Local and international organizations ensure the cyber security

IGU Dilmini Rathnayaka
Faculty of Graduate Studies & Research, Sri Lankan Institute of Information Technology, Colombo.

ABSTRACT

The world is rapidly growing and the crimes are gradually increasing. These crimes are not only depicting the physical world. The crimes are highly improving in the digital world too, which are mostly interact with the internet. When considering the developing and gradually altering world, cyber security is one major requirement for all the internet users that should aware. There are agencies and institutes locally and internationally, who always supporting internet users in case of facing any cybercrime and harassment, and illegal situations. As much as the police, cops, army, law courts are available, these agencies and institutes are willing to support internet users during any unfair situation.

Keyword : - *Cyber security, local, international, cyber crime*

1. INTRODUCTION

This article is describing some agencies, which are possible to support for cyber crimes and contribute consultancy. When thinking about any sort of cybercrime, for instance hacking Facebook, Twitter, Instagram, or any social media account, online bank account, email account, unauthorized access, usage, alteration and deletion of the former mentioned internet-related private asset, bulling through the internet and misuse of personal things by other person are possible to count as cybercrime. During these types of situations, there several agencies and institutes that capable to help the injustice party. Several local and international institutes are willing to provide the service and justice for the predicament person.
As local institutes, Sri Lankans are capable to get support from Sri Lankan Police more specifically from the Sri Lankan Police Cybercrime unit, Sri Lanka Computer Emergency Readiness Team| Coordination Centre (Sri Lanka CERT|CC), University of Colombo, and from TechCERT.

University of Colombo, and from TechCERT.

1) Sri Lanka Police (Sri Lankan Police Cybercrime unit)

Fig-1 : Sri Lankan Police

The Sri Lankan Police Cybercrime unit is the section to make complaints about the **i**nternet crimes which was established at police headquarters. This section is collaborated by the division of the Criminal Investigation Department &Information Technology. This is a government section that undertaken the fully control of cybercriminals and cyber attacks, investigate the offender, getting legal actions against the criminal, and providing

justice to the victim according to the legal way. These investigations and complaints are about hacking Facebook, Twitter, Instagram, or any social media account, online bank account, email account, unauthorized access, usage, alteration and deletion for the former mentioned internet-related private asset, bulling through the internet, and misuse of personal things by other person or any sort of illegal action beyond to the law of Sri Lankan government policies. The police is offering the civil people even by tracking the location of criminal and anyone is allowed to use the www.telligp.police.lkwebsite to complain about the crimes and harassments even by attaching pictures or documents which could use as evidence of the situation[1]. The Sri Lankan Police Cybercrime unit is providing the facility to gain justice during any cyber attack while helping to recover from the situation using a special consultancy program. It is a very good procedure for Sri Lankan government by providing the civil nation to stand against the cyber attacks and deal with those until the situation comes clear.

2) CERT|CC (Computer Emergency Readiness Team | Co-ordination Center)

Fig-2 : Sri Lankan CERT|CC Logo

The CERT|CC was established by the ICT Agency of Sri Lanka during 2006 and it was a Private Limited Liability Company until August 2018. After 2018 it was taken under the authority of the Ministry of Defence. Sri Lanka CERT is entangled with many international collaborations. CERT associations of Japan, China, and the Korean Internet Security Agency are agreed to work collaboratively to deal with the cyber threats efficiently and effectively in the region of Asia Pacific. Additionally, Sri Lanka CERT has taken the necessary actions to collect, analyze, and share the internet traffic data, with the intention of recognizing the internet threats in Sri Lanka and Asia Pacific region. The Sri Lanka CERT works with Global Action Against Cybercrime Project (GLACY) of Europe to improve the cyber security eco-system in the country. Moreover, Sri Lanka CERT is a became a member of International Information Systems, Security Certification Consortium, ICANN, APNIC, ITU, IGF, and Facebook for developing a suitable cyber security ecosystem[2].

The CERT|CC main purpose is to become the major organization as well as the reliable source of instructions on threats and vulnerabilities to the information systems with the use of prevention methods, procedures, and actions. This organization is located in Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07 and the website link is www.cert.gov.lk. The cyber attacks are arising in many forms, more specifically as Denial of Service, bulling the people with the use of internet available photographs and videos, website unauthorized access, and alteration of websites and contents. These actions are committed mostly by individuals for personal gain, terrorists, fraudsters, thrill-seekers, or by an organized group of people. During such cases, CERT|CC acts as the major supportive and life-saving party of cyber security in the nation. It also provides advice about upcoming threats and vulnerabilities which have a higher probability of influencing computer systems and networks, as well as the exclusive assistance from the experts to recover from those cyber attacks. The CERT|CC is assisting to react and provide protection and security against the potential cyber-attacks.
The CERT|CC is willing to look after the security issues of the organizations with providing properly managed security services that are cost-effective. And if someone requires reporting a cyber attack, CERT|CC contributes some channels to complain about the incident. Through the telephone, email, or fax as well as filling the form of their website anyone can easily report the incident. As the major issue of these days, the problems with social media are resolving by CERT|CC as well as providing the consultancy, if in case the victim requires carrying an investigation about the incident, taking legal proceedings, or contacting law penalties for instance Sri Lankan

police.

The service of Sri Lanka CERT|CC can be gain many delivery channels like the Sri Lanka CERT|CC website, remote support by telephone during work hours, e-mail, and fax during work hours, through the seminars, consultations & workshops. The work hours of Sri Lanka CERT|CC is from Mondays to Fridays, 8.30 AM to 5.30 PM. and beyond work hours the help desk numbers can be used to obtain a report about the incidents. There are four major types of services provided by CERT|CC and they are responsive services, comprehension services, research, and policy development services, and advisory services [2]. During the cases of social media, the Sri Lanka CERT|CC is supporting and contributing the technical assistance for the instances like the way of abolishing fake accounts and pages (Ex: Facebook, Instagram), to remove hacked accounts from Facebook, to report and remove the violence and fake pictures, videos, etc which are against to the Facebook policy.

The responsive services by the Sri Lanka CERT|CC include providing assistance for cyber attacks for the computer systems by spam, malware virus infections, and attacks. This organization helps to detect these attacks and respond to these attacks in a suitable way and ensure the stability and availability of the system. These attacks basically doing by the methods of malware attacks, Daniel of Service, Phishing, Threatening emails, information threat, and discloser, etc. The Sri Lanka CERT|CC is also assisting to recognize the problem and act as it needed during the situation while maintaining the system functions. After the system is recovered from the security issues and cyber attacks the Sri Lanka CERT|CC is providing a comprehensive Incident Report mentioning about the nature of the incident, the procedures taken to overcome from the incident, and recommended preventive measures that should follow to avoid from future attacks [2]. But the Sri Lanka CERT|CC is not assisting to investigate the threatening emails, threatening parties, and criminals.
The awareness services of Sri Lanka CERT|CC is providing the education about the significance of information security, as well as the awareness about cyber threats and attacks. It is contributing alerts about how to recognize computer viruses, security issues while providing possible short-term recommendations to deal with those. For now, the alerts are mentioned on Sri Lanka CERT|CC website. They also conducting seminars & conferences to provide enhance the awareness about information security issues, best practices of using security protocols and security standards. In addition to that, they are conducting workshops to the IT professionals to perform their tasks on system security and these are carrying with more detailed and technical methods. Knowledgebase services an awareness procedure with the use of documents, articles, news items, etc which are available in the Sri Lanka CERT|CC website. These are aiming to provide a wide range of knowledge to anyone who has access to the website as well as for the IT professionals to obtain information to enhance their knowledge about information security.

Consultancy Services of Sri Lanka CERT|CC includes a technical assessment to review and analyze the security infrastructure and measures available within an organization and the advisory for national policy, which considered as a national service by developing, introducing, and implementing information security standards within the nation. Moreover, the Research and Policy Development Division of Sri Lanka CERT|CC is providing the service to develop strategies and monitoring policies, conducting researches, projects, and national level surveys that are associated with cyber security of the nation.
But there are not technically doing some actions for instances proceeding legal measures towards the criminal who are related with the social media incident, tracking the criminals' locations, removing the violated web stuff (Eg: photos, videos, posts,) from the social media like Facebook, Instagram, etc, as well as blocking the websites. They only advising and guiding the victim party to recover and take necessary actions. More specifically, the Sri Lanka CERT|CC is not involving for the incidents refer to gossip websites and not assisting to remove those contents and to go through any legal proceedings towards these websites.

3) TechCERT

Fig-3 : TechCERT

TechCERT is located at Dutugemunu Street, Kohuwala, Sri Lanka which is possible to view more details from its website. It is one section of the LK Domain Registry and it began with apreceding project of LK Domain Registry. This was originated with the academic partners focusing to contribute services on computer emergency response among the public and private organizations in Sri Lanka. TechCERT is collaboratively working with some national and global information security organizations which are contributing the modest and latest information about the computer and network security threats, attacks, and vulnerabilities [3]. They are holding major intention to contribute an effective response while assisting in proper and suitable preparedness during computer security issues. Additionally, they provide the appropriate methodologies when implementing proactive procedures to defend the organization's information infrastructure from cyber attacks. This organization helps its customers to build and implement completely combined information security techniques within the company IT infrastructure.

As the main services of TechCERT, protecting the customer IT resources to prevent the exterior cyber attacks and internal attacks, protection of crucial data and information which owned to the customers while avoiding financial drains which harmful for the company reputation, regulate the customer IT policies and practices parallel to the government IT laws and regulations, monitor the service availability, business continuity, and disaster recovery during cyber-attack. The TechCERT is assisting during the instances such to provide threat alerts, vulnerabilities of attacks, security solutions and execute the guidance, to proceed emergency response towards cyber-attacks, control the damage and restore or recover the system, digital forensic investigation, website security and safeguard as well as during firewall audit procedures. When the TechCERT is investigating and setting up customized, well-integrated security technologies within customer IT systems, they may ask for the customer's personal data like email address, firstname, lastname, contact number, usage data, etc to contact with the customers directly and contribute threat alerts. Usage Data is collected automatically by the TechCERT, when the company use their services. This usage data may consist of customer information for instance device's Internet Protocol address, internet browser type and version, the pages that the customer visited to gain the service, the date, and the time duration that the customer spent on the service. As well as the TechCERT is using some tracking techniques and cookies towards their services to analyze and enhance their service with the use of beacons, tags, and scripts [3]. All these data and information are collected by the TechCERT, to contribute a better service while maintaining service quality, to manage alert and aware the customers about security threats and vulnerabilities, to perform better contract while improving the service methodologies, and to keep better connection and contacts with the customers while notifying about the security updates and updates of implementations, to contribute latest news specific offers of their service, etc. The TechCERT ensures not to share the company's sensitive data, protect the privacy of the collected information through the usage data and by other methods, that will never transfer through the internet. It ensures that these data are impossible to achieve by any other third party. It concludes that TechCERT is a company which can trust to obtain their service to protect the company systems' security.

4) University of Colombo

Fig-4 : University of Colombo,Sri Lanka

The University of Colombo website providing the three steps process to take necessary actions against ransomware attacks. It mentioned the first step as back-up the system or computer daily. The critical and crucial information of the system store to a distinct device which is possible to use even offline. It is helping to restore the system after the attack and when the risk is gone, update the system with new versions and strongly continue the working process. The second step is awareness of the employees about ransomware, the cyber-attacks due to phishing, cyber threats, and aware them about timely reporting about the attacks to the responsible person. As the third step, it describing developing a cyber response plan to address the attack, deal with the attack, and recover from the attack. Moreover, the university website providing an email address to contact and know more about these attacks and to ask any question.

There are several organizations that are global or international which help to sustain good behavior within the internet or cyber world [4].

5) National Cyber security and Communications Integration Center

Fig-5 : NCCIC Logo

This organization is responsible to protect the USA nation from physical and cyber-attacks and threats. Cyberspace allowing to operate the business functions, communication, the government to conduct the activities for instance emergency preparedness for certain situations, and almost more section in monitoring the systems and processes. As the whole national security is important, the protection of these systems is crucial to maintain the continuity and reliability of national critical infrastructure including the major resources that affect the economy. The NCCIC providing cyber security and protection towards the government agencies, private companies, and even to the international organizations. NICCIC is capable of analyzing the cyber security, communicate or share that information on time, coordinate the responses, mitigate the risks by the cyber-attacks, and recover from the attacks. The NCCIC consists of four main branches as NCCIC Operations & Integration (NO&I) which responsible to analyses the information, sharing those information and incident management, United States Computer Emergency Readiness Team (US-CERT) which responsible to analyze the digital media about any malicious activity which are focusing on national networks and timely spread the responsive and actionable information among the agencies and companies, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which is responsible to mitigate the risk of national critical infrastructure while enhancing the security control of the systems and National Coordinating Center for Communications (NCC) which is responsible to coordinate, rehabilitation, restoration and rebuilding of the telecommunications services, systems and facilities within any sort of condition[5]. This organization is providing the service for the situations like reducing the risk of cyber attacks and cyber incident response planning, analyses the information and aware the risk and cyber-attack vulnerabilities to the nation, information sharing with local and international collaborate organizations to aware about the threats, share and aware the nation and companies about the cyber attacks, to mitigate , recover and rehabilitate the systems after cyber attacks threats while enhancing the national security practices, etc. More details of the NCCIC could obtain from its website.

6) The European Union Agency for Cybersecurity- ENISA

Fig-6 : ENISA

The European Union Agency for cyber security is an agency that is focused on a better degree of cyber security across Europe. This agency was originated during 2004 which was reinforced by the EU Cyber security Act. This agency contributing assistance to improve the trustworthy of ICT related manufactures and services, processing

under the cyber security certification protocols ,and to face cyber challenges. With the help of ENISA, European citizens may feel secure and protection towards the digital environment, could share knowledge about cyber environment, awareness about the cyber attacks, gain help to confidence about the country's economy. The ENISA is checking on the practice of cyber security policy to avoid the cyber attacks and make sure all sectors of the nation are following these policies, fast response and appropriate operational cooperation, strategic co-ordination towards cyber attacks, aware the citizens and technical actions against the cyber-attacks, make sure the different operational parties are consists of necessary actions and recovery methods, ensuring the all social, market, digital environment and economic balance towards the cyber security, foresight about the cyber-attacks, threats, and solutions with the emerging new technologies, and the knowledge or awareness about the cyber attacks by the people [6]. It shares and expanding the awareness and information about cyber attacks by mentioning the continuous procedure of gathering, organizing, briefing, investigating, and sharing the cyber security information. More details of ENISA could obtain from its website.

7) National Cyber Security Center(NCSC)

Fig-7 : NCSC Logo

NCSC is a self-regulating authority on cyber security which is located in the United Kingdom. This was originated in October 2016and the headquarters are in the city of London. It providing the safety to work online, helping to make the UK the safest place to live and work online [7]. The NCSC is assisting the most crucial organizations, public and private companies in the UK. The NCSC provides their service to understands about the cyber security and gain knowledge, responds to cyber-attacks and mitigate the risk and harm which effects for the company, reduce the cyber security attacks from public and private sector systems, service from the experts to foster cyber security etc.

The NCSC works cooperatively with international associates, law enforcement, and other UK security agencies. The NCSC pay the attention to protect the personal devices of people like smartphones, laptops, computers, and other devices that access the internet. The possibility of cybercriminals to get sensitive data when online banking, online shopping, when using emails, and social media are taken into consideration by NCSC and its providing knowledge to the citizens about these vulnerabilities, possible prevention methods and action plans[7]. The website of NCSC, providing some tips to aware about cyber attacks when the social media or any internet account is hacked and recover the account, unlocking the computer when a ransomware attack occurred, when the username and password are stolen, malware attack to the device, when getting an ambiguous email, calls or messages, to ensure the online bank details are secured, etc. The NCSC is providing their services to self-employees, large and small companies, private and public-sector companies, individuals, families as well as for the cyber security professionals

8) NACSA | National Cyber Security Agency –Malaysia

Fig-8 : NACSA Logo

The National Cyber Security Agency was originated during February 2017. It was considered as the national lead agency that counts on cyber security issues, and it assisting to enhance, reinforce the security of Malaysia when dealing with security threats and cyber-attacks[8]. It is considered as the agency which consists of the best experts and resources to mitigate the cyber attacks in Malaysia. Moreover, the NACSA is devoted to secure the national infrastructure of information, develop and execute the cyber security policies and tactics, ensure the strategic methodologies are works on cyber threats, aware the citizens about the cyber security, monitoring the strategic actions against to the cyber crimes, consulting the organizations about cyber risk management, aware about the appropriate network updates and alterations to make within the system after facing cyber-attacks without any destructions and share the cyber security instructions among global and regional networks. The NACSA Services for individuals include the methods to ensure the protection against cybercrimes and to prevent viruses, phishing and, ransomware. The website of the NACSA contributing details for the individuals about setting a password, updating security software or virus guards, protect the personal or sensitive information, aware about the cyber world, internet ethics, criminals, cyber crimes, report about the issue of web content, personal data, or unauthorized access and be alert on the personal sensitive information[8]. It also provides assistance to protect the business and customer data against cyber threats. The knowledge about the cyber security controls and precautions, the consultancy as well as action plan against to the cyber-attacks which help to prevent financial losses and continue the business process while sustaining the company reputation. The team of Cyber Security and Risk Management at NACSA specifically contributing the advice to plan, manage, execute, and maintain security procedures while providing the opportunity to join with training and internal audit programs. This Agency is considering to develop and maintain secure cyber culture as a service to the government. More details are possible to view through the NACSA website.

CONCLUSIONS

There are many institutes who supports to enhance and ensure the cyber security. It's better to gain and understand about cyber issues and security issues by all the internet users to ensure the privacy and protection of sensitive data. International and local institutes are always willing to help for the internet users and when the user faced for an injustice situation. Unless the government, police, these institutes are doing a service for the entire society. The awareness of cyber attacks is crucial due to that rapid changing cyber space and technology with highly improving cyber crimes.

.REFERENCES

[1]. "SRI LANKA POLICE", *Telligp.police.lk*, 2020. [Online]. Available: http://www.telligp.police.lk. [Accessed: 21- Aug- 2020]

[2]. "Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT)", *Sri Lanka CERT|CC*, 2020. [Online]. Available: https://www.cert.gov.lk/. [Accessed: 21- Aug- 2020]

[3]. "TechCERT - Computer Emergency Readiness Team, Sri Lanka", *Techcert.lk*, 2020. [Online]. Available: https://www.techcert.lk/en/. [Accessed: 21- Aug- 2020]

[4]. "Immediate action to Safeguard Against Ransomware Attacks", *University of Colombo, Sri Lanka*, 2020. [Online]. Available: https://cmb.ac.lk/immediate-action-to-safeguard/. [Accessed: 21- Aug- 2020]

[5]. "National Cybersecurity and Communications Integration Center", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/National_Cybersecurity_and_Communications_Integration_Center. [Accessed: 21- Aug- 2020]

[6]. "ENISA", *Enisa.europa.eu*, 2020. [Online]. Available: https://www.enisa.europa.eu/. [Accessed: 21- Aug- 2020]

[7]. "National Cyber Security Center(NCSC)", *Ncsc.gov.uk*, 2020. [Online]. Available: https://www.ncsc.gov.uk/. [Accessed: 21- Aug- 2020]

[8]. "National Cyber Security Agency", *Nacsa.gov.my*, 2020. [Online]. Available: https://www.nacsa.gov.my/. [Accessed: 21- Aug- 2020]

BIOGRAPHIES

Author - Ms. IGU Dilmini Rathnayaka - Currently working as Information Technology Demonstrator in Department of Remote Sensing and GIS, Faculty of Geomatics, Sabaragamuwa University of Sri Lanka. Graduated as BSc(Hons) Computer Science & Software Engineering degree holder from University of Bedfordshire, United Kingdom. Currently, following MSc in Information Management at Sri Lankan Institute of Information Technology.