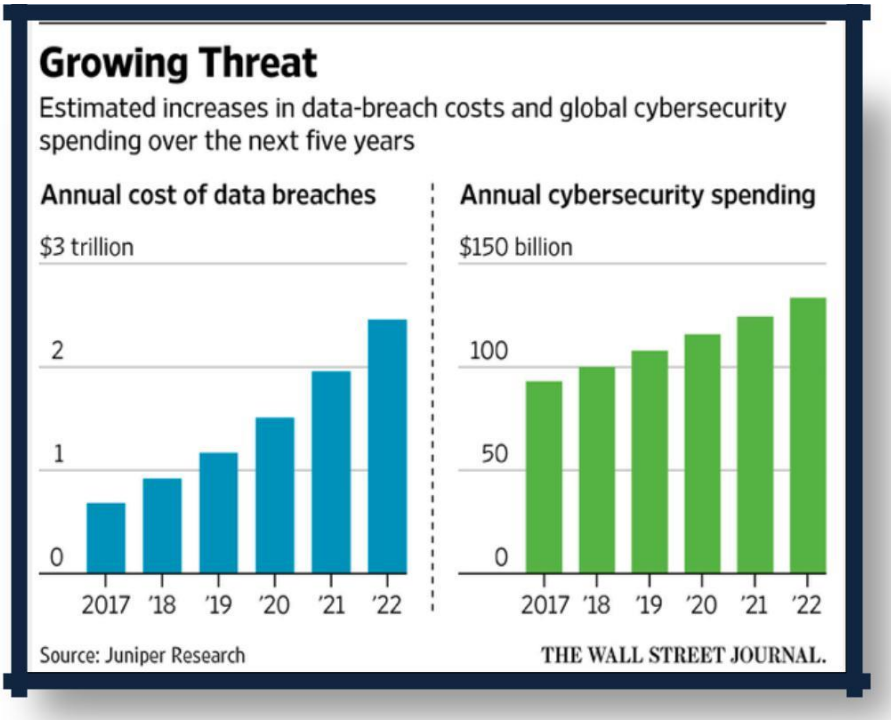
b. Against property of an individual: i. Computer vandalism.ii. Transmitting virus. iii. Internet intrusion. iv. Unauthorized control over computer system. v. Hacking /cracking.

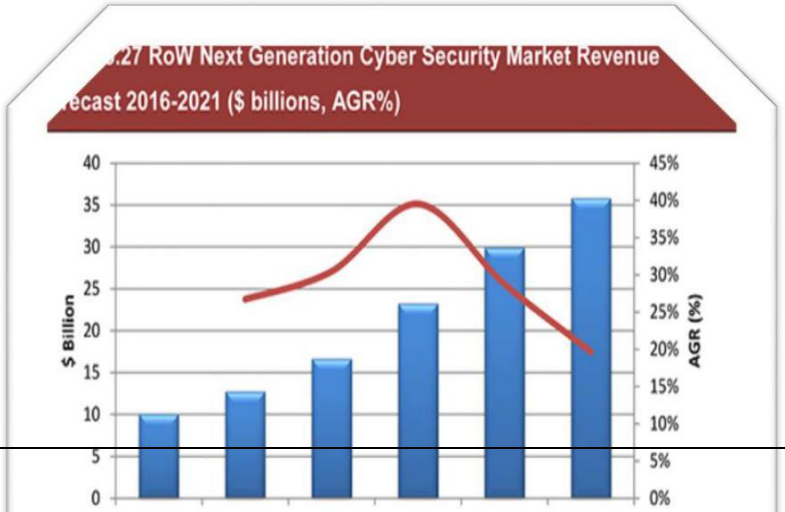
2. Against Organizations:

a. Against Government, Private Firm, Company, Group of Individuals: i. Hacking & Cracking. ii. Possession of unauthorized information. iii. Cyber terrorism against the government organization. iv. Distribution of pirated software etc.

3. Against Society at large: i. Pornography (specially child pornography). ii. Polluting the youth through indecent exposure. iii. Trafficking.

Growing Threat:





The two major findings are here under:

1. "No unified International Cyber Laws, Legal gaps in National Laws, No special Cyber Laws in states"
2. Mere steps by MNC's particularly in the field of Information Technology and relevant to it

Thus, this field is inviting it's evils like hacking, fraud, malware, cheating, privacy less, security less etc. Such victims losing their valuable information on other side countable loss of hard earned valuable money, crime records, murders, suicides, mental disorders, disputes are noticed.

Innocence of a common man, lack of infrastructures, non availability of suitable software, mere knowledge of laws, partial implementation of laws, gaps in international laws are becoming major investment free businesses for International Fraudulent Communities. Interestingly knowing experts' opinion that, 90 % of breaches occur as a result of user clicking on an inappropriate website link.

Let us review the perceptions of few worldwide eminent personalities:

"Russian President Putin & myself discussed forming an impenetrable Cyber Security Unit so that Election Hacking & many other negative things will be guarded" - **US President** Donald Trump on Twitter (08/08/2017 - Silver Chips Online)

“Mutual resignations by 7 cyber security experts working under US President Trump, stated President is not keen on issues related to failures of Cyber Security” – Eeenadu.net 26-08-2017

"**UK Government** proposed 77 Million Pounds to an organization for Cyber Security Failures" - Deccan Chronicle (01/08/2017 - IS Buzz News)

"SHANGHAI - **China**'s much anticipated Cyber Security Law CSL is came into effect from 01-06-2017. MNC's feel the heat. It focus on "Personal Information & Important Data". Approval from regulatory authority is required before transferring the data abroad" - Forbes.com(29/07/2017)

"**Europe** has announced IP Expo 2017 showcase to help organisations and individuals looking to innovate and evolve through cyber technology in October 2017 at Excel, London" - Informationsecuritybuzz.com 25/07/2017

"**Former Advisor to Bill Gates** Mr. Alex Gouneres, CEO to Polyverse company raises $2M for Cyber Security startup" - Geekwire.com 10/05/2017

"In ransomeware attack, where does **Microsoft**'s responsibility lie?" by Newyark Times - Economictimes.com 16/05/2017

"**Cyber Security is Dead**, the top cyber security risks in Asia Pasific in near future" - Forbes Technologies Council on 06/06/2017

“With few accepted rules of behaviour in cyberspace, countries as big as China or as small as Bahrain can be expected to use these kinds of attacks. And they may eventually spill over into real-world military conflicts.” Adam Segal - Sr. Journalist, **UAE** 03/08/2017

"PM Malcolm Turnbell launched **Australia** Cyber Security Strategy in April 2016, still there is lot to be done" - theconversation.com 02/06/2017

“13% of increase in cost per stole of record, 12 % of increase in the total cost of data breach in India” - Venugopal N - Director, **SAARC**, CPST Ltd. - 08/08/2017

"Many people hesitate to share their stories about getting hacked, majorly in **Asian countries**" - William H Saito, Contributor - Cyber Security Innovation, **Japan** 05/07/2017

“In June 2017, hackers believed to be tied to the Vietnamese government stole and released transcripts of the talks between President Rodrigo Duterte of the **Philippines** and **US** President Donald Trump, and between MrDuterte and President Xi Jinping of **China**.” - straitstimes.com 02/08/2017

“By 2025, Cyber Security is poised to become **$ 25 Billion Global Industry**, India needs 10 Lakh employees in Cyber Technology, with estimation of 2.25 Lac Crores rupees with minimum share of 10 % of present IT Industry” - Rama Veda Sri, CEO - Data Security Council of **India** - Eenadu.net 08/08/2017

“50 % increase in mental stress in youth, suicide attempts have increased 3 times in just last 3-4 years in **USA**” - recent survey - Eenadu.net04/08/2017

"It's disadvantage to say that we are from Israel because on of my best friends India PM Modi wants to close cooperation with Israel in Cyber being he has good reason to do so. We strengthening Israel's Cyber Security otherwise serious threat" by BenjminNetanyatu, **Israel** PM in conference Cyber Week 2017 at Tel Aviv University, Jerusalem - Livemint.com 03/07/2017

"**British** computer expert Devon 23 years old, created software harvests bank details and slod it for $2000 and he is released on bail" by **US** prosecutors - BBC.com 05/08/2017

"The hacker delivered a video letter to **HBO** CEO Richard Pleper says - we successfully breached into your huge network HBO, one of our difficult targets to deal with, took 6 months" - Hollywoodreporter.com 08/07/2017

"Digital Drive puts India at greater cyber attack risk" **Russia**n firm KESPERSKY - firstpost.com 07/08/2017

"Hackers lured to American Energy sector using cyber hacking techniques due to lack of sensors and control" - Indianexpress.com05/03/2017

“Amounts being lost on credit/debit cards without receiving OTP’s, I have lost Rs. 2.6 Lacs in a single shot” - Srinivas (Victim), Sr. IT official in a reputed MNC - Eenadu.net 06/08/2017

“World biggest Online Payments organisation formed, Vantip buying worldly for $ 12.1 Billion covering 146 countries with 126 currencies allowed” - **London** Report - 01/08/2017

“The hacking wars are going to be much worse. Reports last month that the United Arab Emirates (**UAE**) orchestrated the hacking of a Qatari news agency, helping to incite a crisis in the Middle East, are as unsurprising as they are unwelcome.” -straitstimes.com 02/08/2017

"Challenges in Cyber Security are evolving on a daily basis. There are new puzzelsro solve them. It's constant learning that keeps the work enticing" by John Kuhn - Manager, **IBM** X Force, Senior Threat Researcher

"Cyber Police arrested a 26 years old man working in Central Paramilitary Force for hacking Indian popular Actress KarrenaKapur Income Tax e-filing account" - DNAIndia.com 03/01/2017

“Wanna laugh: Faced with Wannacry attack, Andhra Pradesh cops unplug systems and save data. 25 % of computer network of Andhra Pradesh Police Department is hacked. Andhra Pradesh Chief Minister Chandrababu Naidu drafted policy, all Government agencies implementing IT projects shall earmark 5% of annual IT budget towards compliance of IT Act 2000” - Newindiaexpress.com 16/05/2017

“Round the clock, 25 % of world youth spending to pass time” - PEW Research Centre, **UK** 29/06/2017

“Maximum Credit/Debit card transactions have been hacked by US and EUROPE countries in VISA/MASTER type cards without generating OTP itself” – Nagaraju, Sr Bank Officer, India (Eenadu – 22-08-2017)

“Department of Information Technology, Government of India has issued notices to Apple, Samsung, Sony, Appo, Micromax, Motorola, etc. mobile manufacturing companies to report on initiatives taken for protection of data” (Eenadu – 22-08-2017)

“Challenges for Cyber security and need of 20 lacs experts in next 4 years” (Eenadu – 22-08-2017)

"Adverse impacts of online games involving nature of gambling, betting, unethical contents victimizing young age group, hence banned in my state by amending laws" – Kalvakuntla Chandrasekhara Rao, Chief Minister – TS, India

Review of Literature

UNO @ Cyber Security

5 July 2017 – Only about half of all countries have a cybersecurity strategy or are in the process of developing one, the United Nations telecommunications agency today reported, urging more countries to consider national policies to protect against cybercrime. Releasing its second Global Cybersecurity Index (GCI), the International Telecommunication Union (ITU) said about 38 per cent of countries have a published cybersecurity strategy and an additional 12 per cent of governments are in the process of developing one. The agency said more effort is needed in this critical area, particularly since it conveys that governments consider digital risks high priority. "Cyber security is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective," stated the report, adding that cybersecurity is "becoming more and more relevant in the minds of countries' decision makers."Last month, a cyber-attack crippled tens of thousands of machines around the world. It is unclear who was behind the attack, prevention and mitigation measures to reduce the risks posed by cyber-related threats can and should always be put in place," said ITU

Geneva, 05 July 2017

ITU, the United Nations specialized agency for information and communication technology, has published the Global Cybersecurity Index 2017 (GCI-2017), which measures the commitment of ITU's 193 Member States to cybersecurity and is the second in this index series.

"At ITU, we are committed to making the Internet more secure, safer and trustworthy, for the benefit of all," said Houlin Zhao, ITU Secretary Generalfive pillars of the ITU Global Cybersecurity Agenda as: legal, technical, organizational, capacity building and international cooperation.

"As the global community rapidly embraces ICTs as key enabler for social and economic development, it is vital that cybersecurity is made an integral and indivisible part of the digital transformation," said BrahimaSanou, Director of the ITU's Telecommunication Development Bureau. "We continue to encourage governments to consider national policies that take into account cybersecurity so that everyone can reap the benefits of the online world."

Secretary-General Houlin Zhao.

The use of force between states is definitively forbidden in International Law since the advent of the UN Charter.This prohibition is also a principle of customary International Law, as noted by the ICJ in the Nicaragua case.163 Nevertheless, there are two undisputed exceptions to this principle: the right of self-defense (Article 51 of the UN Charter) and the collective action by the

UN as decided by the Security Council (Article 42 of the UN Charter). The threat of a major Internet attack is no doubt a primary question of national security. This kind of computer network attack may be defined as a virtual attack, that is, an attack using the Internet as opposed to a physical attack, to a state's Internet infrastructure. The latter broadly understood as the combination of technological systems, connected to the Internet, controlling essential public utilities and national security services.

From the point of view of International Law, the first question to be answered is whether or not a COMPUTER NETWORK ATTACK can be considered a use of force, or even an armed attack and when. Before we try to develop any analysis, it would be good to bear in mind some previous assumptions. As we maintained before with regard to the question of jurisdiction, the location of the attack must be determined according to the "effects doctrine"; that is, what matters is not the physical location of the attacker but where the effects of the attack are felt.

Cyber Laws: A Global Perspective

International Law has played the role of a catalyst between states, solving some issues that affect mainly e-commerce and that require cooperation, i.e. an international response articulated through the application of traditional doctrines of conflict of laws for the problem of free speech and content regulation, international treaties for the protection of intellectual property rights, or some kind of Safe Harbor agreements for the protection of privacy rights. International Law has yet another role to play with regard to the regulation of the Internet. International Law tools and institutions may answer some of the questions that have not been, or only been tentatively, addressed to date. These questions are of an undisputed international flavor, and therefore, only International Law can answer them. International Law should be ready to react mainly to the

possibility of invoking self-defense in the case of a cyber-attack; the likelihood of considering Internet's core resources as part of the Common Heritage of Mankind; and the prospect of regarding access to the Internet as an International Human Right.

Introduction In the today's era of rapid growth, Information technology is encompassing all walks of life all over the world. These technological developments have made the transition from paper to paperless transactions possible. We are now creating new standards of speed, efficiency, and accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used to store confidential data of political, social, economic or personal nature bringing immense benefit to the society.

The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness and enactment of necessary legislation in all countries for the prevention of computer related crime.

Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law-making and law-enforcing authorities find this new environment deeply threatening.

Why is there a need for a separate law to govern the Cyber World? This may also assume significance looking to the fact that the phenomenal spread of Internet has been enabled mainly due to the absence of a centralized regulating agency. Anyone who has access to a computer and a telephone network is free to get hooked to the Internet. This uncontrollable growth of the Internet makes the need for regulation even more badly felt. Systems across the globe have many different rules governing the behavior of users. These users in most of the countries are completely free to join/ leave any system whose rules they find comfortable/ not comfortable to them. This extra flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult for System Administrators to have a check on Frauds, Vandalism or Abuses, which may make the life of many online users miserable.This situation is alarming as any element of distrust for Internet may lead to people avoiding doing transactions with online sites thereby directly affecting e -Commerce growth. The (Mis)Use of Internet as an excellent medium of communication may in some situations lead to direct damage to physical societies. Non-imposition of taxes on online transactions may have its destructive effect on the physical businesses and also government revenues. Terrorists may also make use of web to create conspiracies and make violence in the society. Therefore, all of us whether we directly use Internet or not, will like to have some form of regulation or external control for monitoring online transactions and the cyber world for preventing any instability.

Cyber Legislations Worldwide

To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria,

Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore.

However, no country has fully resolved all the issues such as legal, enforcement and prevention of crime. The legislations enacted by different countries cover only few of the classified computerrelated offences. However, looking to the dynamic and fast changing technology, new types of offences may pop-up frequently. Some of the major types of offences against which many countries across the globe have enacted various Acts (mostly at preliminary levels) are as follows: - 1. Unlawful access to data in computers, 2. Damaging data in computer etc. 3. Possession of device to obtain unauthorized telephone facilities, 4. Unauthorized access to computer and computer material 5. Committing mischief with data. 6. Data spying, 7. Computer fraud, 8. Forgery of prohibitive data, 9. Alteration of data, 10. Computer sabotage. 11. False entry in an authentic deed 12. False entry in permit license or passport 13. Electronic record made wrongfully 14. Electronic record made wrongfully by public servant 15. Interferences with business by destruction or damage of computer 16. Interferences with computer 17. Destruction of public document 18. Destruction of private document 19.Unauthorised access with intention to commit offences/ computer crimes 20.Unauthorised use and interception of computer services. 21. Knowingly access of computer without authorization related to national defense or foreign relation. 22.Intentional access of computer without authorisation to obtain financial information 23. Unauthorized access of computer of a Govt. Deptt. Or agency Knowingly causing transmission of data/program to damage a computer network, data or program or withhold or deny use of computer, network etc. 25. Knowingly causing transmission of data/program with

risk that transmission will damage a computer network, data or program or withhold or deny use of computer, network etc, anunauthorised access of computer with intent to defraud.

REFERENCE TO LAWS

The Draft Statute of the International Criminal Tribunal for Cyberspace (ICTC) consisting 34 Articles majorly working on Competence of International Tribunal and its organization with status, privileges and immunities, Violations of the Global Treaty on Cybercrime, Global Cyber attacks against critical communications and information infrastructures, Preparatory acts on Cyber-crime, Jurisdiction, Non-bis-in-idem, Composition of Chambers and its Officers and members, Rules of procedure, evidence, prosecution, Investigation, Trial proceedings, Rights of the accused, protection of victims and witnesses, Judgments, Enforcement of Penalties and sentences, Review and appellate proceedings, Pardon, cooperation and judicial assistance, Annual Report etc., But sucha detailed draft could not interpret and control massive increase in international cyber crime day to day.

The probability of Security Council of United Nations deciding Cybercrimes to refer a case to ICJ is quite low. The advisory Jurisdiction of ICJ is also worth nothing, in determining whether a cyber attack constitutes an act of aggression or a use of force.

International Law major ruling “NOT TO HARM EACH OTHER” is one of the main reasons for omission of actions against such cyber attacks originated particularly from a state.

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use: Digital Signature within a public key infrastructure Biometric Device PINs Passwords Scanned handwritten signature Signature by Digital Pen Clickable “OK” or “I Accept” or “I Agree” click boxes Information

Security and Cyber Law 33 The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law

A 24X7 mechanism has been envisioned to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for crisis management. Some highlights of this strategy are as follows: Promotion of research and development in cybersecurity. Developing human resource through education and training programs. Information Security and Cyber Law 17 Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cybersecurity initiatives.

US surveillance program PRISM have demonstrated how a legal entity network and computer system outside a particular jurisdiction is subject to surveillance without the knowledge of such legal entitiesU.S. government has declared October as the National Cybersecurity Awareness month

Cyber laws in India Keeping in line with other countries, India also has passed its first cyber law, The Information Technology Act 2000, which aims to provide the legal backbone for enabling e -commerce in the country. However the arrival of Internet resulted in the rise of new and complex legal issues. Though India has a detailed and well-defined legal system in place, with laws like the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on. But at the time of enactment of these laws nobody could really visualise about the Internet. We must remember that all the existing laws in place in India were enacted keeping in mind the relevant political, social, economic, and cultural scenario of the corresponding time. As like the rest of the world, the existing laws of India also could not handle the various cyber space activities. As such the need arose for a Cyber Law.

Salvador Declaration Article 42 to establish to examine the view to examining options to strengthen existing and propose new national and international legal responses to cyber crime.

The international Expert Group had its first meeting in Vienna in January 2011 and made additional remarks that large scale attacks are emerged which are not fully covered in the convention.

In March 2011, Department of Information Technology released a Draft on the National Cyber Security Policy to secure cyber eco-system establishing awareness against threats, legal environment in support of safe and secure cyber peace, adequate trust and confidence in electronic transactions, enhancement of law, protection of IT gateways and networks, 24X7 mechanism for cyber security, management for preventive and protective, response and recovery actions, security technology, Crime prevention, protecting data etc.

In contrast, security complexity and the deployment of disruptive technologies can affect the timeto detect and contain a data breach. Although some complexity in an IT security architecture isexpected to deal with the many threats facing organizations, too much complexity can impact theability to respond to data breaches. Disruptive technologies, access to cloud-based applicationsand data as well as the use of mobile devices (including BYOD and mobile apps) increase thecomplexity of dealing with IT security risks and data breaches. As shown in the research, cloudmigration at the time of the data breach and mobile platforms were shown to increase the cost.

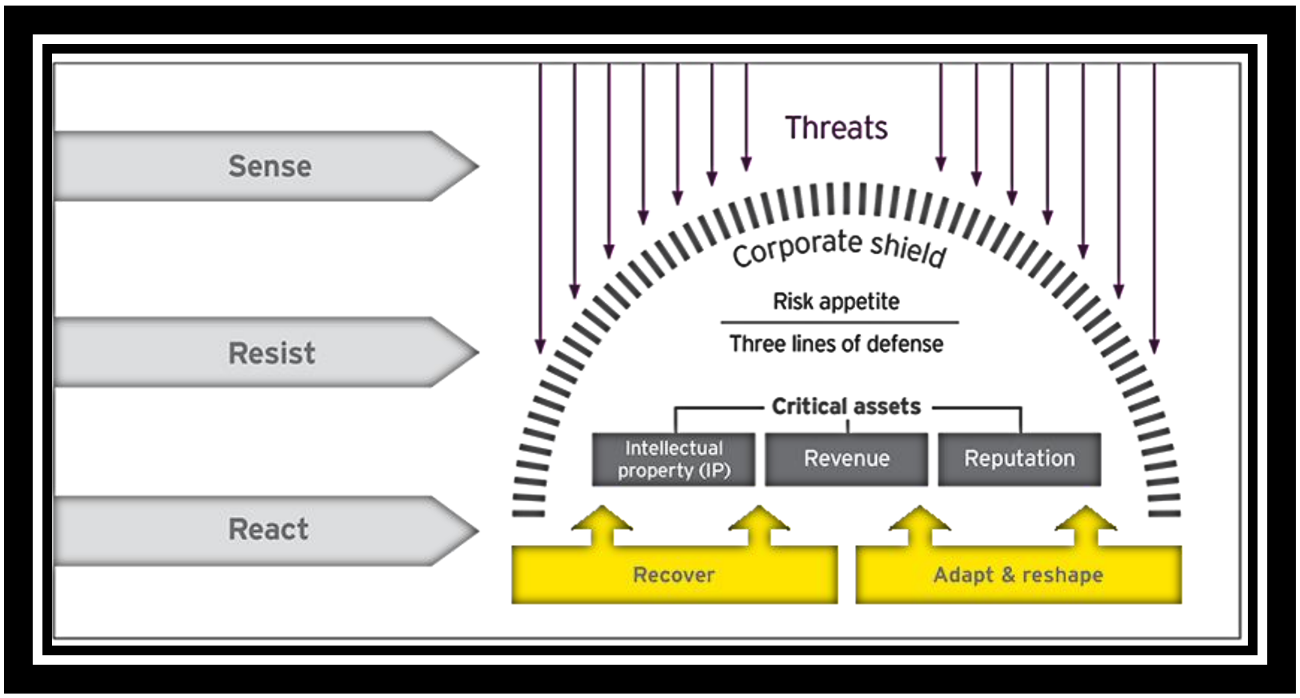
Organizations in Australia, Germany, France and the United Kingdom were able toimprove their ability to keep customers and, as a result, reduced the cost of data breach.Organizations in Australia, the United Kingdom and Germany also were able to limit the number of customer records lost or stolen and, as a result, had lower costs. Whereas, countries in theMiddle East and the United States experienced a higher percentage of churn and had highercosts. Organizations in Brazil, India, the Middle East and South Africa had data breachesinvolving more lost or stolen records, which increased their costs. The individual country reportspresent in greater detail the cost components and factors that affected the cost.

Achieving greater cyber resilience as a society and within organizations will require a more concerted effort to uncover and manage new risks inherent in emerging technologies. Organizations must have the right leadership and processes in place to drive the security measures required by digital advancements.

Many businesses are just beginning this journey: Relatively few respondents (34%) say their organizations plan to assess Internet of things (IoT) security risks across the business ecosystem.

Organizations in certain countries are more likely to have a data breach. Throughout thepast four years, this research has studied the likelihood of one or more data breaches over a 24-month period. South Africa and India have the highest estimated probability of occurrence.Germany and Canada have the lowest probability of a data breach in the next 24 months. Detection and escalation costs are highest in Canada and lowest in Brazil. Data breachcosts to detect and escalate the incident are forensic and investigative activities, assessment andaudit services, crisis team management and communications to executive management andboard of directors. The average detection and escalation costs for Canada was $1.46 million. In contrast, the average cost for detection and escalation for Brazil was $0.43 million.

Notification costs are the highest in the United States. These costs include the creation ofcontact databases, determination of all regulatory requirements, engagement of outside experts,postal expenditures, email bounce-backs and inbound communication setups. Notification costsfor organizations in the United States were the highest ($0.69 million), whereas India had the lowest ($0.02 million).

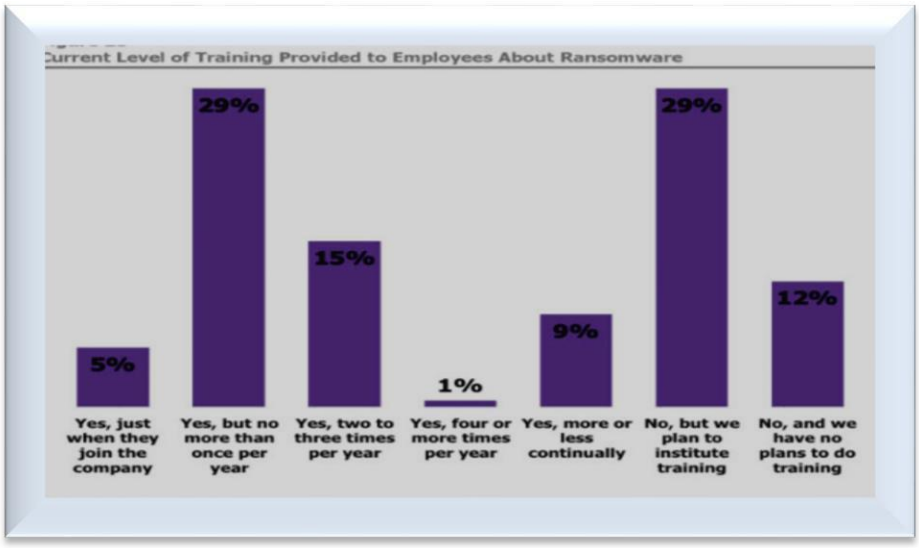


The United States and the Middle East spend the most on post data breach response. Postdata breach response activities include help desk activities, inbound communications, specialinvestigative activities, remediation, legal expenditures, product discounts, identity protectionservices and regulatory interventions. In the United States, these costs were $1.56 million and$1.43 million in the Middle East. Companies in the Middle East and Canada have the highest indirect per capita costs and the United States has the highest per capita indirect costs. The Middle East and Canada had thehighest direct per capita cost (both $81). These costs refer to the direct expense outlay toaccomplish a given activity such as engaging forensic experts, hiring a law firm or offering victimized protection services. The United States had the highest indirect per capita cost ($146). Malicious or criminal attacks target Middle East and U.S. organizations.

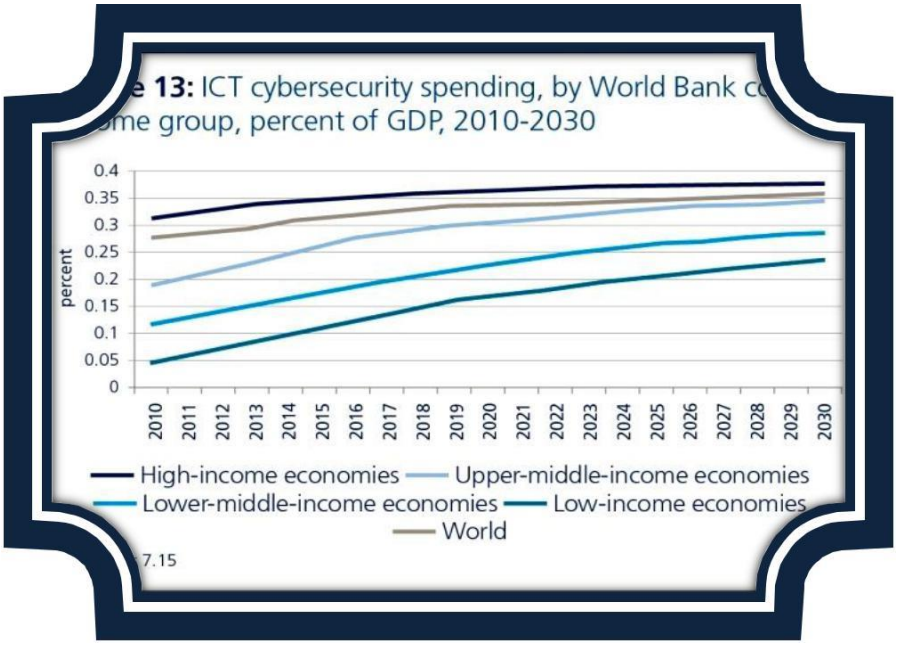
Fifty-nine percent ofbreaches in the Middle East and 52 percent of breaches in the United States were due to hackersand criminal insiders. Only 40 percent of data breaches in Italy and South Africa were due tomalicious attacks. Italian and ASEAN organizations have the highest percentage of human errorat 36 percent and 35 percent, respectively. German and Indian organizations were most likely toexperience a data breach caused by a system glitch or business process failure (34 percent and33 percent, respectively).

Number of exposed or compromised records by country or region. Figure 3 reports theaverage size of data breaches for organizations in the countries and regions represented in thisresearch. On average, organizations in India, the Middle East and the United States had thelargest average number of breached records. Australia, South Africa and Italy had the smallestaverage number of breached records. Later in this report, we show the relationship between thenumber of records lost or stolen and the cost of data breach.

Training provided to employees:

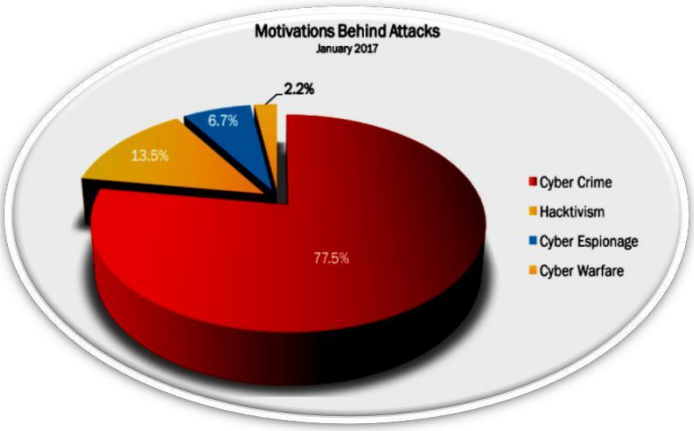


Why the cost of data breach fluctuates across countries



What explains the significant increases in the cost of data breach this year for organizations in theMiddle East, the United States and Japan? In contrast, how did organizations in Germany,France, Australia, and the United Kingdom succeed in reducing the costs to respond to andremediate the data breach? Understanding how the cost of data breach is calculated will explain the differences among the countries in this research.

Motivation behind attacks:



Incidents @ Industry Wise:

INDUSTRY	PERCENTAGE OF INCIDENTS
Financial and Insurance Services	7.55%
Retail / Merchant	0.63%
Education	3.77%
Government	6.92%
Healthcare	42.77%
Nonprofits	1.89%
Other Business	36.47%
TOTAL	100%

Recommendations:

- Establish International Cyber Laws duly states to amend their existing laws enforcing:
- Establishing an International Taskforce for law enforcement, INTERPOL, Financial Industry, MNC's, IT companies etc.
- Establishing an International Criminal Court / Tribunal for Cyberspace as existing International Criminal Court is missing a link with Cybercrime and it must be a United Nations court of law by the Security Council in accordance with UN Chapter VII
- Such a serious cybercrime prosecutor shall be responsible for independent prosecution. Organizing of Global Treaties frequently
- "Cyber Security Software" should be a part of Operating System , automatically updated in frequent intervals
- Allotment of International Unique ID / Registration Number by approving the each website is one of the good solutions
- Email and Mobile OTP must be mandatory fields for every cyber transaction
- International Monitoring System/ Cyber Police warranted
- All IT companies mandatorily start "Efficient Cyber Security wing" within them
- Every software crossing country should have approval from respective country's regulatory authority
- Conducting regular training programs to IT officials and other organizations performing IT related activities like banking, e-commerce etc
- Cyber Security and Laws should be made as a compulsory subject to all IT and related Graduation and Post Graduation Degrees
- All websites must have approvals on their updates

- Strengthen government sectors
- Educate youth and conduct awareness programs frequently

- Ban websites performing illegal activities / crime/ like promoting terrorism, white collar offences, hacking, containing objectionable / abusive content, leaking nation's security / privacy matters etc.
- Strict punishments by imposing long imprisonments and awarding big penalties to criminals
- Do not keep the "remember password" button active
- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws
- Legal adoption of cloud computing
- Formulation and implementation of e-mail policy
- Legality of Bit-coins Framework for blocking websites
- Regulation of mobile applications With the formation of cyber-law compulsions, the obligation of banks for cyber-thefts and cyber-crimes would considerably increase in the near future. Indian banks would require to keep a dedicated team of cyber law experts or seek help of external experts in this regard.
- To recognize the areas for stakeholders of digital and mobile network where Cyberlaw needs to be further evolved. To work in the direction of creating an international network of cybercrimes. Legal authorities could then be a significant voice in the further expansion

of cybercrimes and cyber law legislations throughout the globe. Information Security and Cyber Law 8 Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity.

- Most corporate boards are not proactively shaping their companies' security strategies or investment plans. Only 44% of respondents say their corporate boards actively participate in their companies' overall security strategy. Senior leaders driving the business must take ownership of building cyber resilience. Establishing a top-down strategy to manage cyber and privacy risks across the enterprise is essential. Resilience must be integrated into business operations.

- A company's risk management strategy should be informed by a solid understanding of the cyber threats facing the organization and an awareness of which key assets require the greatest protection. There should be a coherent risk appetite framework. Leadership must drive the development of a cyber risk management culture at all levels of the organization.

- It is essential to promote research and development in cybersecurity so that we can come up with robust solutions to mitigate cyber risks. Cyber Security Research is the area that is concerned with preparing solutions to deal with cyber criminals. Most corporate boards are not proactively shaping their companies' security strategies or investment plans. Only 44% of respondents say their corporate boards actively participate in their companies' overall security strategy. Senior leaders driving the business must take ownership of building cyber resilience. Establishing a top-down strategy to manage cyber and privacy risks across the enterprise is essential. Resilience must be integrated into business operations.

- A company's risk management strategy should be informed by a solid understanding of the cyber threats facing the organization and an awareness of which key assets require the greatest protection. There should be a coherent risk appetite framework. Leadership must drive the development of a cyber risk management culture at all levels of the organization. With increasing amount of internet attacks, advanced persistent threats and phishing, lots of research and technological developments are required in the future. Cybersecurity Research – Indian Perspective In the recent years, India has witnessed an enormous growth in cyber technologies. Hence it calls for an investment in the research and development activities of cybersecurity. India has also seen many successful research outcomes that were translated into businesses, through the advent of local cybersecurity companies.
- Basic approaches for creation of Cyber Laws Following are the basic approaches for creation of Cyber Laws, which will ensure the smooth governance of Internet globally:

a) Formulation of new laws and amendment of existing laws by nations within their present territorial boundaries thereby attempting to regulate all actions on the Internet that have any impact on their own population. b) Nations may enter into multi-lateral international agreements to establish new and uniform rules specifically applicable to conduct on the Internet. c) Creation of an entirely new international organization, which can establish new rules and new means of enforcing those rules.

- Establishing a Suitable framework There is a dire need for the emergence of a well-defined framework of Cyber Laws, which should be able to do the following: 1) Create and implement a minimum set of guiding rules of conduct that would facilitate efficient Communications and reliable Commerce through the use of Electronic medium. 2) Define, punish and prevent wrongful actions that attack the electronic medium or harm others.

- One of the greatest concerns of the field of Cyber Laws has been the absence (or rather delay) of a well-defined and comprehensive framework of law across the globe. Today's Internet was born in the early 1960's while the initial efforts for its regulation could only surface in the late 1990's. This problem has been further aggravated by the steep rise in usage of Internet in the recent years all over the world and that too in the absence of any appropriate legal framework.

- Surely, the Cyber Law scenario is globally more complicated than traditional laws owing to the reason that the range of activities which are to be governed by these laws are largely technology driven, an area which is dynamically changing and is beyond anyone's control. However enactment of these laws pose opportunities for nations to carve model Cyber Societies for the future thereby taking a lead in becoming Global IT Powers.

Conclusion:

The Cyber Law defined as a thoughtful group conversation about core values and distinct benefits to the Society will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically defined territories.