PATNA WOMEN'S COLLEGE 1940

**Computer Science (BCA)**

**Explore–Journal of Research**
**ISSN** 2278 – 0297 **(Print)**
**ISSN** 2278 – 6414 **(Online)**
© Patna Women's College, Patna, India
http://www.patnawomenscollege.in/journal

# Cyber Crime and Cyber Security: Different sides of the same coin

• **Ankita Kumari** • **Nandita** • **Deep Mallika**
• **Anshu**

Received : November 2016
Accepted : March 2017
**Corresponding Author : Anshu**

**Abstract :** *Cybercrime is posing a very serious threat in today's world. The cyber criminals are always in search to find out the new ways to attack the possible internet victims. Our attention is usually drawn to "Cyber Security" when we hear about "Cyber Crimes". Thus, Cyber Crime and Cyber Security can be treated as "Different sides of the same coin".*

*Our cyber security research focuses mostly on combating cybercrime and protecting the social fabric.*

*This paper is an attempt to provide a glimpse of various types of cybercrimes prevalent in modern technological society and what steps can be taken to protect ourselves from these cybercrimes.*

*We focus on a case study of fighting cybercrime in India and Bihar; discuss problems faced.*

***Keywords:*** *Cyber Crime, Denial of Service (Dos), Cyber Stalking, Phishing,Spoofing,Cyber, Criminals, Cyber Security, IDS, DIDS.*

**Ankita Kumari**
BCA III year, Session: 2014-2017,
Patna Women's College, Patna University, Patna,
Bihar, India

**Nandita**
BCA III year, Session: 2014-2017,
Patna Women's College, Patna University, Patna,
Bihar, India

**Deep Mallika**
BCA III year, Session: 2014-2017,
Patna Women's College, Patna University, Patna,
Bihar, India

**Anshu**
Asst. Professor, Department of BCA,
Patna Women's College, Bailey Road,
Patna – 800 001, Bihar, India
E-mail : sayhi2anshu@gmail.com

## Introduction :

Cybercrime has fast established itself as the "Achilles heel" of living in the cyber age.

Cybercrime is part of a continuum of activity that ranges from cyber safety challenges to threats to national security.

Cybercrime can encompass criminal activity from cyberbullying to state-sponsored theft of intellectual property.

Cybercrime can be devastating to individuals, communities and business at both ends of the scale.

Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk, stemming from both

physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

**Objectives :**

- To spread awareness of how Cyber Crime is threatening an individual's or society's or nation's security.
- To explain a clear picture of processes which are undertaken to minimize or defend cybercrimes.
- Acquire a sharp understanding of how cybercrimes can create an economic loss to a nation as well as deteriorate global economy.

**Hypotheses :**

- EXCESSIVE RELIABILTY on technology is the major reason behind the rapid increase of Cyber Crime and for this very reason there is unawareness about Cyber Security.
- We hypothesize that each of these groups of predictors impact:
  - people's decision to reduce online participation,
  - consumer behavior

  We concluded that concern over cyber crime imposes greater opportunity costs in terms of reducing online participation than actually experiencing cyber crime.

***Methodology :***

- **Research Strategy:** Initiatives and activities aimed at increasing awareness of the risks posed by cybercrime will be prioritised, with the goal of promoting behavioural change and raising capability to mitigate those risks.
- **Research Questions:**These questions provided a basis for the research in order to find the awareness of Cyber crime and Cybersecurityamong respondents.
- **Priority Actions :**
  1. Build capability to address cybercrime
  2. *Enhancing response to cyber incidents*
  3. *Combating cybercrime*
- **Sample and Respondents:**The primary target respondent was a working professional who was aware of the various computer crimes and security issues within his/her organization.

  Strengthening the security and resilience of cyberspace has become an important homeland security mission.

***Observations :***

The observation from this research study highlights several facts.

**1. Threat perception of cybercrime in India:** In this increasingly hyper-connected world,cybercrime has emerged as a major threat, as is acknowledged by an overwhelming 89% of our survey respondents (Fig. 1).

**2. Trends of cybercrime in India :** The respondents have experienced cybercrime in the last year. It's evident that only half of the respondents have been victims of cyber attacks in the last year, which indicated that the number of cybercrime incidents in India has been on the rise (Fig. 2).

**3. Impact of cybercrime in India :** 48 per cent of the respondents indicated that they suffer disruption of their business processes and reputation damage as a result of a cyber attack. Cyber attacks have often led to financial losses (either direct or indirect) as indicated by 45 per cent of our survey respondents (Fig. 3).

**4. Sectors prone to Cybercrime :** 58% of our survey respondents perceive financial services sector as more likely to be prone to cybercrime. In this sector, the value to the attacker would be internet banking and brokerage (Fig. 4).

**5. Motivation for Cyber Attacks :** (Fig. 5)

**6. Targets of Cyber Attacks :** 58% indicated that cybercrime attacks are now taking the shape of an organised crime for illicit financial gains / money or to cause unsolicited malicious damage (Fig. 6).

**7. Measure taken to prevent Cyber Crime:** In the present scenario, Cyber crime has become a major threat, which needs to be prevented . Yes, it is true that we cannot prevent it 100% but what we can do is take strict measures to safeguard ourselves and protect others (Fig. 7).

**Case Study : India**

India is yet to realize the full potential and benefits of a public-private partnership in the cybersecurity as well as cybercrime space (Fig. 8).

- ACCUSED IN RS 400 MILLION SMS SCAM ARRESTED IN MUMBAI
- CITY PRINCIPAL SEEKS POLICE HELP TO STOP CYBER CRIME
- UTI BANK HOOKED UP IN A PISHING ATTACK
- ONLINE CREDIT CARD FRAUD ON E-BAY

**Case Study : Bihar**

- PATNA POLICE'S CYBERCRIME CELL STILL DEFUNCT
- CYBERCRIME CELL YET TO BE A REALITY IN STATE (Fig. 9)

**Steps taken to Promote Cyber Security in Patna:** (Fig. 10)

**Contribution of Patna Women's College to Promote Cyber Security :** (Fig. 11)

**Conclusion :**

- **A look to the future and roadblocks in the present :** Cyber attackers have now taken advantage of the increasing popularity of mobile phone applications and games by embedding malware into them. Despite the increasing cyber threat risks, many people are not aware of cybercrimes. Cyber threats can be hard to quantify in terms of likelihood and business impact. As a result, many people do not fully understand the nature of the threat and tend to inaccurately assume that cyber security is a technical issue.
- **A way forward :** Adopting a preventive approach towards cybercrime can reduce the number of cybercrimes and may not cause loss either for the individual or for the nation. So let's secure ourselves and hope for a "**SECURED INDIA"**.

**"India fights against Cyber Crime"**

**LIST OF FIGURES**

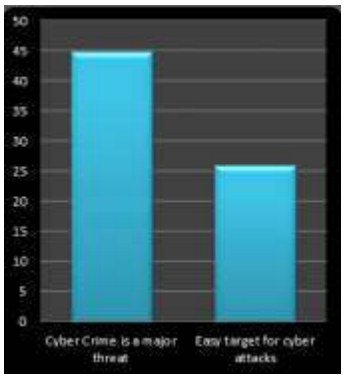


**Fig. 1**

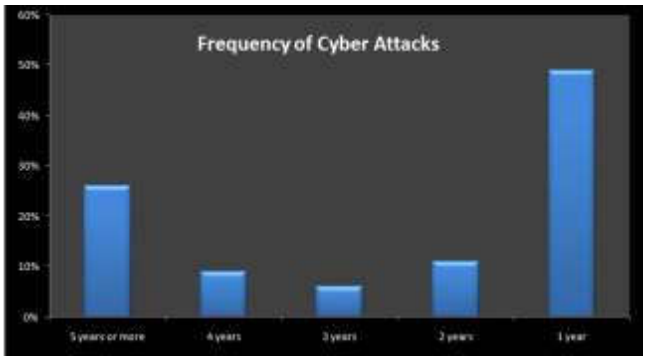


**Fig. 2**


**Fig. 3**

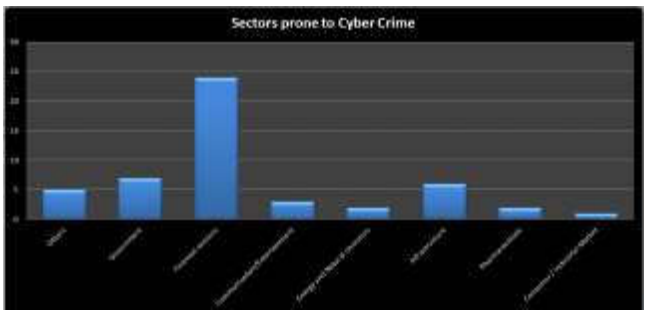


**Fig. 4**

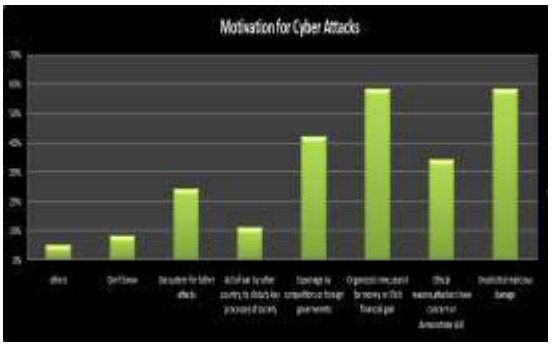


Fig. 5

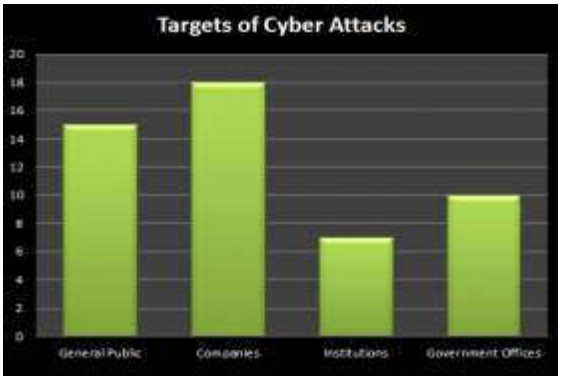


Fig. 6


Fig. 7

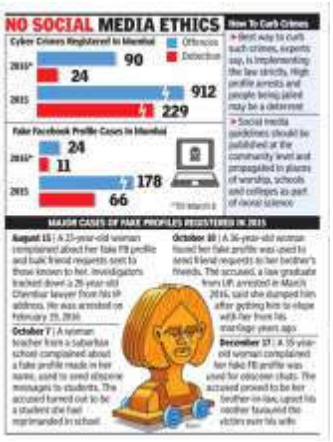


Fig. 8


Fig. 9

साइबर सिक्योरिटी के लिए एथिकल हैकिंग टूल जरूरी

सीयूएसबी में साइबर सिक्योरिटी पर सेमिनार का आयोजन

patna@inext.in

PATNA(7 Oct) : साउथ बिहार सेंट्रल यूनिवर्सिटी (सीयूएसबी) के कम्प्यूटर साइंस डिपार्टमेंट में बुधवार को साइबर सिक्योरिटी विषय पर सेमिनार का आयोजन किया गया. मुख्य वक्ता सेक्लब्स सिस्टम्स प्राइवेट लिमिटेड के सीईओ शेष सारंगधर ने कहा कि किसी भी देश की सुरक्षा के लिए साइबर सिक्योरिटी बहुत ही आवश्यक है. एथिकल हैकिंग बहुत ही उपयोगी टूल है. इंटरनेट की दुनिया में नए तकनीक का आविष्कार हो रहा है. लाखों की संख्या में हर दिन वेबसाइट लांच हो रहे हैं. ऐसे में डेटा को हैकिंग से सुरक्षित रखना एक बहुत बड़ा चुनौतीपूर्ण कार्य है. इसी को ध्यान में रखकर वेबसाइट डेटा को सुरक्षित रखने के लिए वेबसाइट ऑनरों की ओर से कानूनी तौर पर एथिकल हैकर को नियोजित किया जाता है जो लगातार शोध करते रहते हैं. एथिकल हैकर का प्रमुख कार्य कानून के तहत वेबसाइट की सुरक्षा सुनिश्चित करने के साथ-साथ संबंधित तकनीकी गड़बड़ी को ठीक करना है. कंप्यूटर साइंस विभाग के हेड डॉ आर राजेश, डॉ प्रभात रंजन, नेमी चन्द राठौर, हस्मता रौय एवं जयनाथ चाटय मौजूद थे. चौधराजो मो मुदस्सीर आलम ने बताया कि सारंगधर के साथ-साथ टीम के सदस्य राहुल एवं आनंद ने भी एथिकल हैकिंग पर विचार रखे.

Fig. 10


Fig. 11

***References:***

http://www.computerworld.com/category/cybercrime-hacking

http://techin.oureverdaylife.com/types-cyber-crimes-penalities-1808.html

http://internetsecurity101.net/top-11-cybercrime-prevention-tips/

http://paperpresentationtopicsandpapers. blogspot.com/2010/01/cyber-crime-and-security. html?m=1

http://www.enotes.com/research-starters/social-impacts-cyber-crime

http://www.cyberlawsindia.net/cases.html