Mapping the Cyber Crime Landscape :

Threat Actors, Target, Motives and Vectors: Case Stories

Why map and measure cybercrime?

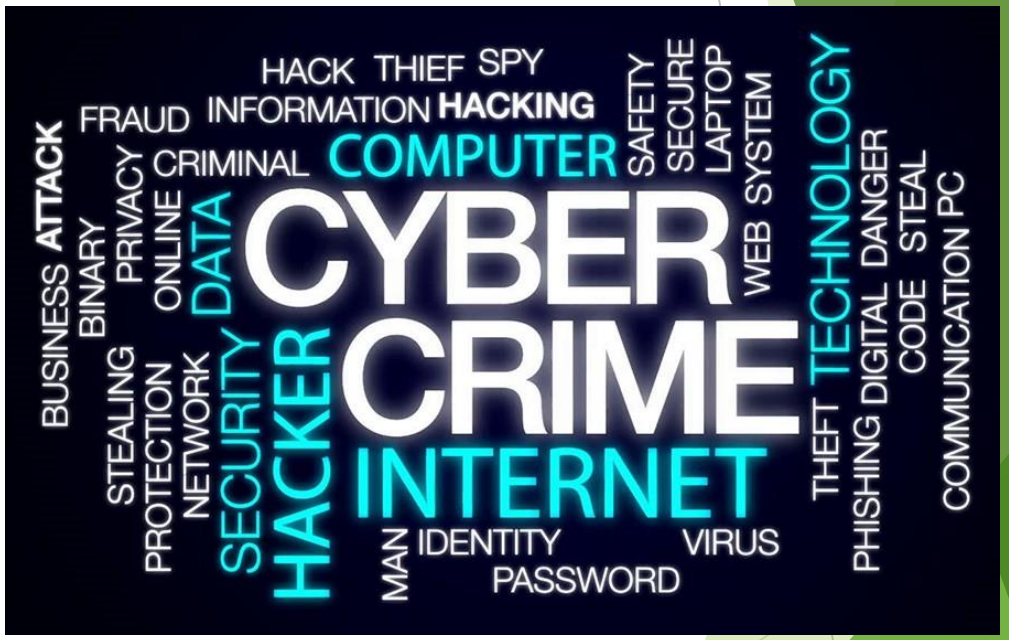
- What is the nature and extent of cybercrime? It seems to be a simple question, yet it is currently impossible to answer in terms of incidence and prevalence across populations.
- In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that nearly one percent of global GDP, close to $600 billion, is lost to cybercrime each year.

Cybercrime real time threat map

- https://www.fireeye.com/cyber-map/threat-map.html
- https://cybermap.kaspersky.com/
- https://threatmap.checkpoint.com/

Cyber Crime:

Cybercrime is any type of criminal activity that involves the use of a computer or other cyber device and/or network.



- Computers used as the tool
- Computers used as the target

Classification of Cybercrime

It can be classified into four major categories as:

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society

Other classifications

- **Cyber-dependent crimes:** offences that can only be committed by using a computer, computer networks, or other form of ICT.
- For example spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks.
- Primarily directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

- **Cyber-enabled crimes:** These are traditional crimes that are increased in scale or reach by the use of computers, computer networks or other ICT.
- Examples can include fraud (including phishing and other online scams), theft, and sexual offences against children.

Further

- Financial fraud crimes
- Cyberterrorism
- Cyberextortion
- Cybersex trafficking
- Cyberwarfare
- Obscene or offensive content
- Online harassment
- Drug trafficking
- Cyber mis-information/fake news
- Identity theft

Latest Trends in Cybercrime

- Politically-motivated attacks are on the rise
- Increased attention to public utilities being paid by foreign hackers
- Distributed denial of service (DDOS) attacks using the Internet of things (IoT)
- Increasing sophistication in spear phishing attacks
- Cyber criminals are using tools and techniques to make detection even more difficult
- Zero-day attacks are on the decline

Cybercrime Facts

- Cybercrime has recently surpassed illegal drug trafficking as a criminal money-maker
- A personal identity is stolen once every 3.1 seconds as a result of cybercrime
- Nearly half of all cybercrimes are committed against small businesses
- Exponential growth in the number of potential victims including: smartphones, cars, railways, planes, power grids, security cameras, IoTs etc.
- Hacking tools for sale and Hackers on hire
- Digital currency laundering services
- Hosting services designed for malware
- “Customer service” centers for ransomware
- The Dark Web is home for a huge array of criminal services and products

Factors that enable Cybercrime

- **Connectivity**: more individuals/devices online
- **Mobility**: businesses online with staff working remotely on less secure networks
- **Cyber knowledge**: low levels of digital security awareness and cyber hygiene
- **Sophistication**: threat actors with evolving skills and tactics
- **Under-reporting**: reluctance to report cybercrime offences

  This failure to report crimes means there is a lack of data on how cybercriminals are operating and the technologies used to commit crimes.
- **Legislation and jurisdiction**: lack of criminalization of cybercrime and cross-jurisdictional complexity

Threat Actors

- **CYBER THREAT**: A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.
- **CYBER THREAT ENVIRONMENT** is the online space where cyber threat actors conduct malicious cyber threat activity.
- **CYBER THREAT ACTORS**: Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in any different place.

TOP 15 CYBER THREATS

enisa

1 

Malware

2 

Web-based attacks

3 

Phishing

4 

Web application attacks

5 

Spam

6 

DDoS

7 

Identify theft

8 

Data breach

9 

Insider threat

10 

Botnets

11 

Physical manipulation, damage, theft and loss

12 

Information leakage

13 

Ransomware

14 

Cyberespionage

15 

Cryptojacking

Motives

Cybercrime is committed by threat actors with different motivations:

- Hacktivists who use the Internet as a means of protest
- Criminals, such as:
  - opportunistic or curious beginners testing their skills
  - online child abusers
  - organized crime groups intent on making money
- Nation-state sponsored advanced persistent threat (APT) groups who carry out espionage, raise funds or attack critical infrastructure.

The Cyber Threat Spectrum

THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

CYBER THREAT ACTOR		MOTIVATION
NATION-STATES		GEOPOLITICAL
CYBERCRIMINALS		PROFIT
HACKTIVISTS		IDEOLOGICAL
TERRORIST GROUPS		IDEOLOGICAL VIOLENCE
THRILL-SEEKERS		SATISFACTION
INSIDER THREATS		DISCONTENT

Targets

ACTOR	MOTIVE	TARGETS
Nation States	Economic or Military	IP or Infrastructure
Organized Crime	Financial Gain	IP, Banks, PoS
Terrorists / Extremists	Cause Support	Highly Visible Targets
Hackers / Hacktivists	Publicity, Watch it burn	Anything and Everything
Trusted Insiders	Revenge, Financial Gain	Your Data and/or Networks

Vectors

- **Cyber Attack vector:**

The method or way by which an adversary can breach or infiltrate an entire network/system. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

- **Attack surface:**

The sum-total of points on a network where attacks can occur where an unauthorized user (the “attacker”) can try to manipulate or extract data using a myriad of breach methods (the “cyber attack vectors”).

1. The network
2. Users
3. Email
4. Web applications
5. Remote access portals
6. Mobile devices

Threat vectors are categorized as either programming or social engineering

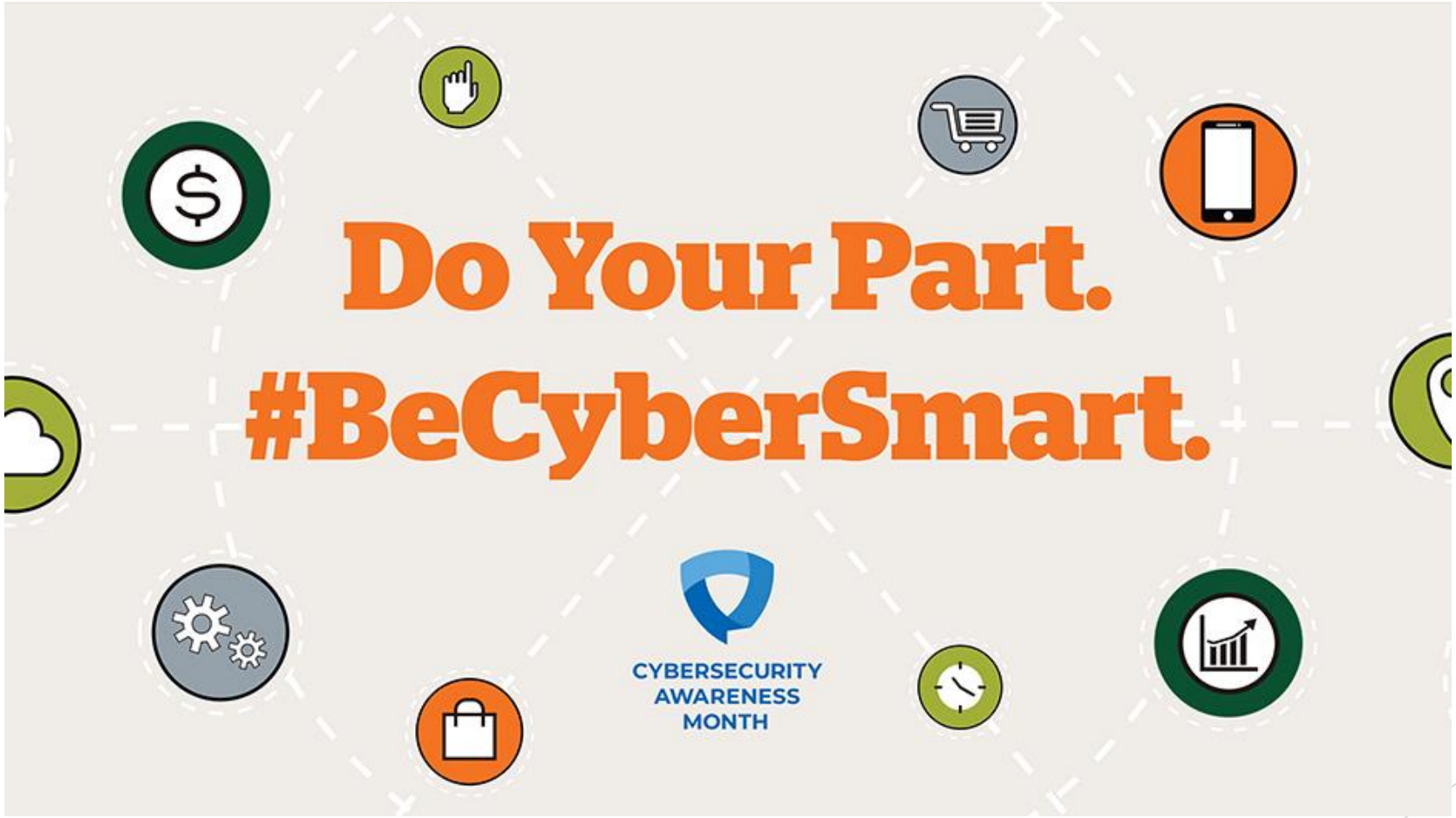
Programming Threat Vectors	Social Engineering Threat Vectors
Viruses	Instant messages
Trojans	Text messages
Malware/ransomware	Chat room messages
Macros	Poor password protection
Pop-ups	Phishing
Bogus email attachments or web links	Baiting
Drive-by-downloads	Spoofing
Rootkits	Cybersquatting
SQL injection	Man-in-the-middle or session hijacking
Unpatched vulnerabilities	Credential reuse
Brute force/cracking	Domain shadowing or hijacking
Distributed denial-of-service (DDoS)	Malvertising
Misconfigured cloud services like Google Cloud, Amazon Web Services (AWS)	Disgruntled employees

- **Virus** - A non-autonomous program that replicates and spreads by infecting (attaching itself to) systems, programs or files.
- **Worm** - Code that is able to replicate and spread autonomously through systems and networks.
- **Trojan horse** - A program containing unexpected hidden functionality, potentially operating alongside expected behaviour
- **Software Bomb** – An element of malicious code, typically hidden within a larger program, that is activated on the basis of either a time-based trigger (time bomb) or a logical condition being met (logic bomb).
- **Adware** – software that automatically displays banner or pop-up advertisements, or redirect search requests to advertising websites. Adware is not necessarily malware, can be classed as such when used in the hands of cybercriminals.
- **Crimeware** – a broad category, referring to malware designed to conduct or enable illegal online activities.
- **Ransomware** – malware that blocks users' access to their data (typically by encrypting it) unless a ransom is paid to recover it.
- **Spyware** – malware designed to gather and share information without the knowledge of the individual or organisation using the infected system.

Why is it important to think in terms of threat vectors?

- Once the vulnerable threat vectors are identified, strong cybersecurity can decrease the number of attack surfaces a cybercriminal can use.
- Some prevention strategies include:
  - Multi-factor authentication
  - Strong password policies
  - Offline backup
  - Strict policy enforcement
  - Continuous employee training
  - Additional smart device security
  - Web filters
- No single method alone is foolproof. Just as there are multiple threat vectors, there should be multiple layers of security and protection.

Cyber awareness and cyber hygiene



How to report a Cybercrime?

- https://cybercrime.gov.in/
- For Cybercrime awareness
  - @Cyberdost (twitter)
  - #cyberdost (youtube)

- Cyber Crime Wing, CID, Meghalaya Police,
  - Email: ccw-meg@gov.in
  - Telephone: 0364-2504001
    9402519391
  - Toll free helpline: 155260

Case Stories