GNITED MINDS
Journals

A RESEARCH ON ANALYZING A CYBER CRIMINAL OFFENSE, PROTECTION AND PRIVACY LAW

www.ignited.in

International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

A Research on Analyzing a Cyber Criminal Offense, Protection and Privacy Law

Gagan Deep Singh[1] Dr. K. P. Yadav[2] Dr. Yogesh Sharma[3]

[1]Doing Ph. D. from Jodhpur National University, Jodhpur

[2]Director Mangalmay Institute of Engineering & Technology Noida

[3]HOD Mathematics in Jodhpur National University, Jodhpur

Abstract – The paper shows that the levels of internet use still vary widely: while more than half of EU citizens access the internet at least once a day (54%), a substantial minority (28%) say that they never access the internet. Besides accessing the internet from a laptop computer or netbook (62%) or a desktop computer (53%), 35% of internet users access the internet through a smartphone, and 14% use a tablet computer or touch screen. Around half of internet users in the EU say they use social networking sites (53%), buy goods or services online (50%) or do online banking (48%), while 18% sell goods or services. There is considerable variation in the online activities that respondents undertake in different countries. 28% of internet users across the EU are not confident about their ability to use the internet for services like online banking or buying things online. 70% say that they are fairly or very confident.

When using the internet for online banking or shopping, the two most common concerns are about someone taking or misusing personal data (mentioned by 37% of internet users in the EU) and security of online payments (35%). Internet users have changed their behaviour in a number of ways because of security concerns. 34% say that they are less likely to give personal information on websites, while 40% do not open emails from people they don't know. 46% have installed anti-virus software. However, only around half (48%) of internet users in the EU have changed any of their online passwords during the past year.

EU citizens feel better informed about the risks of cybercrime that they did in 2012. The proportion that feels very or fairly well informed has increased from 38% to 44%, while fewer respondents say they do not feel very or at all well informed about the risks of cybercrime (52% compared with 59% in 2012). Around half of internet users in the EU are concerned about experiencing identity theft (52%) and about being the victim of online banking fraud (49%). Just under half of internet users are concerned about: having their social media or email account hacked (45%); accidentally discovering child pornography online (44%); scam emails or phone calls (43%); and online fraud (42%). In addition, 37% are concerned about not being able to access online services because of cyberattacks, and 35% are concerned about accidentally encountering material which promotes racial hatred or religious extremism. These levels of concern about specific types of cybercrimes are lower than in 2012, with the largest decrease in relation to identity theft (down from 61% to 52%), while concern about becoming a victim of cybercrime in general has slightly increased.

---------------------------♦-----------------------------

INTRODUCTION

The emergence of the Internet in the late 1980s led to the evolution of cyberspace as a fifth domain of human activity and in last two decades, Internet has grown exponentially worldwide. India too has witnessed significant rise in cyber space activities and usage of internet so much so that it has not only become one of the major IT destinations in the world but has also become the third largest number of Internet users after USA and China. Such phenomenal growth in access to information and connectivity has on the one hand empowered individuals and on the other posed new challenges to Governments and administrators of cyberspace.

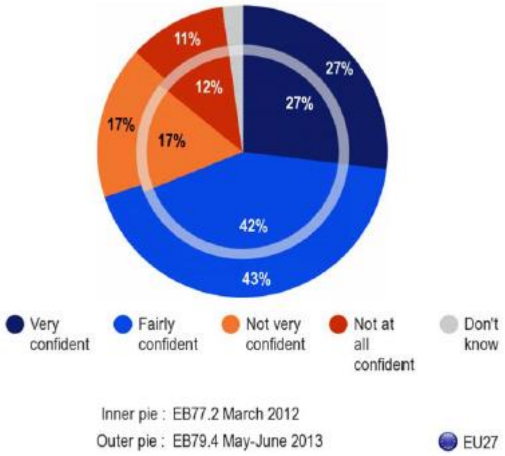
Cyber space has unique characteristics *viz.* anonymity and difficulty of attribution, coupled with enormous potential for damage and mischief. This characteristic not only adds to the vulnerabilities but also makes cyber security a major concern across the globe since it is being exploited by criminals and terrorists alike to carry out identity theft and financial fraud, conduct espionage, disrupt critical infrastructures, facilitate terrorist activities, steal corporate information and plant malicious software (malware) and Trojans. The emergence of cloud and mobile technology has further complicated the cyber threat landscape. Moreover, with the advent of sophisticated and malicious cyber tools physical damage on critical infrastructure and systems are inflicted and systematically information from targeted systems are stolen. All this makes cyber security an issue of critical importance with profound implications for our economic development and national security. Given the growing threats to cyber assets and all pervasive inter-connected information systems, countries around the world are engaged in actions for ensuring security of their cyber space.

Cybersecurity strategies recognise that the economy, society and governments now rely on the Internet for many essential functions and that cyber threats have been increasing and evolving at a fast pace. Most strategies aim to enhance governmental co-ordination at policy and operational levels and clarify roles and responsibilities. They reinforce public-private cooperation. They emphasise the need to respect fundamental values such as privacy, freedom of speech, and the free flow of information. They also call for improved international co-operation. Some strategies also support more flexible and agile policy approaches, and emphasise the economic dimension of cybersecurity policy. Some create the conditions for a multistakeholder dialogue in the cybersecurity policy making and implementation process.

CONFIDENCE ABOUT INTERNET TRANSACTIONS

This chapter looks at internet users' confidence in using the internet for online banking or buying things online. It then examines the concerns that internet users have about these activities, and finds out whether respondents have changed their internet behaviour as a result of any concerns. Throughout the chapter, findings are based only on people who ever use the internet.

Confidence - The majority of internet users across the EU (70%) say that they are at least fairly confident about their ability to use the internet for things like online banking or buying things online, including 27% who say they are very confident. However, 17% are not very confident and 11% are not at all confident.



Base: Internet users (QC1) (n=18,983 in EU27)

There is considerable variation by country in the level of confidence that respondents have in using the internet for things like online banking or buying things online. These variations tend to reflect the levels of actual use of the internet for these activities, as described in the previous section.

Concerns - Internet users were asked what concerns they have about using the internet for things like online banking or buying things online. Respondents answered in their own words and were not prompted with possible options.

The two most common concerns are about someone taking or misusing personal data (mentioned by 37%) and security of online payments (35%). Some respondents also express a preference for conducting transactions in person (24%), while 15% are concerned about not receiving goods or services that they buy online. Around a quarter of internet users (23%) say they have no concerns about using the internet for things like online banking or buying things online.

Impact On Behaviour - The actions that respondents are most likely to take are installing anti-virus software (46%) and not opening emails from people they don't know (40%). Other changes include being less likely to give personal information on websites (34%), only visiting websites that they know and trust (32%), only using their own computer (26%) and using different passwords for different sites (24%). Other actions are mentioned by around one in six respondents: 17% say they are less likely to buy goods online and 15% are less likely to bank online, while 16% have changed their security settings. In addition, 6% have cancelled an online purchase because of suspicions about the seller or website. However, 18% of respondents say they have not made any changes because of concerns about security issues.

CYBER SECURITY SCENARIO IN INDIA

In keeping with the general trend of growth of information technology worldwide, in India too there has been tremendous growth in use of information technology in all walks of life. The internet user base has increased to 100 million and total broadband subscriber base has increased to 12.69 million. The target for broadband connections by 2014 is 22 million. Today, India has 134 major ISPs, 10 million registered domain names (1 million '.in' domains) and over 260 data centers all over the country.

Significant increase in cyber space activities and access to internet use in the country has resulted in increased opportunities for technology related crime. Coupled with this, lack of user end discipline inadequate protection of computer systems and the possibility of anonymous use of ICT – allowing users to impersonate and cover their tracks of crime, has emboldened more number of users experimenting with ICT abuse for criminal activities. This aspect, in particular, has a significant impact in blunting the deterrence effect created by legal framework in the form of Information Technology Act 2000 and other well-intended actions of enhancing cyber security in the country. As a result, today Indian cyber threat landscape, like other parts of the world, has seen a significant increase in spam & phishing activities, virus and worm infections, spread of bot infected systems. The rate of computer infections and spam & phishing activities in the country keep fluctuating, making India figure among the active sources, as is generally seen in developed economies with high rate of IT usage.

MANAGEMENT STRUCTURES AND ACTIONS PLANS

Most strategies aim to improve the public administration's organization and co-ordination to address cyber security. Almost all strategies assign clearer responsibilities in the government and/or establish new organizational structures. Some place a strong emphasis on the need for high-level leadership. While all countries target the same objectives, the organizational arrangements they make vary and reflect their cultures and styles of government. In general, however, strategies place a strong emphasis on the identification of a co-ordination point at the policy level and at the operational level. Policy coordination can be assigned to Prime Minister, Cabinet office (Australia, Japan, United Kingdom), or Head of State (*e.g.* "Cybersecurity Czar" reporting to the White House), to a specific agency for cybersecurity attached to a co-ordination body (*e.g.* the French ANSSI) or to a Ministry (Canada, Germany, Netherlands). Co-ordination at operational level generally relies on a central point which varies considerably across countries. Some countries also created a specific body for public-private coordination and to provide advice to the government regarding how to balance cybersecurity, economic objectives and fundamental values.

The protection of CII is generally part of the cybersecurity strategies although countries generally have specific policy documents to address this challenge. Some strategies stress the need to better integrate CII management structures with other cybersecurity structures as an objective (Netherlands). Measures for the protection of CII vary depending on the level of advancement of each country in that area and are generally based on public-private co-operation. They include preparatory measures such as cybersecurity incident response plans and improved crisis management plans, the development of business continuity arrangements, the organization of exercises, the creation of a rapid response capacity with international reach, the improved co-ordination of and information sharing amongst the various players (*e.g.* suppliers and operators of CI, public and private actors, etc.), the development of legal frameworks, international alliances, the promotion of standards and the organisation of audits.

EXPERIENCE AND CONCERNS ABOUT SPECIFIC CYBERCRIMES

Around a third of internet users across the EU (32%) say they have received an email or phone call fraudulently asking for access to their computer, logins or personal details. This is by far the most common type of cybercrime experienced by respondents. In total, 7% of internet users say that this has happened to them often, while 25% say it has happened occasionally.

In addition, 14% of internet users say that they have accidentally encountered material which promotes racial hatred or religious extremism, while 12% have not been able to access online services because of cyber-attacks, 12% have had their social media or email account hacked, and 10% have experienced online fraud (where goods are not delivered, counterfeit or not as advertised). Across the EU, 7% of internet users say they have been a victim of credit card or banking fraud online, and 6% say they have experienced identity theft.

For the items that were also included in the 2012 (all items except social media or email account being hacked and being a victim of credit card or banking fraud online), the levels of experience have mostly remained similar. The main exception is receiving emails or phone calls fraudulently asking for computer access or details; the proportion that has experienced this is lower in 2013 than in 2012. However, the wording of this item is different, so it is not advisable to make a direct comparison on this measure.

CYBER CHALLENGES

The cyber threat landscape is dynamic and evolving with innovative technologies, techniques and actors and offenders are well versed with technology and they are exploiting the lack of situational awareness of defenders. Cyber threats like espionage and Denial of Service (DoS) attacks to offensive actions by adversarial State and Non-State actors. Several countries are developing sophisticated malicious codes as lethal cyber weapons. Large scale mapping of SCADA (Supervisory Control and Data Acquisition) devices using specialized tools, pose major challenge for any country.

DeitY, in their background note, has outlined the following as the main issues and challenges observed in the cyber space:-

- Expanding role and implementation of Information Technology across all sectors in the country

- Growth in volume and complexity of Information Technology ecosystem in the country

- Growth in volume of transactions and sensitive data exchange

- Rapidly changing security and threat landscape

- Paradigm shift in attack vectors and nature of their launch

- Difficulty in tracing origin of attack

- Need for reducing cyber security risk exposure of IT infrastructure and ecosystem in the country

- Responsibility to ensure that proper processes, technology, governance structure and compliance to laws and regulatory requirements are followed in a borderless environment

- Defending borderless environment poses challenges which are dynamic in nature.

CYBER SECURITY AND RIGHT TO PRIVACY

As per the background note furnished on the subject, balancing cyber security, cybercrime and right to privacy is an extremely complex task due to the nature of the cyber space which is borderless. It requires the maturity and competence of seasoned professionals who have skills in multiple disciplines at the same time, namely technical (deep understanding of ICT and cyber security), protection (technical, process and administrative controls), legal and regulatory, constitutional, diplomacy, communication skills, public policy, psychology and economics to name a few.

“Regarding personal information and the right to privacy already, the IT Act, section 43A and 72A has got provisions to safeguard the personal information in the sense that if any organisation which is in possession of the private personal information of the individuals, reveals to other without consent of the individual, it is a punishable offence under the IT Act with imprisonment of up to three years. If any such case comes to the notice, immediately cognizance can be taken. It is already provided under section 72A. So, the companies are obliged to keep confidentiality of the personal information of individuals. Apart from the legal provisions, more workable and more operative thing is the fact that India is one of the top most countries in the world in terms of business processes outsourcing (BPO) operations.

So, a large number of IT companies in this country are receiving personal data of people from all over the world and they are processing that data as per their client’s requirement without any major concerns or complaints. It is a question of survival also. If this information is traded by these companies, then obviously the reputation of the company as well as the country will be on stake. Hence, there is also available a commercial safeguard, a professional safeguard apart from the legal safeguard. That I would say regarding the privacy.

CONCLUSIONS

Many respondents say they have changed their behaviour because of security concerns, for example by not giving out personal information or not opening e-mails from unknown sources. At the same time, only around half of internet users have changed any of their online passwords during the past year. Overall, most internet users are confident about their ability to use the internet for things like online banking or buying things online, although a substantial minority do not feel confident.

EU citizens feel better informed about the risks of cybercrime than they did in 2012, although many still do not feel very or at all well informed. Frequent internet users and those who are confident online tend to feel better informed. A third of internet users across the EU say they have received a scam email, and other types of cybercrime have been experienced by a substantial number (albeit a minority) of internet users in the EU, including online fraud, identity theft, hacking of email or social media accounts and online harassment.

Internet users express high levels of concern about cyber security. The majority agree that the risk of becoming a victim of cybercrime has increased in the past year; that they are concerned that their online personal information is not kept secure by websites; and that they are concerned that information is not kept secure by public authorities. The emergence of sovereignty considerations in cybersecurity strategies is an evolution that is likely to influence policy making in the longer term. At this stage, sovereignty considerations are kept separate from the economic and social aspects of cybersecurity but intersections are becoming visible. For example, in some cases, policy and/or operational co-ordination is led by agencies whose missions focus on sovereignty considerations; some strategies call for facilitating technology spillovers from the intelligence community to the cybersecurity industry sector; new industry suppliers and products benefitting from R&D investments driven by sovereignty considerations are entering the cybersecurity marketplace; and finally, in some countries, the military and intelligence communities are becoming important potential suppliers of cybersecurity jobs. Understanding the implications of this crossfertilisation in the short, medium and longer term might become increasingly relevant to inform the cybersecurity policy making process.

REFERENCES

- ANSSI (2011), "Defense et sécurité des systèmes d'information. Strategie de la France". Available at www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

- Australian Government (2011), "Connecting with Confidence. Optimising Australia's Digital Future". Available at http://cyberwhitepaper.dpmc.gov.au/sites/default/files/documents/connecting_with_confidence_public_discussion_paper.pdf.

- BBC, "How the Assam Conflict Creates a Threat to All India" (August 20, 2012). Available at http://www. bbc.co.uk/news/world-asia-india-19315546. Accessed December 27, 2012.

- Council of Europe (2011), "Cybercrime strategies". Discussion paper prepared by the Global Project on Cybercrime. Available at www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports -Presentations/2079_cy_strats_rep_V20_14oct11.pdf.

- Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation, Cristin Goodwin and Paul Nicholas, Microsoft, October 2013. (http://aka.ms/national-strategy).

- Dutch Ministry of Security and Justice (2011), The National Cyber Security Strategy (NCSS). Strength through cooperation. Available at http://english.nctb.nl/Images/cyber-security-strategy-uk_tcm92-379999.pdf.

- ENISA (2011a), "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report", p. 12. Available at www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-techreport/at_download/fullReport.

- Jim Yardley, "Panic Seizes India as a Region's Strife Radiates," The New York Times (August 17, 2012). Available at http://www.nytimes. com/2012/08/18/world/asia/panic-radiates-from-indianstate-of-assam.html?pagewanted=all&_r=0. Accessed December 27, 2012.

- Kondhwa-attacks-on-northeast-students. Accessed January 3, 2013.

- The Times of India, "Doctored MMS Clip Provoked Attackers: Cops." Available at http://articles.timesofindia. indiatimes.com/2012-08-14/india/33200173_1_mmsclip-

- Zee News, "Northeast Issue: Exodus Subsides in Bangalore, No Let Up in Chennai, Pune." Available at http://zeenews.india.com/news/nation/north-eastpeoples- exodus-continues_794432.html. Accessed January 2, 2013.