

Ethical Hacking

Table of contents

- Course outcome and course objectives
- Module wise syllabus discussion
- ISE Plan
- Market Analysis
- Introduction to ethical hacking
- 60 sec data
- Technology Triangle
- Security objective
- Vulnerabilities, threat and attacks
- Phases of ethical hacking

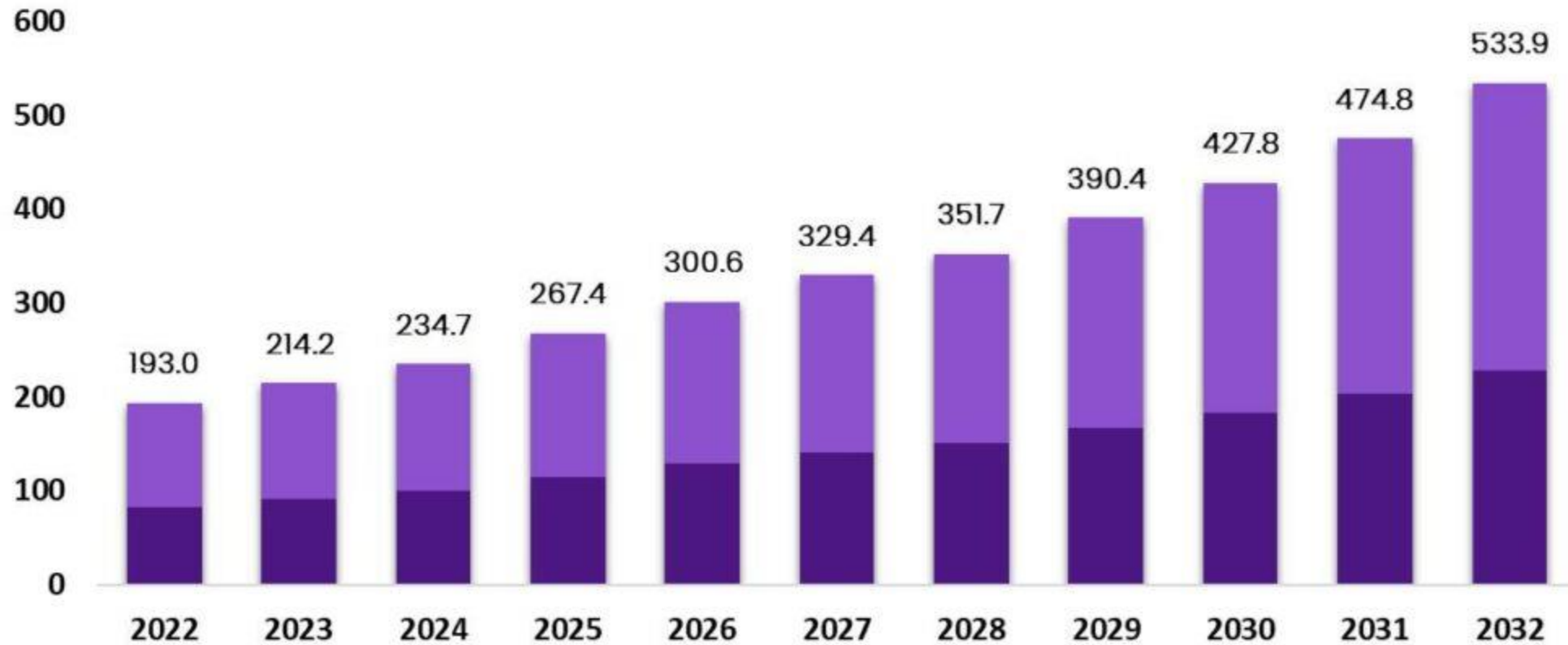
Market Analysis

Global Cyber Security Market

Size, by Component Type, 2022-2032 (USD Billion)

■ Solutions

■ Services



The Market will Grow
At the CAGR of:

11%

The forecasted market
size for 2032 in USD:

\$533.9B



market.us
ONE STOP SHOP FOR THE REPORTS

BY REGION



KEY COMPANIES

- AlgoSec
- BAE Systems Inc.
- Centrify Corporation
- Cisco Systems Inc.
- CyberArk
- DataVisor
- EMC Corporation
- Intel Security
- LogRhythm Inc.
- Palo Alto Networks
- F5
- Fortinet, Inc.
- F-secure
- Hewlett-Packard Enterprise
- IBM Corporation
- Proofpoint Inc.
- Qualys
- RevBits
- SentinelOne
- SonicWall

BY TYPE

- Enterprise
- Network
- Application
- Endpoint
- Others

BY DEPLOYMENT MODE

- On-Premise
- Cloud-Based

BY END-USER

- BFSI
- IT & Telecom
- Healthcare
- Retail
- Defense and Government
- Travel and Hospitality
- Others

BY ORGANISATION SIZE

- Large Enterprises
- Small and Medium Businesses

BY SOLUTION

- Encryption
- Unified Threat Management
- Identity and Access Management
- Data Loss Prevention
- Antivirus/Anti-Malware
- Risk and Compliance Management
- Disaster Recovery
- Others

BY COMPONENT

- Solutions
- Service

CAGR
(2022-2030)

9.7%



TOP 15 CYBERSECURITY THREATS

SPRINTZEAL
Empowering Engineers

1



Ransomware Attacks

2



Internet of Things (IoT) Vulnerabilities

3



Social Engineering and Phishing Attacks

4



Supply Chain Attacks

5



AI-Powered Cyber Threats

6



Advanced Persistent Threats (APTs)

7



Zero-Day Exploits

8



Cloud Security Risks

9



Mobile Malware and Vulnerabilities

10



Insider Threats

11



Artificial Intelligence (AI) Misuse

12



Data Breaches and Privacy Violations

13



Advanced Phishing Techniques

14



Nation-State Cyber Attacks

15



Cryptocurrency-Related Threats

Cyber Attacks 2023

[Top 5 Ransomware Attacks in India](#)

[List of Data Breaches and Cyber Attacks in 2023](#)

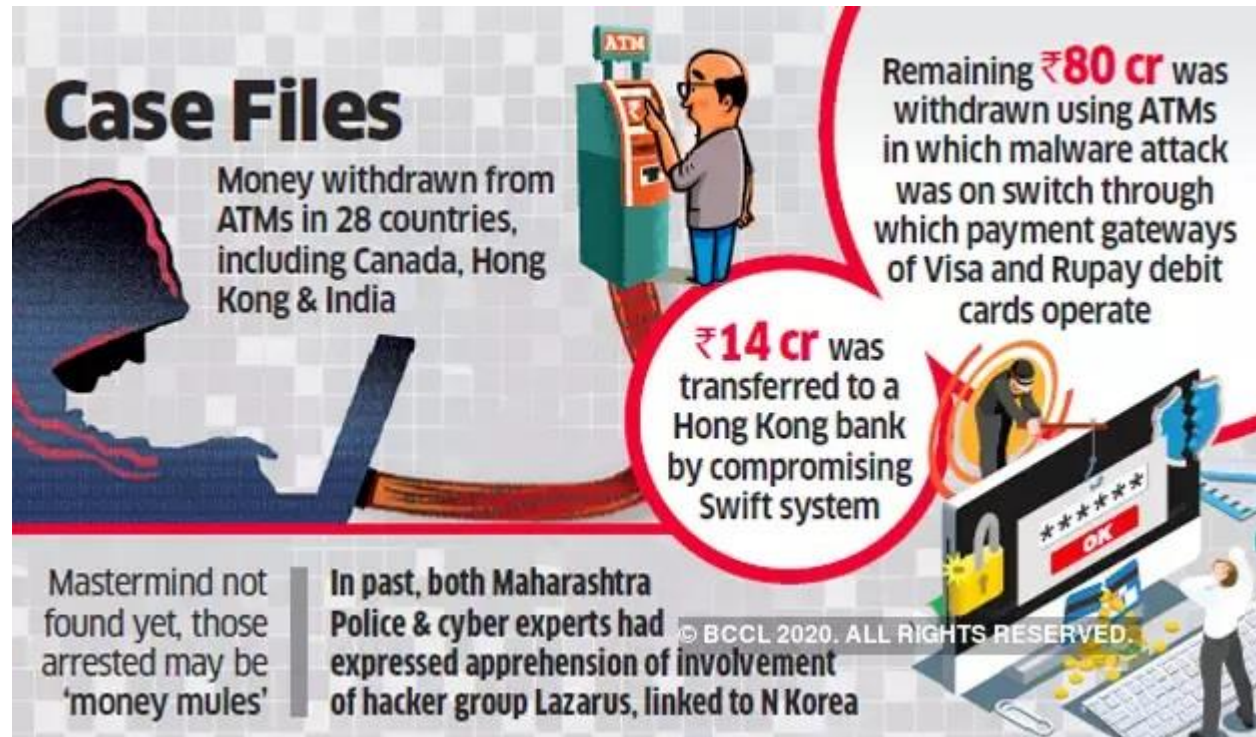
- **SolarWinds**
- **Microsoft Exchange**
- **REvil Demands \$50M Ransom**
- **Colonial Pipeline**
- **Microsoft's (Print)**

Cyber Attacks of 2021

Cyber Attacks of 2020

- **Software AG Ransomware Attack**
- **Telegram Hijack**
- **Seyfarth Shaw Malware Attack**
- **Carnival Corporation Data Breach**

Cyber Attacks in India



The 2019's Biggest Cyber Attacks in India

Cosmos Bank Cyber Attack in Pune

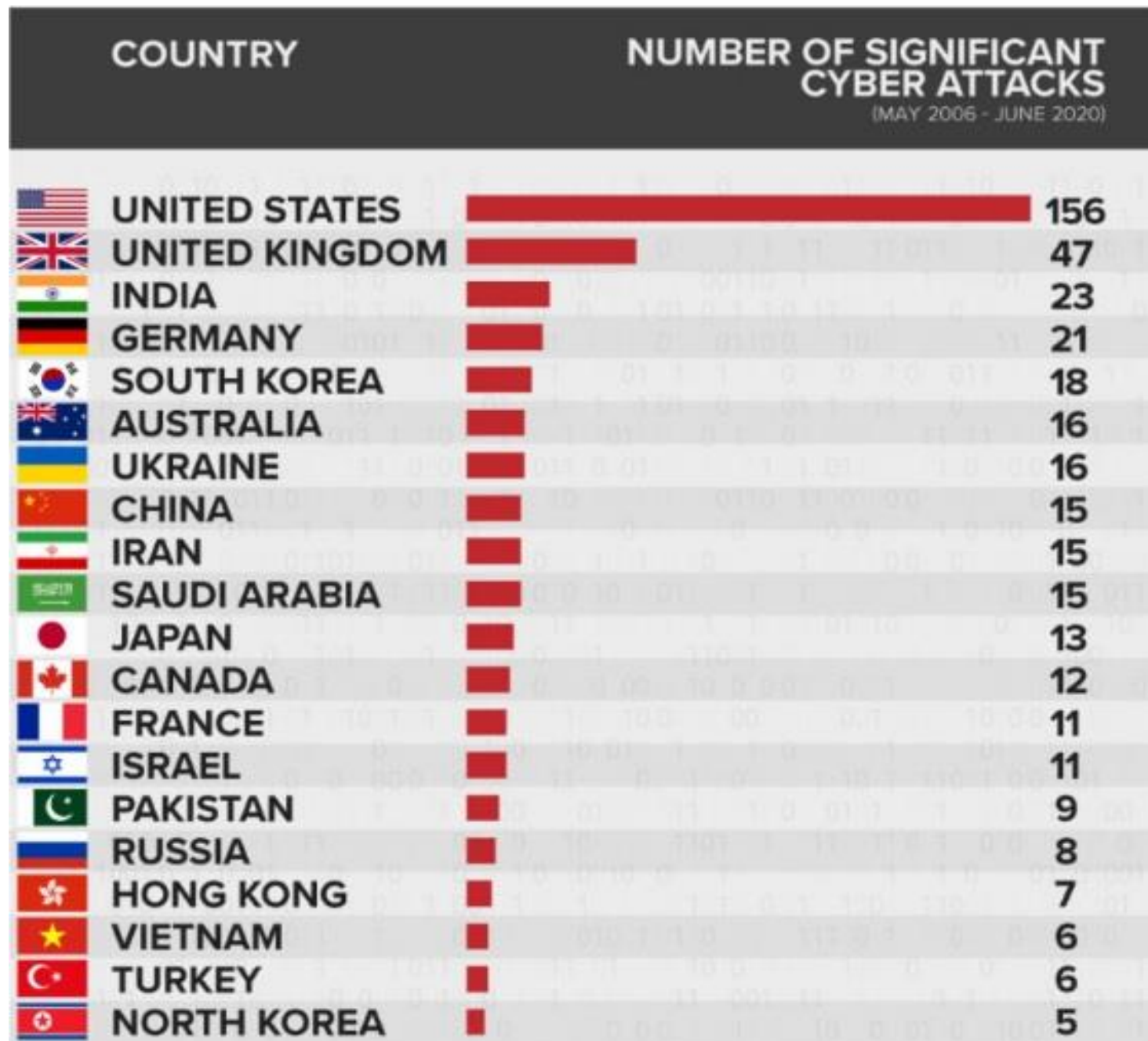
ATM System Hacked

UIDAI Aadhaar Software Hacked

Hack Attack on Indian Healthcare Websites

SIM Swap Scam

Source-[5 Biggest Cyber Attacks in India | Everything You Need to Know | Kratikal](#)



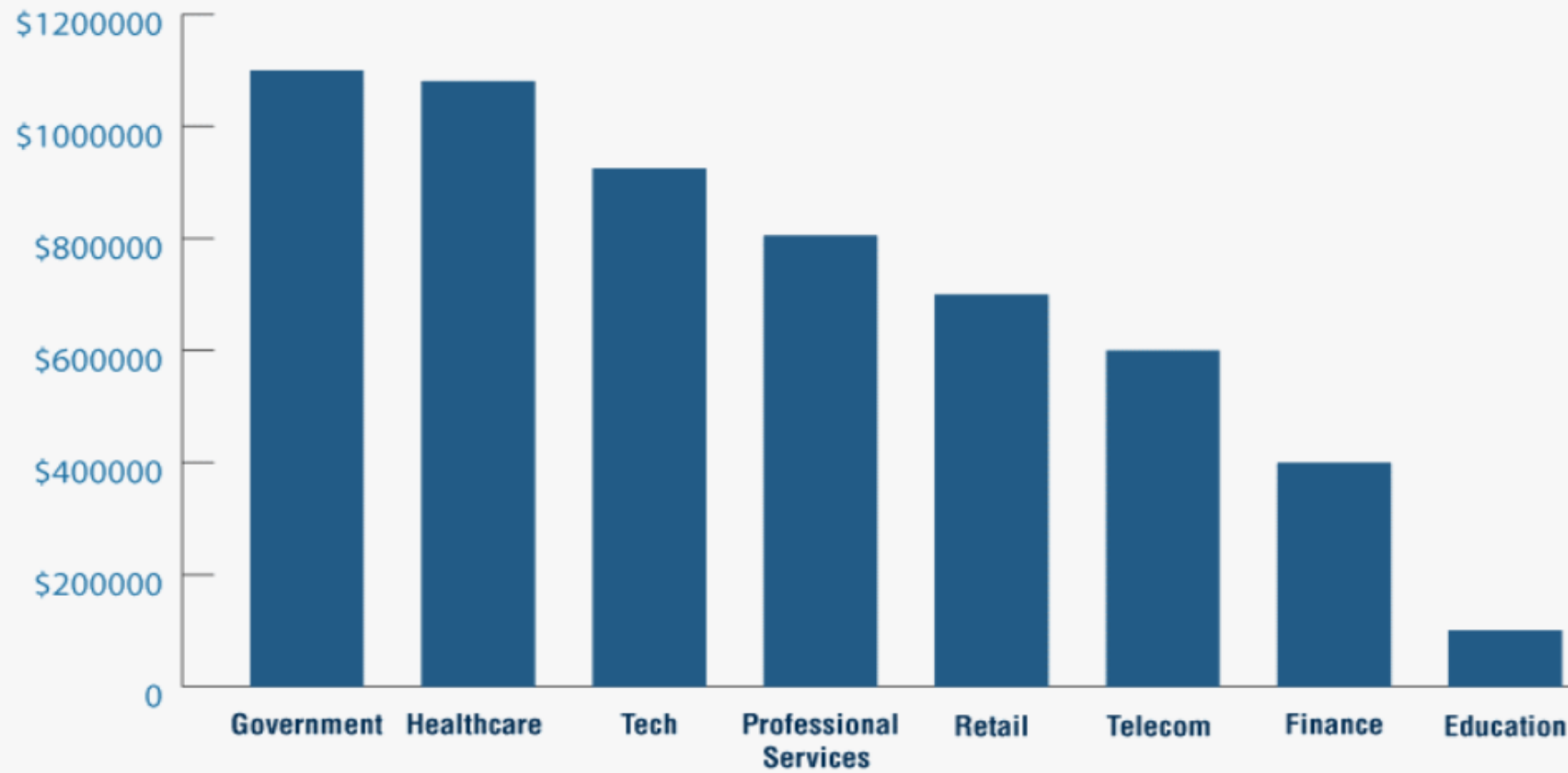
- Source- [India third most 'cyber attacked' country | www.cioandleader.com](http://www.cioandleader.com)

Case Study

Few more from 2014-2015

- ebay
- Google play- Turkish hacker-Malformed APK
- JPMorganChase

Estimated Sector-wise Cyberattack Cost [7]



Estimated cyber-attack cost by sector

Source: Security Magazine

Information Security laws and standards

- Payment card industry data security standard (PCI-DSS)
 - Build and maintain a secure network,Implement strong access control measures,Protect cardholder data,Regularly monitor and test networks,Maintain a vulnerability management program,Maintain an information security policy.
- ISO/IEC 27001:2013
- Health Insurance portability and accountability act (HIPAA)
- Sarbanes oxley act (SOX)
- Digital millennium copyright act(DMCA) and federal information security management act(FISMA)
- India-
 - The patents act,trademark act,copyright act- ipindia.nic.in
 - information technology act dot.gov.in



System/Network Admin

What is Cybercrime?

Introduction to Ethical Hacking

What is Ethics

What is Hacking

The need of Cyber security

Ethical Hacking


What is Ethics



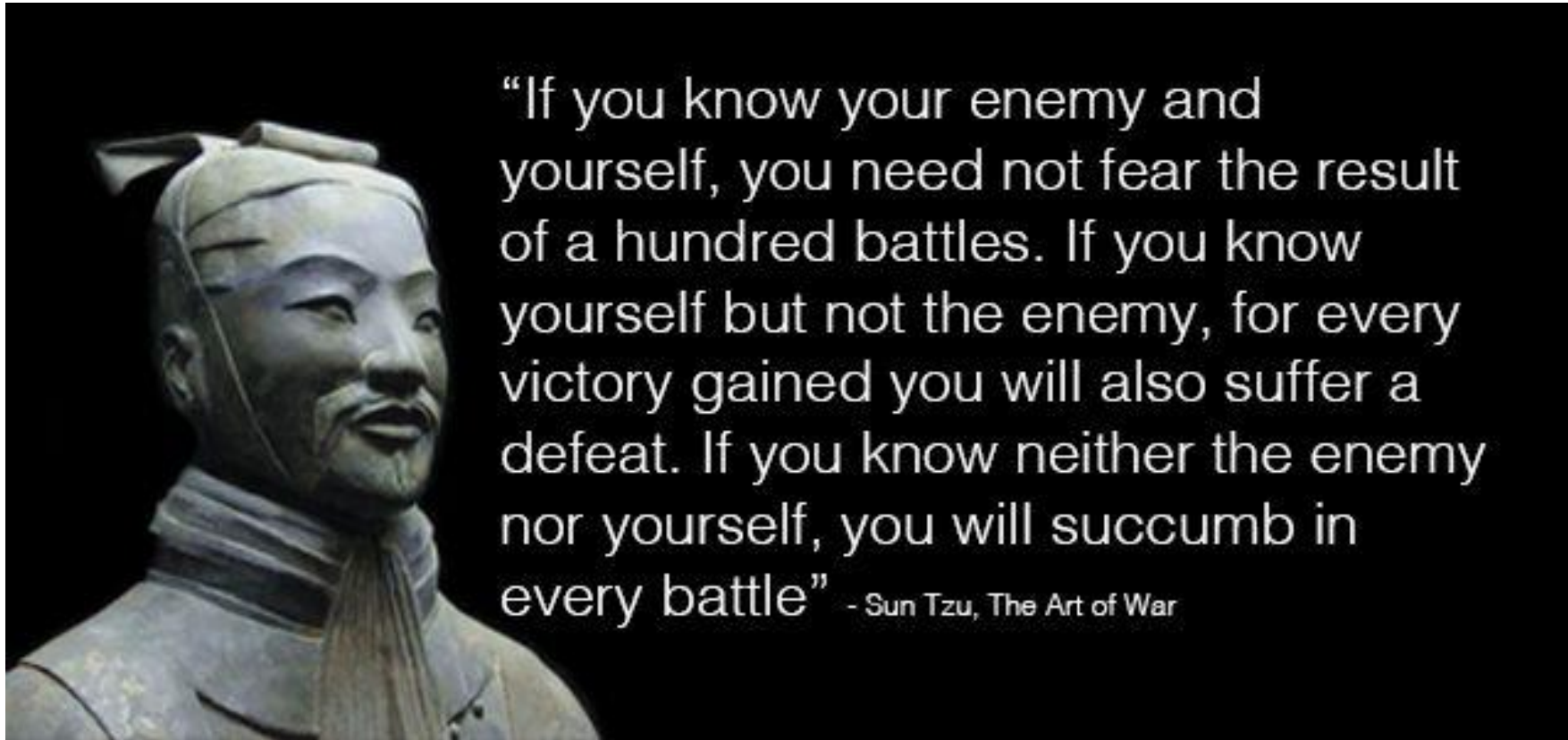
Code of Ethics

['kōd ōv 'e-thiks]

A set of rules and principles designed to encourage ethical conduct among a group of professionals.

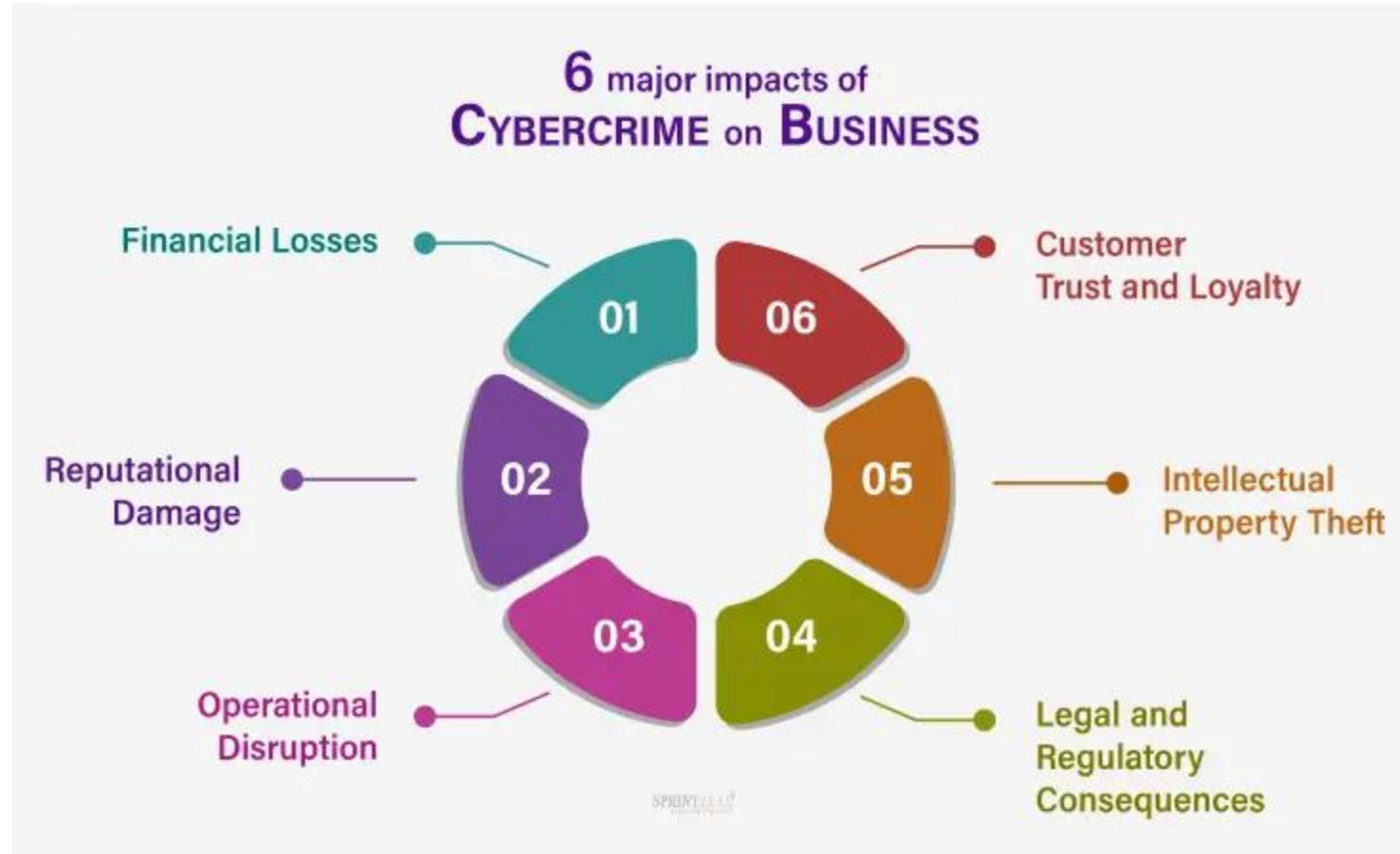
 Investopedia

What is Hacking



Protecting yourself is hacking

The need of Cyber security



Ethical Hacker / Hacker



4,400 Cyber Attacks on Indian Banks Every Day

13.2 lakh cyber attacks took place during January–October 2023



No. of cyber attacks

Vulnerable services

7.2 Lakh
(54.4%)

Unauthorised network scanning

4.4 Lakh
(33.3%)

Virus code

1.4 Lakh
(11%)

Others

15,499 (1.2%)

Phishing
711 (0.1%)

Website Intrusion
Malware Propagation
967 (0.1%)

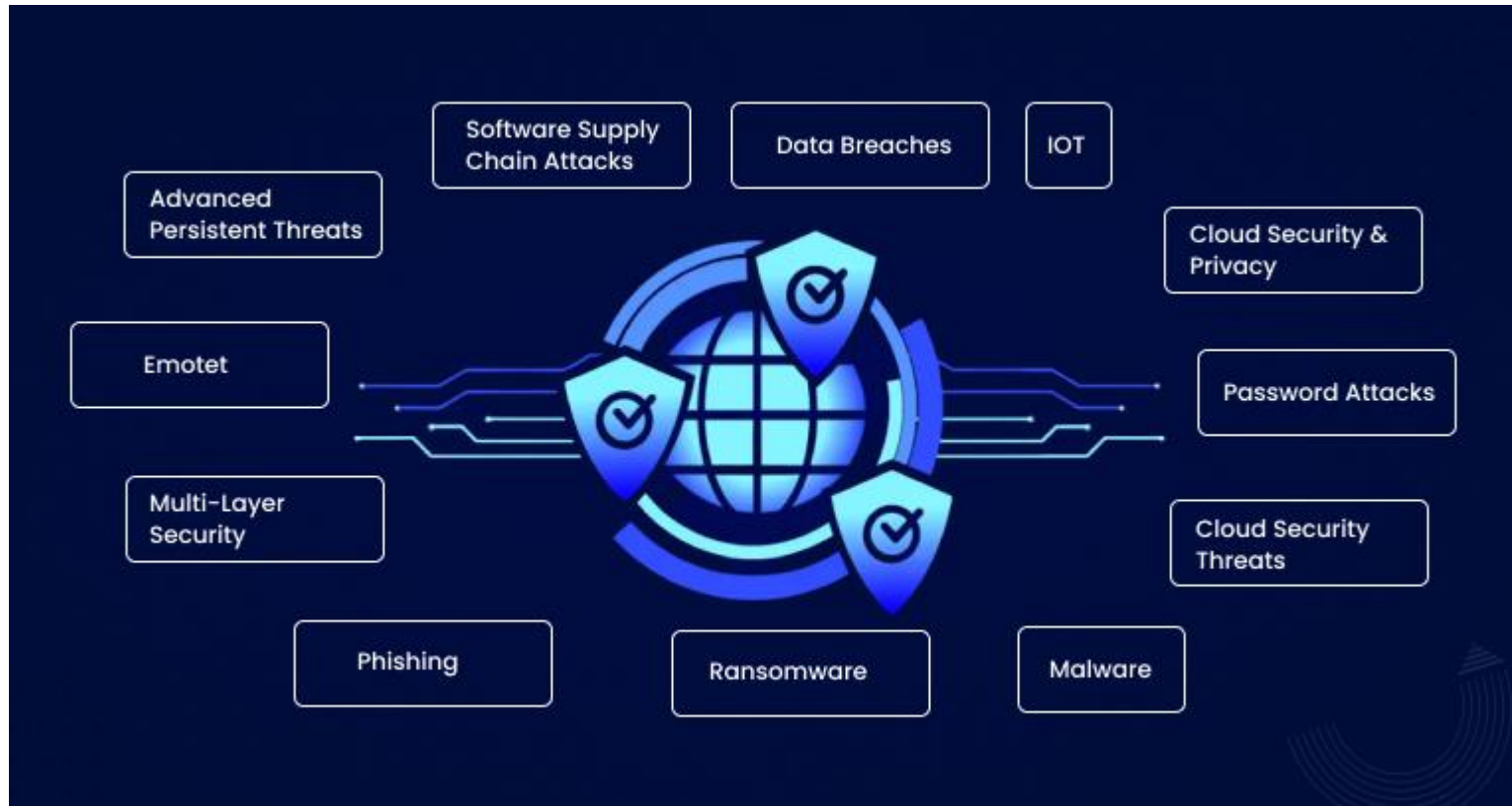


Source: RBI

Graphics: Samrat Sharma & Mudita Singh



Top 12 Biggest Cybersecurity Threats for 2023



What happens online in 60 seconds

THE INTERNET IN 2023 EVERY MINUTE



Created by: eDiscovery Today & LTMG

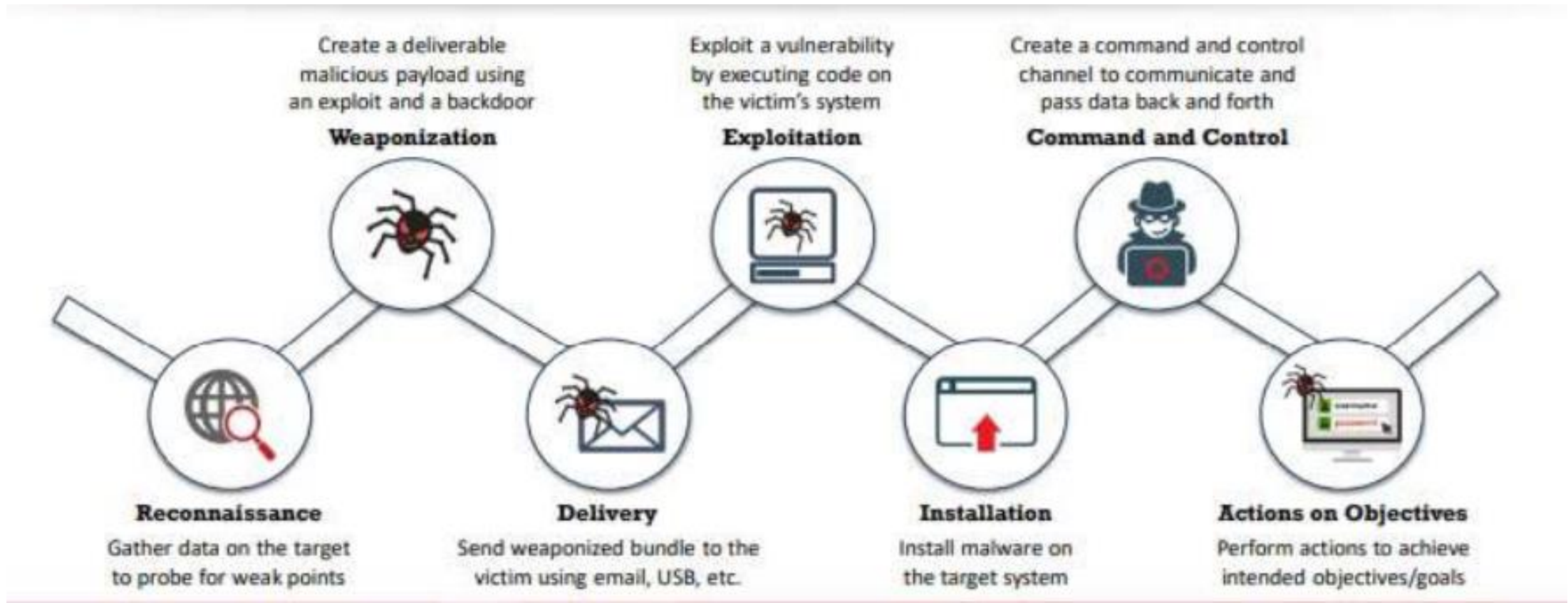
Motives, goals, and objectives of Information security attacks

- Attack
 - Attack = Motive(Goal)+Method+Vulnerability

Classification of Attacks

Passive Attacks	<ul style="list-style-type: none">• Passive attacks do not tamper with the data and involve intercepting and monitoring network traffic and data flow on the target network• Examples include sniffing and eavesdropping
Active Attacks	<ul style="list-style-type: none">• Active attacks tamper with the data in transit or disrupt the communication or services between the systems to bypass or break into secured systems• Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	<ul style="list-style-type: none">• Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or disrupt access to information• Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	<ul style="list-style-type: none">• Insider attacks involve using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems• Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	<ul style="list-style-type: none">• Distribution attacks occur when attackers tamper with hardware or software prior to installation• Attackers tamper with the hardware or software at its source or in transit

Cyber Kill Chain Methodology



What is hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources



- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose



- Hacking can be used to steal and redistribute intellectual property, leading to **business loss**



Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware



02

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise



03

Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**



Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

Types of Hackers around the Globe

- Black Hat
- White Hat
- Grey Hat
- Suicide hacker
- Script kiddies
- Cyber Terrorists
- State sponsored
- hacktivist

Types of Hackers



Black Hat



**Black Hat
Hackers**



**Suicide
Hackers**



White Hat



**White Hat
Hackers**



**Red Hat
Hackers**



**National Supported
Hackers**



Grey Hat

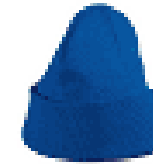


**Grey Hat
Hackers**



**Malicious
Insider**

Junior Hackers



**Script
Kiddies**



**Green Hat
Hackers**



**Blue Hat
Hackers**



Element of Information Security

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-Repudiation

Security, Functionality and Usability Triangle



Threats

- Threats Categories
 - Host
 - Natural
 - Physical
 - Application
 - Human
 - Network

Attack Vectors

- Cloud computing threats
- Advanced persistent threats
- Viruses and worms
- Mobile Threats
- Botnet
- Insider Attack

Vulnerability research

- OS vendors
- Application Vendors
- Hardware vendors
- MAnufacture
- Component vendors
- Security sites/blogs

Hacking Phases

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining access
- Clearing Tracks

