Global Cyber Security and ICAO Strategy for Aviation Cyber Security

PRESENTED BY:

SANJEEV SINGH KATHAYAT

PRAMOD CHAUDHARY

PRADIN TAMRAKAR

NEPAL

Global Cybersecurity Threats

The major cyber security issues faced in Nepal are:

- Identity theft
- Spam email marketing
- Cyber bullying
- Child online protection
- Copyright issues
- Hacking
- Banking Fraud
- Phishing

Identity Theft

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

Hacking

Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most “hackers” attack corporate and government accounts. There are different types of hacking methods and procedures.

Scamming

Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

Phishing

Phishers act like a legitimate company or organization. They use “email spoofing” to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

Fraud

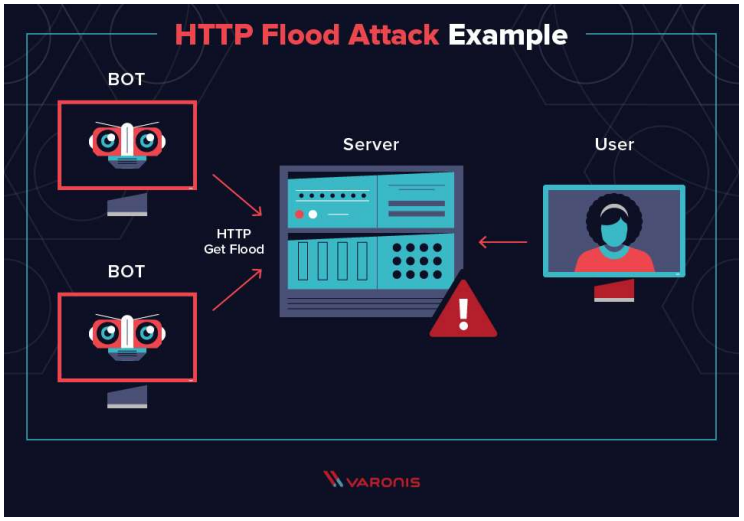
Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

Ransomware

Ransomware is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransomware. In 2017, over $5 billion is lost due to global ransomware.

DDoS Attack

DDoS or the Distributed Denial of Service attack is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system.

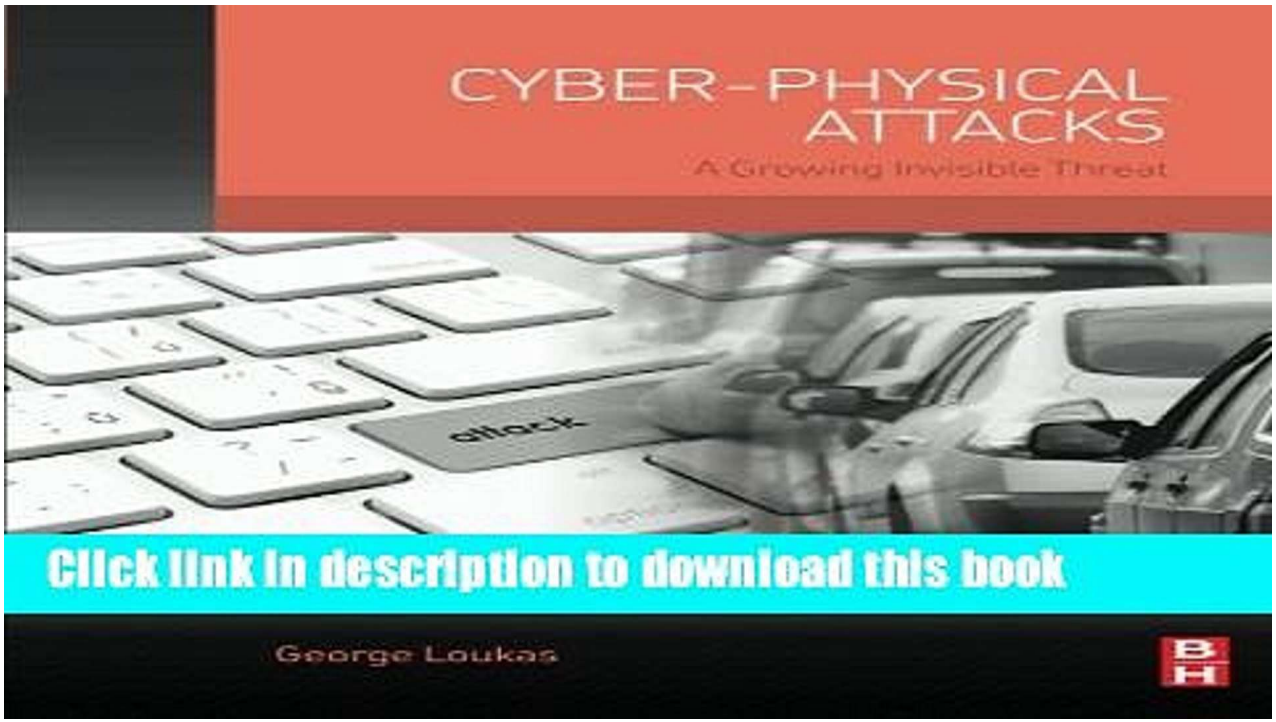


Cyberbullying

Cyberbullying is one of the most rampant crimes committed in the virtual world. It is a form of bullying carried over to the internet. On the other hand, global leaders are aware of this crime and pass laws and acts that prohibit the proliferation of cyberbullying.

Cyber-Physical Attacks

The ongoing threat of hacks targeting electrical grids, transportation systems like road, train and aviation , water treatment facilities, etc., represent a major vulnerability going forward.



State-Sponsored Attacks

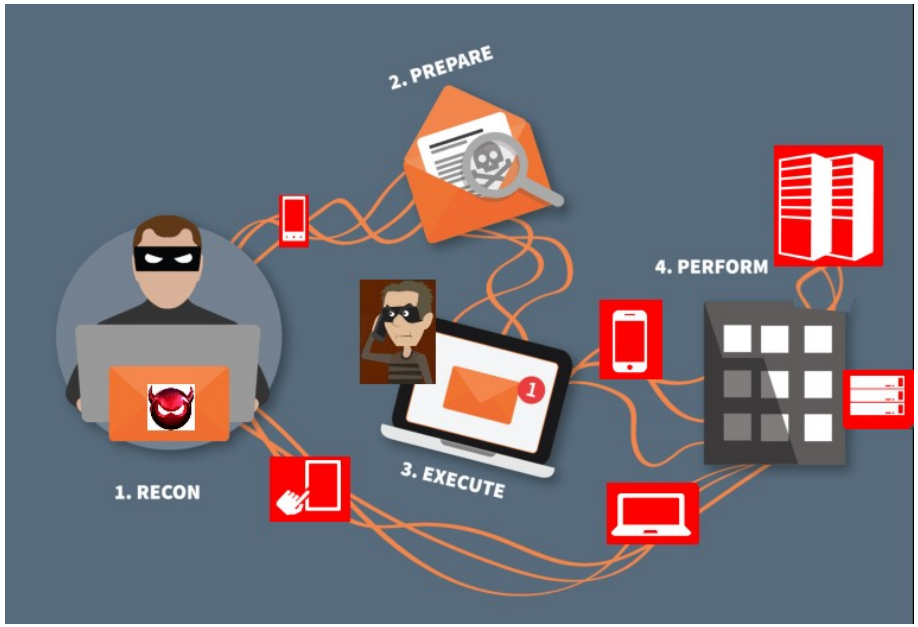
Beyond hackers looking to make a profit through stealing individual and corporate data, entire nation states are now using their cyber skills to infiltrate other governments and perform attacks on critical infrastructure

Computer Viruses

Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

Social Engineering

Social engineering is a method in which cybercriminals make a direct contact with you through phone calls, emails, or even in person. Basically, they will also act like a legitimate company as well. They will befriend you to earn your trust until you will provide your important information and personal data.



Software Piracy

The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

The Major Cyber Security Issues in Nepal and Effort of Government of Nepal for Cyber Security

The popularity and availability of the internet are increasing day by day. By the end of 2016, about 48% of the world's population was using the internet. Today billions of people are connected to the internet via many devices to share information and make the world a small place. This global surge of the rise of the Internet hasn't left Nepal untouched.

In terms of the total number of internet users, Nepal ranks 73 in the world with about 5 million internet users. Currently, about 18% of the population of Nepal is using the internet but with the advancement in technology, the number of users growing by 12 to 15% each year.

With this huge increasing number of people sharing and transferring an enormous amount of data on the internet, a danger arises which does and should alarm every internet user. "Cybercrimes" are offenses that are committed against individuals or institutions to cause physical, mental or financial harm using telecommunication networks such as the internet. The number of cyber-

Reported Cyber Crime Cases

SN	Report Received	Jul 2016 to Jul 2017	Jul 2017 to Jul 2018	Jul 2018 to Jul 2019	Total
1	Central Investigation Bureau	96	131	135	362
2	Crime Division	1197	1482	1938	4617
3	Metro Police Range Kathmandu	25	81	136	242
	Total	1318	1694	2209	5221

Current Year Statistics Reported, only in Cyber Bureau (Jul 2019 to Dec 14, 2020)

Cases	Number
Facebook / Messenger	940
Viber	4
Whats App	0
IMO	2
YouTube	3
Twitter	2
Instagram	6
Web Site Hacking	0
Other	15
Total	972

Effort of Government of Nepal for Cyber Security

As modernization and development is deriving world to digitation, evolving in technology also fetching challenges in society. Numbers of cyber crime incident were reported as hacking, phishing, cyber bullying, cyber stalking, ATM hacking, ransomware, spam email, fraud, Social Engineering etc. To address the challenge Government of Nepal stepped toward Cyber Security as follows.

- **Law, Policy and Regulation Level**
- **Research & Coordination Level**
- **Law Enforcement & Awareness Level**

Law, Policy and Regulation Level

- Government of Nepal passed the bill of "Electronic Transaction Act - 2008".
- NTA (Nepal Telecommunication Authority) drafted Cyber Crime Policy & in pipeline process for Declaration.
- MCIT (Ministry for Communication & Information Technology) formed ITERT (Information Technology Emergency Response Team) headed by Director General of MCIT in 30 April 2019 to strengthen & reinforce the cyber policies.

Research & Coordination Level

Also formed CSMC (Cyber Security Monitoring Center) headed by Director of MCIT in 30 April 2019 which includes "Nepal Police, Cyber Bureau" as well, to analyze & investigate cyber threats in Nepal and to coordinate with MCIT & Nepal Police Cyber Bureau.

Law Enforcement & Awareness Level

1. Formed Cyber Bureau under Nepal Police headed by DIGP (Deputy Inspector General of Police) in 2019.
2. Formed Cyber Crime Unit under Metropolitan Police Crime Division, Nepal Police.
3. Formed Cyber Crime Unit Under Central Cyber Bureau (CIB), Nepal Police.
4. Lunching "Community Police Partnership Program" to aware Communities and Students (Class 1 to 12) about Cyber Security, Traffic, Human Trafficking, and Drugs awareness.
5. Establishment of Digital Forensic Investigation Units in various level.

Role of ICAO for Cyber Security for Civil Aviation

- Acknowledging the urgency and importance of protecting civil aviation's critical infrastructure, information and communication technology systems and data against cyber threats, ICAO is committed to developing a solid cyber security framework. The 40th Session of the ICAO Assembly adopted Assembly Resolution A40-10 – *Addressing Cyber security in Civil Aviation*.

- The resolution addresses cyber security through a horizontal, cross-cutting and functional approach, reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and calls upon States to implement the ICAO Cyber security Strategy.

Strategy of ICAO

ICAO's vision for global cyber security is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow. This can be achieved through:

- Member States recognizing their obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cyber security;

- Coordination of aviation cyber security among State authorities to ensure effective and efficient global management of cyber security risks, and

- All civil aviation stakeholders committing to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security and continuity of the air transport system.

The 56th Conference of Directors General of Civil Aviation of Asia and Pacific Regions

- The 56th Conference of Directors General of Civil Aviation of Asia and Pacific Regions was recently held in Kathmandu, Nepal from 19 to 23 August 2019. On this conference, IATA has presented the discussion Paper regarding the Aviation Cyber Security.

- It was mentioned that Global Aviation being one of the most complex and integrated systems of information and communications technology in the world it is a potential target for a large-scale cyber-attack and cyber threats to the civil aviation sector are real and their likelihood is increasing. Due to the increased digitization and connectivity as well as interdependent and global nature of the aviation sector, cyber security incidents could rapidly scale up and have impact internationally.