Chapter 1
Fundamentals of Cybersecurity

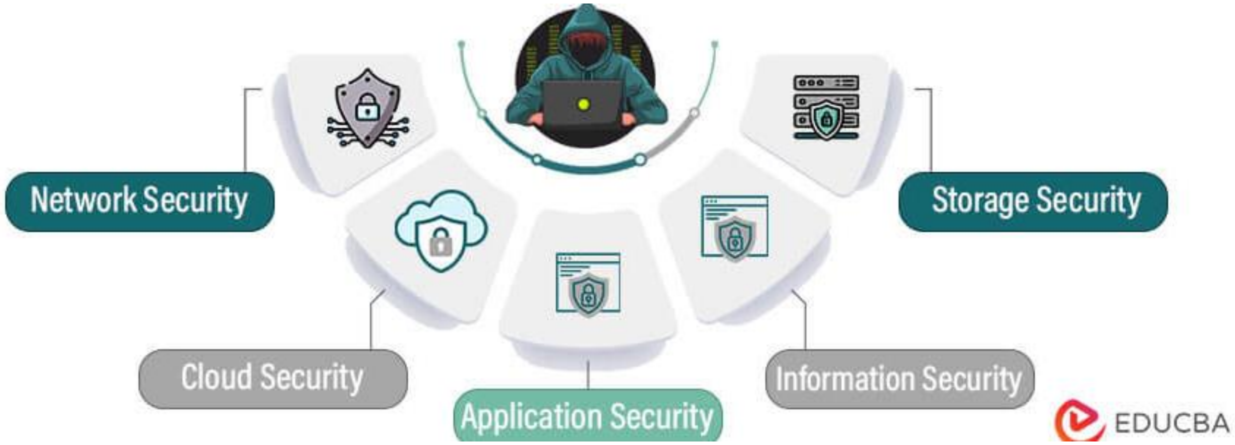
Outline

- Definitions
- CIA Triad
- Motive behind cyber crimes
- Cyber Vocabulary
- Vulnerability
- Threat and Threat actors
- Threat Maps

5W1H framework (Who, What, When, Where, Why, and How)

What is Cybersecurity?

- Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks
- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use
- Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats



Why is it called Cybersecurity?

- Should it be called “Information Security”?
  - No. Because there’s a lot more than securing critical information, we are concerned with hardware, smart city, IoT, etc.

- Should it be called “Network Security”?
  - No, because everything may not be connected to a network

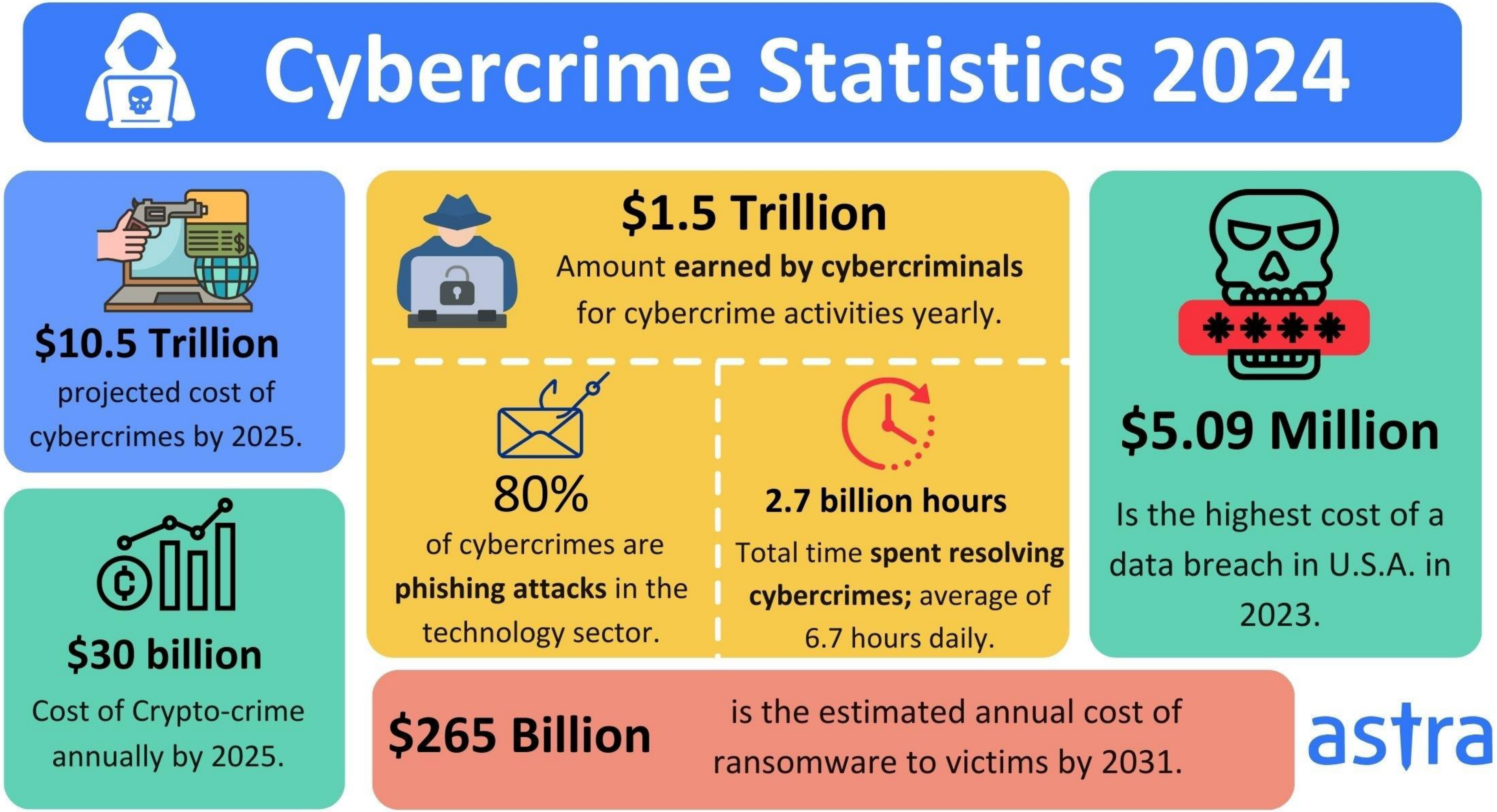
- Should it be called “Computer Security”?
  - No. The computer is not the only thing that is making us vulnerable. Sometimes the best solution (or attack) is not technical. Examples: social engineering, lock picking, impersonation, phishing

Cybersecurity is a broad term that encompasses various aspects of security, including information security, network security, and computer security.

Definition of **cybersecurity** as provided in ITU-T

“**Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that are used to protect the cyberspace environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability, integrity, which may include authenticity and non-repudiation; and confidentiality.”

Why do we need cybersecurity?



Cybercrime Statistics 2024

$10.5 Trillion

projected cost of cybercrimes by 2025.

$1.5 Trillion

Amount **earned by cybercriminals** for cybercrime activities yearly.

80%

of cybercrimes are **phishing attacks** in the technology sector.

2.7 billion hours

Total time **spent resolving cybercrimes;** average of 6.7 hours daily.

$5.09 Million

Is the highest cost of a data breach in U.S.A. in 2023.

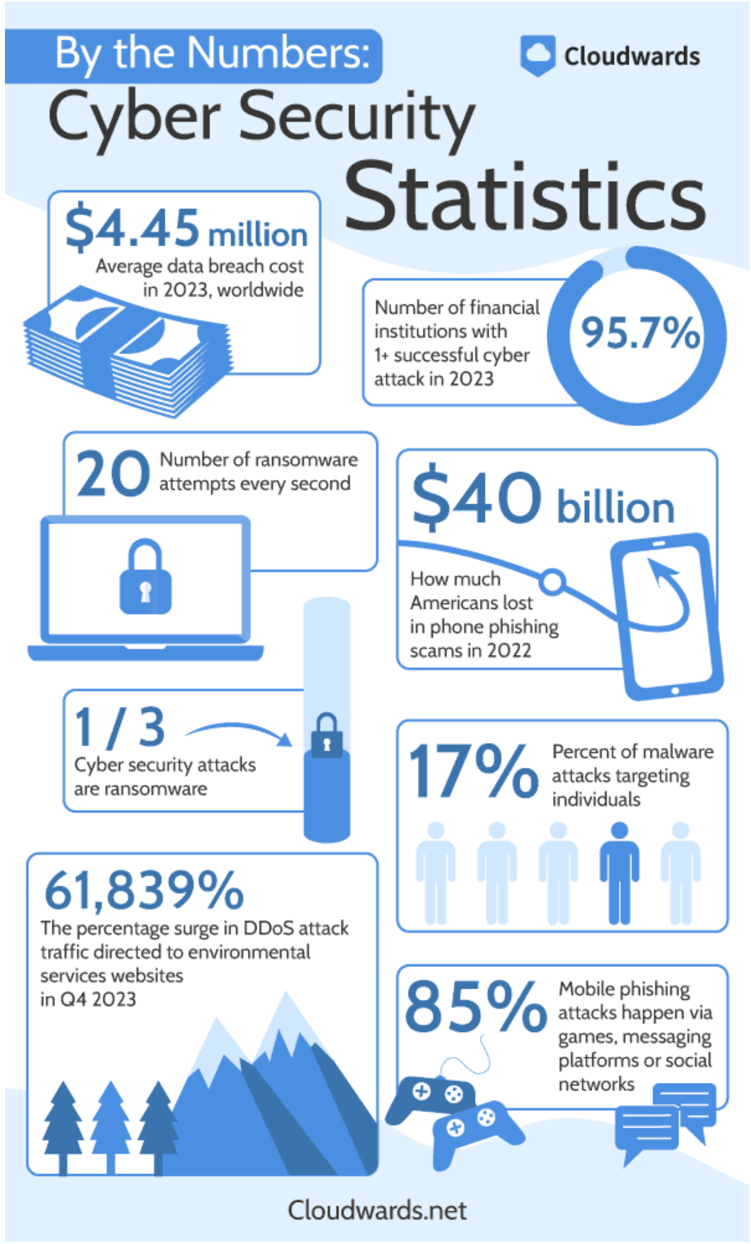
$30 billion

Cost of Crypto-crime annually by 2025.

$265 Billion is the estimated annual cost of ransomware to victims by 2031.

astra

Why do we need cybersecurity?

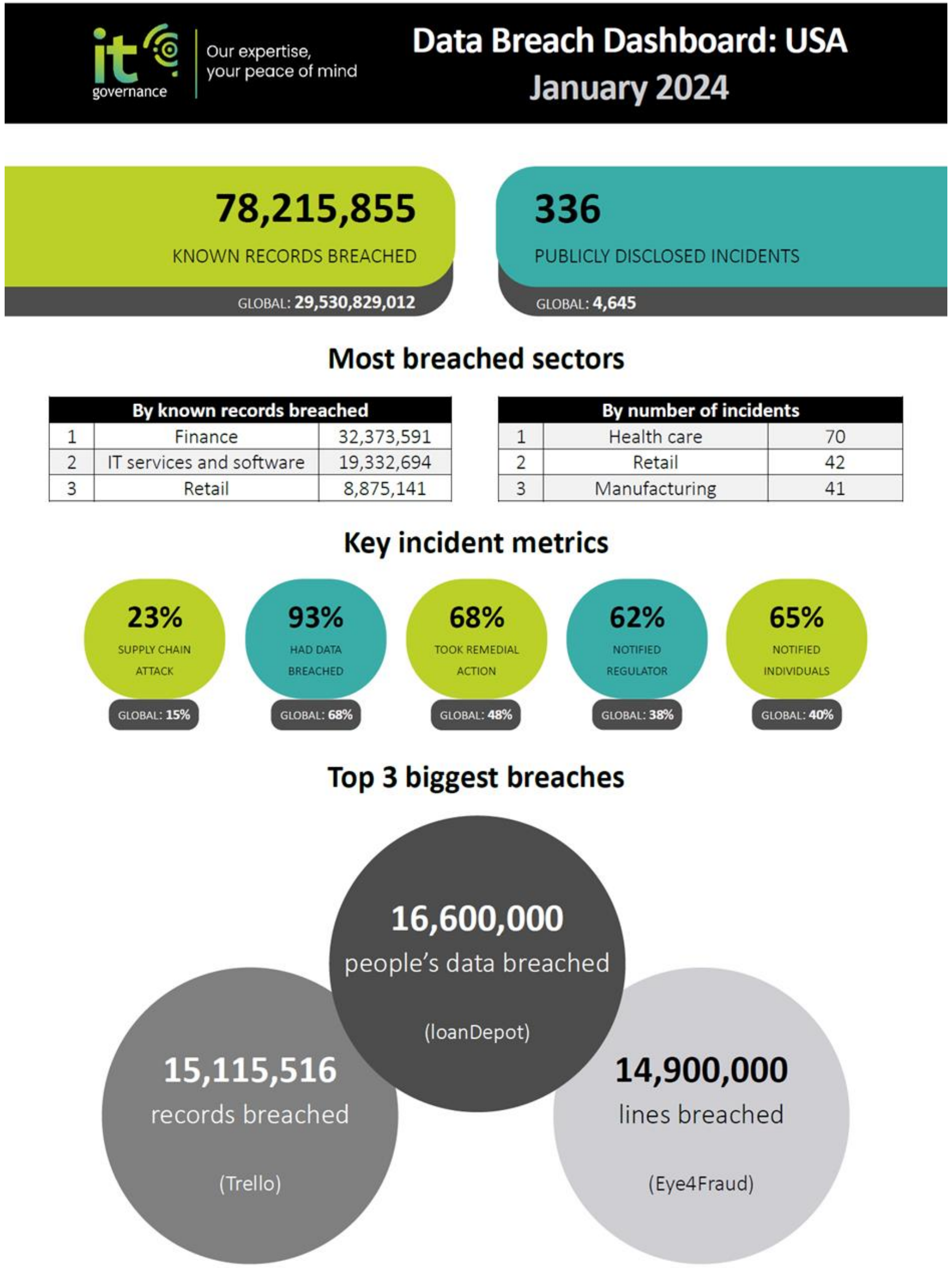

By the Numbers:
Cloudwards
Cyber Security Statistics
$4.45 million
Average data breach cost in 2023, worldwide
Number of financial institutions with 1+ successful cyber attack in 2023
95.7%
20 Number of ransomware attempts every second
$40 billion
How much Americans lost in phone phishing scams in 2022
1 / 3
Cyber security attacks are ransomware
17% Percent of malware attacks targeting individuals
61,839%
The percentage surge in DDoS attack traffic directed to environmental services websites in Q4 2023
85% Mobile phishing attacks happen via games, messaging platforms or social networks
Cloudwards.net

- •On average, there are 2,200 cyber attacks per day, or about one every 39 seconds

- •1 in 10 small businesses suffer a cyber attack each year

- •60% of small businesses go out of business after being victims of a cyber attack

- •Cybercrime is predicted to cost $10.5 trillion by 2025



it governance
Our expertise, your peace of mind

Data Breach Dashboard: USA
January 2024

78,215,855
KNOWN RECORDS BREACHED
GLOBAL: **29,530,829,012**

336
PUBLICLY DISCLOSED INCIDENTS
GLOBAL: **4,645**

Most breached sectors

By known records breached		
1	Finance	32,373,591
2	IT services and software	19,332,694
3	Retail	8,875,141

By number of incidents		
1	Health care	70
2	Retail	42
3	Manufacturing	41

Key incident metrics

23% SUPPLY CHAIN ATTACK — GLOBAL: **15%**

93% HAD DATA BREACHED — GLOBAL: **68%**

68% TOOK REMEDIAL ACTION — GLOBAL: **48%**

62% NOTIFIED REGULATOR — GLOBAL: **38%**

65% NOTIFIED INDIVIDUALS — GLOBAL: **40%**

Top 3 biggest breaches

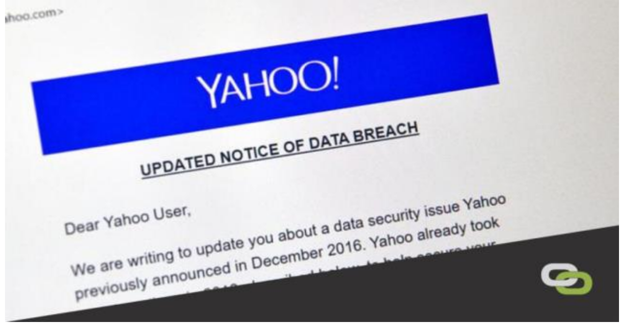
16,600,000
people's data breached
(loanDepot)

15,115,516
records breached
(Trello)

14,900,000
lines breached
(Eye4Fraud)

	Organization name	Sector	Known number of records breached
1	loanDepot	Finance	16,600,000
2	Trello	IT services and software	15,115,516
3	Eye4Fraud	Finance	14,900,000
4	Raptor Technologies, LLC	IT services and software	4,024,001
5	Concentra	Health care	3,998,162

Some famous Cyber Attacks



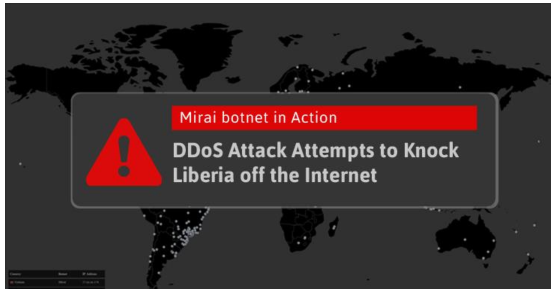
hoo.com>

YAHOO!

UPDATED NOTICE OF DATA BREACH

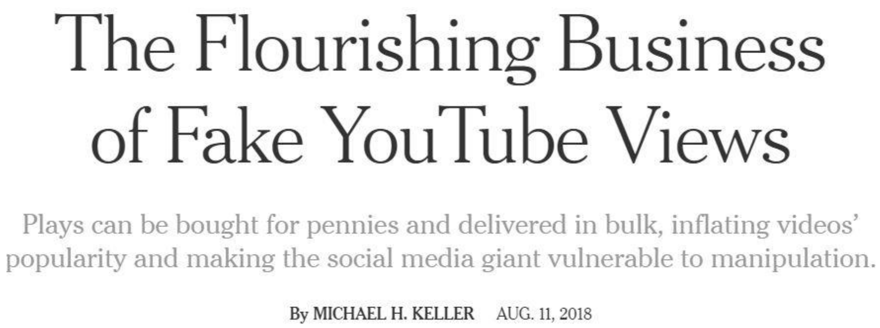
Dear Yahoo User,

We are writing to update you about a data security issue Yahoo previously announced in December 2016. Yahoo already took



Mirai botnet in Action

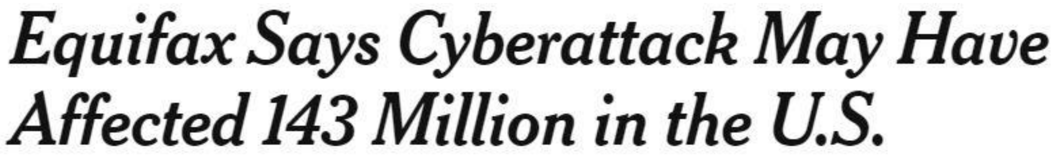
DDoS Attack Attempts to Knock Liberia off the Internet



The Flourishing Business of Fake YouTube Views

Plays can be bought for pennies and delivered in bulk, inflating videos' popularity and making the social media giant vulnerable to manipulation.

By MICHAEL H. KELLER AUG. 11, 2018

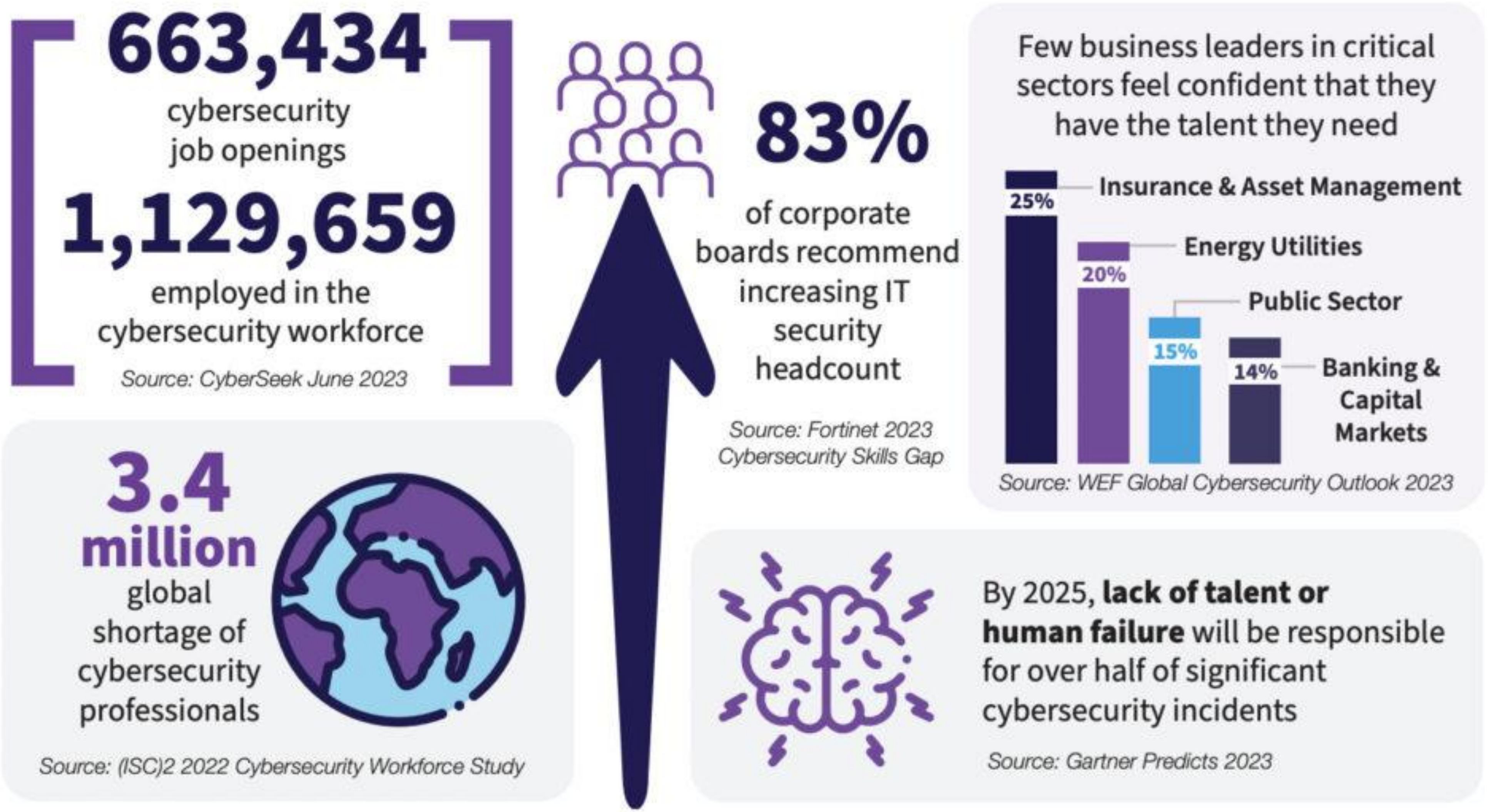


Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

Haveibeenpwned.com

Read more

Shortage of Cyber Workforce



663,434 cybersecurity job openings

1,129,659 employed in the cybersecurity workforce

Source: CyberSeek June 2023

83% of corporate boards recommend increasing IT security headcount

Source: Fortinet 2023 Cybersecurity Skills Gap

Few business leaders in critical sectors feel confident that they have the talent they need

Source: WEF Global Cybersecurity Outlook 2023

3.4 million global shortage of cybersecurity professionals

Source: (ISC)2 2022 Cybersecurity Workforce Study

By 2025, **lack of talent or human failure** will be responsible for over half of significant cybersecurity incidents

Source: Gartner Predicts 2023

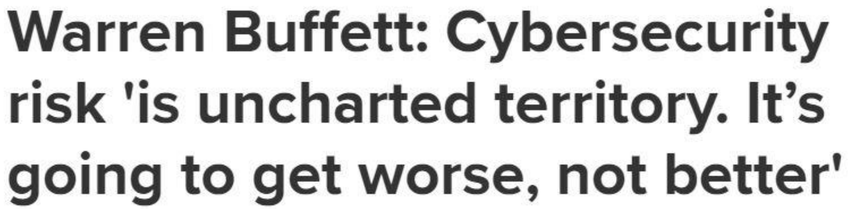
How to Assure Security: Risk Management

- We cannot secure everything!!
  - National Vulnerability Database (NVD) has 277633 vulns (01/15/2025)
  - New vulns reported in 2024 30000+
- Different vulns have different financial impacts
- We must prioritize remediation
- What is the business context?
- Information security becomes “risk management” (chapter 5)

https://nvd.nist.gov/
https://nvd.nist.gov/general/nvd-dashboard

Why is cybersecurity more important now than ever before?

1. Increased Digital Dependency
2. Sophisticated Cyber Threats
3. Explosion of Data
4. Rising cost of breaches
5. Rise of Emerging Technologies
6. Protection of Critical Infrastructure
7. Regulatory Requirements
8. Protection of Personal Privacy
9. Prevention of Identity Theft and financial security
10. National security



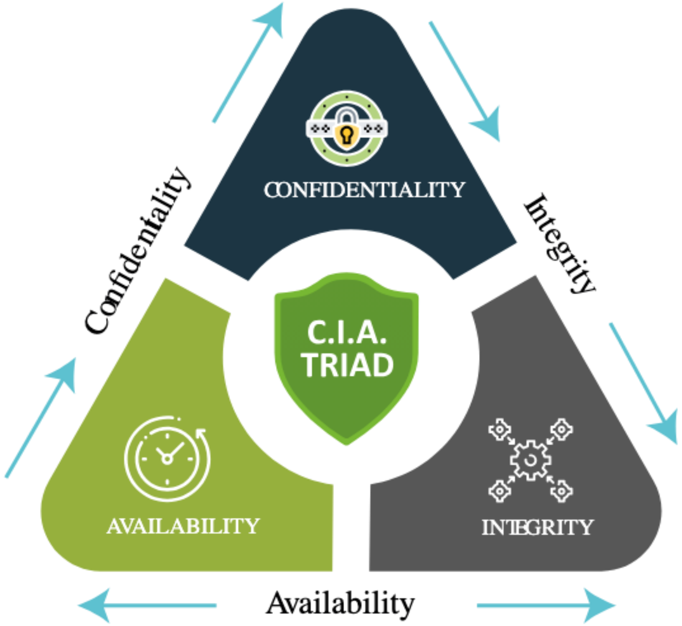
Warren Buffett: Cybersecurity risk 'is uncharted territory. It’s going to get worse, not better'

Read more

Principles of Cybersecurity

- **Information security (**InfoSec): Practice of protecting information from unauthorized access, disclosure, disruption, destruction, or modification.
- Goal of InfoSec is to preserve three information security principles: C, I , A

- CIA triad is a common model that forms the basis for the development of security systems
- Used for finding weakness and methods for creating solutions
- Plays a crucial role in keeping your data safe and secure against growing cyberthreats



Confidentiality

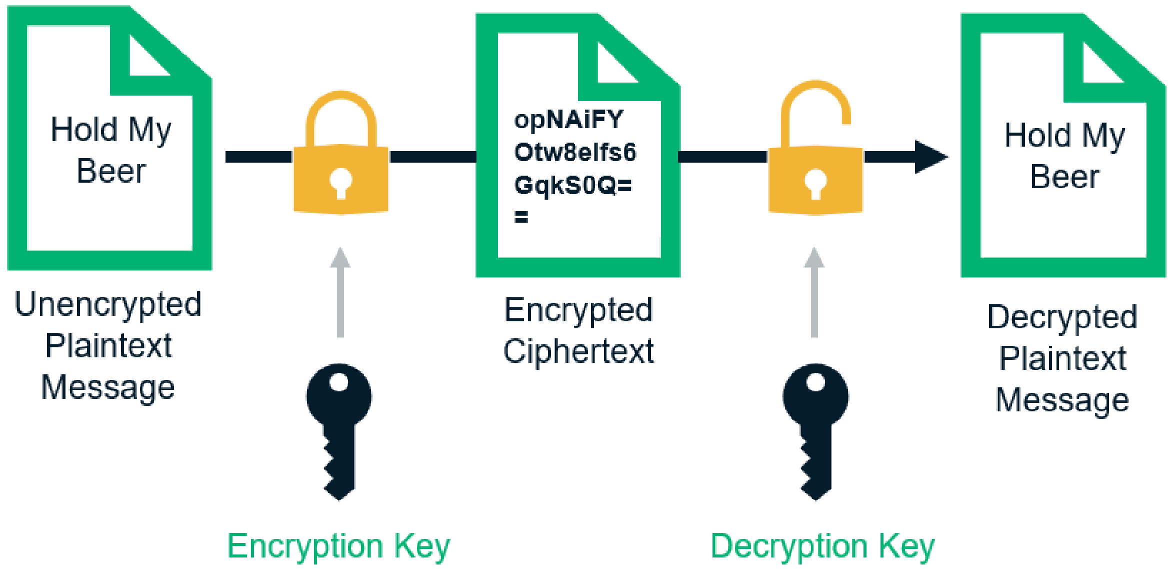
- **Confidentiality** is the process of keeping an organization or individual’s data private and ensuring only authorized people can access it

- **Threats**:
  - ➢Stealing passwords, capturing network traffic, social engineering attacks
  - ➢Unintentional breach: emailing sensitive information to wrong recipients, publishing private information on public websites

- **Controls:**
  - ➢Tight access control, proper encryption, strong passwords, authentication systems

Example: Data confidentiality

- Confidentiality means data should only be disclosed to authorized users
- Helps maintain trust between organizations and their users by ensuring data security
- Example: Encryption can be used to preserve data confidentiality


Hold My Beer
Unencrypted Plaintext Message
opNAiFY Otw8elfs6 GqkS0Q= =
Encrypted Ciphertext
Hold My Beer
Decrypted Plaintext Message
Encryption Key
Decryption Key

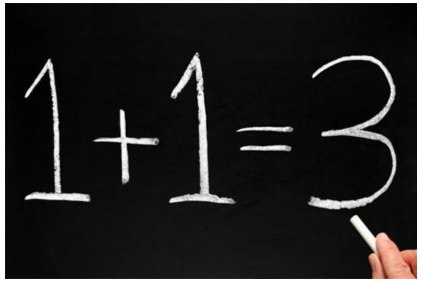
Integrity

- Principle that data has not been changed, destroyed, or lost in an unauthorized or accidental manner
  - ➢ ensure the correctness and completeness of data

- **Threats**: Malicious alterations, insider threats, human error, malware

- **Data at rest** (data stored on systems), **data in transit** (data transmitted between systems), and **data in use** (data in processing) should be protected to maintain data integrity

- Controls:
  - ➢Access Control, checksums, hash verifications, encryption
  - ➢User training, audit trails



Availability

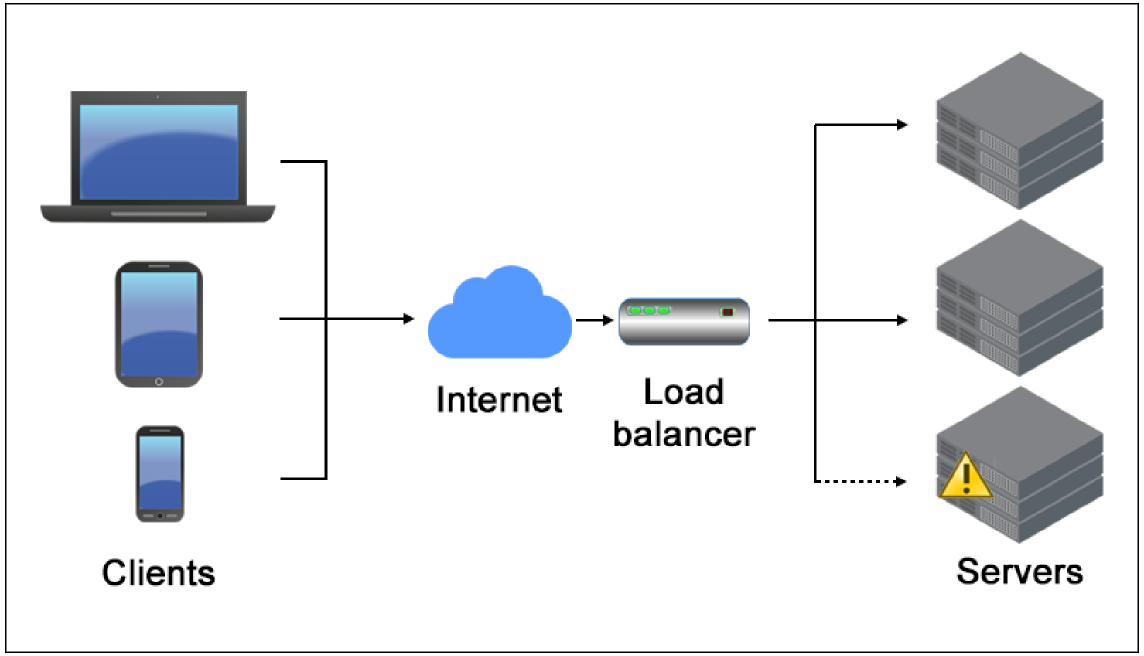
- **Availability** is the security principle that ensures information is accessible by authorized users whenever required
- Aim is to ensure reliable access to the data or systems without significant delay

- **Threats**:
  - ➢Hardware failures, natural disasters, software issues, DoS, DDos

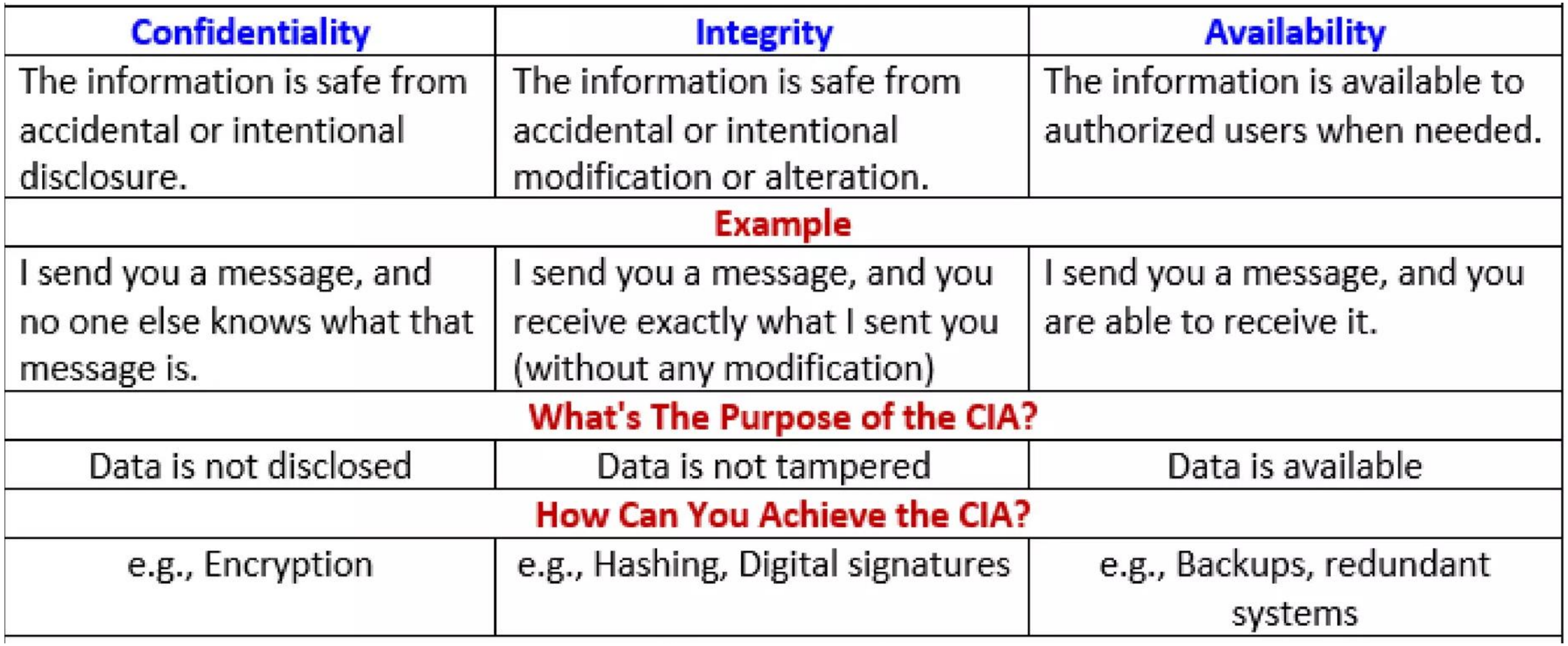
- **Controls:**
  - ➢Redundancy, backups, firewall, regular monitoring
  - ➢ regular maintenance, failover mechanisms

Example: Load balancer for preserving data availability

- Improves data availability by distributing web traffic across multiple identical web servers
- If a web server fails, the load balancer directs the traffic to the other web server to preserve data availability



Summary: The CIA Triad



Confidentiality	Integrity	Availability
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems

Each element addresses a critical aspect of protecting information and systems from cyber threats, and together, they ensure comprehensive security coverage

Violating the CIA Triad: If You Were An Attacker, What Are Your Goals/Motivation?

- Steal sensitive information, such as personal data, financial records, or trade secrets, for financial gain or to sell on the dark web

- **Blackmail:** Attackers may gather compromising information to extort individuals or organizations

- **Identity Theft:** Stolen personal data can be used to commit identity theft and various forms of fraud

- **Ransomware:** Encrypting a victim's data and demanding payment for decryption can disrupt operations and extort money

- **Competitive Advantage:** Sabotaging a competitor's online presence can provide an advantage in the marketplace

More Potential Goals/Motivations

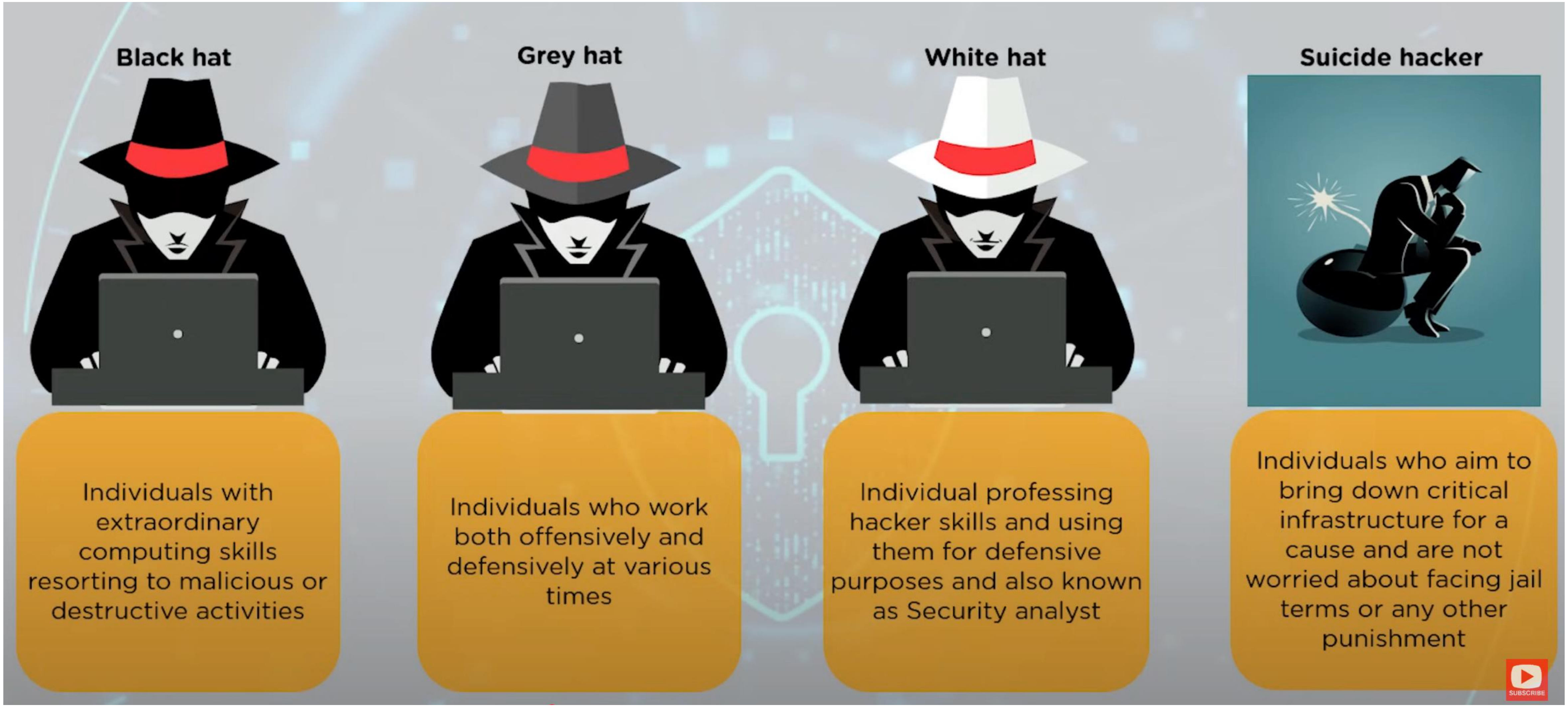
- **Vandalism:** Disrupting services or defacing websites to cause harm or embarrassment to the target
- **Information Warfare:** Manipulating information to spread misinformation or propaganda for political, ideological, or disruptive purposes
- **Data Manipulation:** Attackers may alter data to cause confusion, discredit individuals or organizations, or manipulate financial systems for personal gain
- **Fun:** Some do it for fun
- **Downtime and Disruption:** Attackers might launch DDoS attacks to overload servers, rendering websites and services unavailable to legitimate users

Vocabulary

Why is vocabulary important?

- There is a problem with vocabulary in this field. People use these words for different meanings

- **Event** - Could be anything
- **Incident** - A malicious event, potential to cause harm
- **Bug** - An error that exists in the implementation level (i.e. only exists in source code); very correctable
- **Flaw** – An error at a much deeper level, particularly in the design and likely at the code level, can be very difficult and costly to correct
- **Hacker** - A creative programmer; a positive connotation
- **Cracker** - The bad guy, the attacker, what media coins "hacker" (the negative connotation)



Black hat

Individuals with extraordinary computing skills resorting to malicious or destructive activities

Grey hat

Individuals who work both offensively and defensively at various times

White hat

Individual professing hacker skills and using them for defensive purposes and also known as Security analyst

Suicide hacker

Individuals who aim to bring down critical infrastructure for a cause and are not worried about facing jail terms or any other punishment

Black hat - An attacker with harmful intents
White hat (ethical hacker) - An attacker with good intents (i.e., the white knight)
Gray hat - An attacker with good and bad intents

Image Source: Simplilearn

Vocabulary

- **Script kiddie** - An unskilled person who uses pre-existing scripts and tools to exploit a system's vulnerabilities
- **Exploiting** - Act of taking advantage of a weakness in the system
- **Exploit** - Software program that performs the exploiting
- **Risk** - Likelihood that an attacker will take advantage of that vulnerability

Reading: 100 cybersecurity terms

Vulnerability, threat, threat actor

- **Vulnerability** - A security bug; a weakness in a system that can potentially be exploited by an attacker

- **Threat**: A threat is any event that can potentially impact a system negatively through unauthorized access, destruction, disclosure, modification of data, and/or denial of service
  - ➢Accidental - Software or operator error
  - ➢Intentional - Virus, ransomware, phishing, Dos
  - ➢Natural - Earthquake, hurricane, flood

- **Threat actor**: A threat actor is a person or group who exploits a vulnerability
  - Black hat, white hat, grey hat, script kiddie

Other Threat Actors

- **Advanced persistent threat (APT):** threat actor who gains unauthorized access to a high-value target for an extended period of time
  - ➢ Typically sponsored by a nation, state sponsored group, or other advanced cybercriminal organizations with the aim of stealing government, military or corporate secrets of another nation

➢ **Advanced Techniques:** employ advanced and evolving techniques, including zero-day exploits, custom malware, and sophisticated social engineering, to breach their targets

➢ **Long-Term Focus:** APT attacks are not opportunistic but rather strategic and patient

➢ **Targeted:** attackers carefully select their targets, often based on geopolitical, economic, or industrial motivations

➢ **Persistence:** APT groups maintain access to the compromised systems for as long as necessary to achieve their goal

➢ **Custom Malware:** develop custom malware specifically tailored for their targets

Other Threat Actors

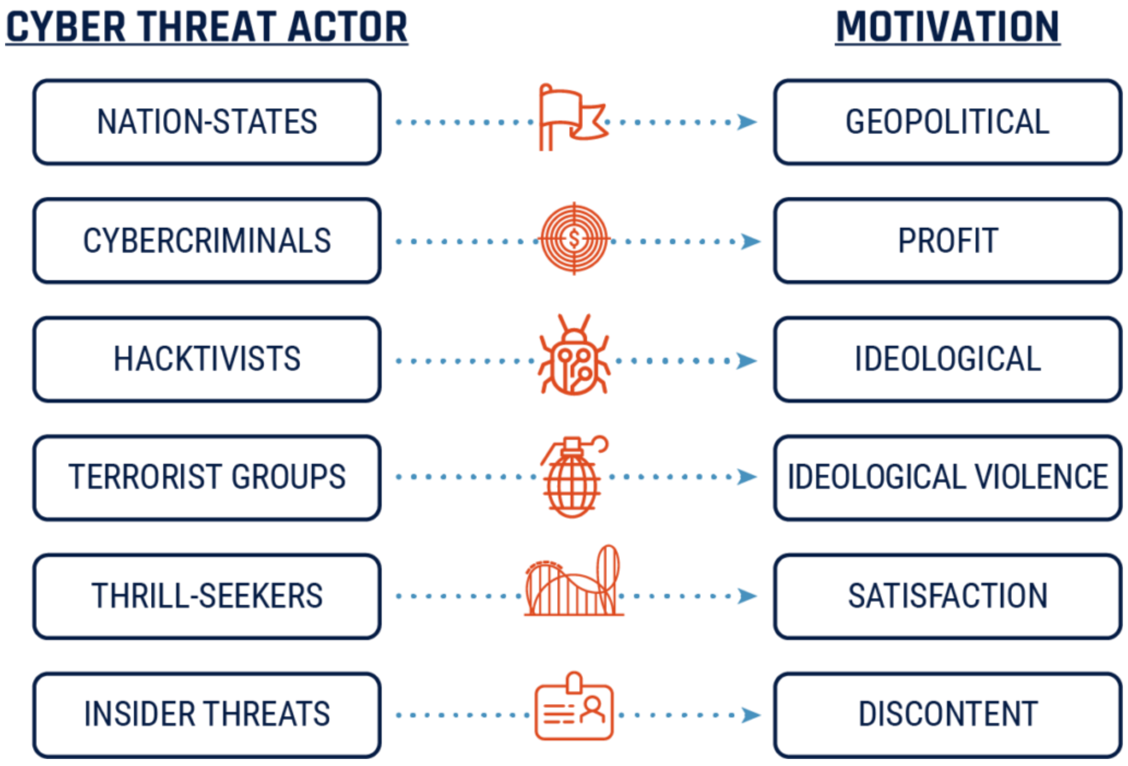
- **Hacktivist**: Uses computer-based techniques to promote the activist's agenda

- **Organized Crime Syndicates:**: Criminal organizations that engage in cybercrimes, such as ransomware attacks, credit card fraud, or identity theft, for financial gain

- **Terrorist Organizations:** Some terrorist groups use cyberattacks as a means to disrupt critical infrastructure or promote their agenda.

Other Threat Actors and Motivation

- **Competitor**: Rival organization whose activities have the potential to reduce another organization's share of the market
- **Insiders:** Largest information security threats to a business actually comes from an unlikely source: its employees, contractors and business partners
- **Shadow IT and Unintentional Threats:** Employees or entities unknowingly introducing vulnerabilities through unauthorized tools or poor security practices.



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

Image Source: https://cyberhoot.com/cybrary/threat-actor/

Attack vector / threat vector

- Attack vector/ threat vector, is a path or means by which an attack is realized
- Common attack vectors include:
    - ➢**Direct access**: Accessing a computer or network directly through a physical connection
    - ➢**Wireless**: Intercepting and modifying wireless data
    - ➢**Email**: Attaching malware to an Email or including a link to a malicious website
    - ➢**Supply chain**: Modifying a hardware or software product as the product moves through the supply chain
    - ➢**Social media**: Delivering customized attacks against a target based on the target's social media posts
    - ➢**Removable media**: Delivering malware using removable media such as USB flash drives

Attack vector / threat vector

- Threat actor can attach a malware to an Email and sent it to the user

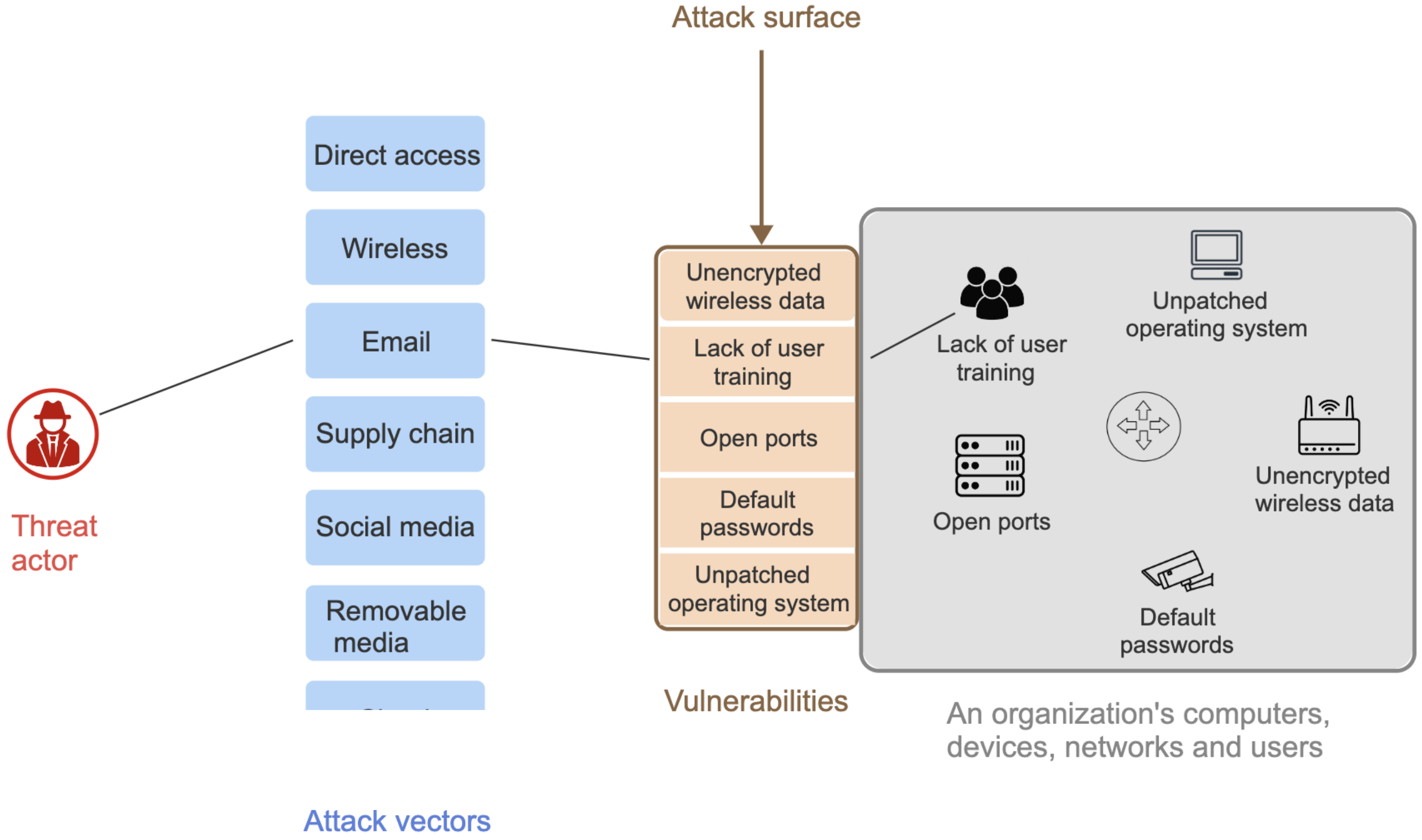
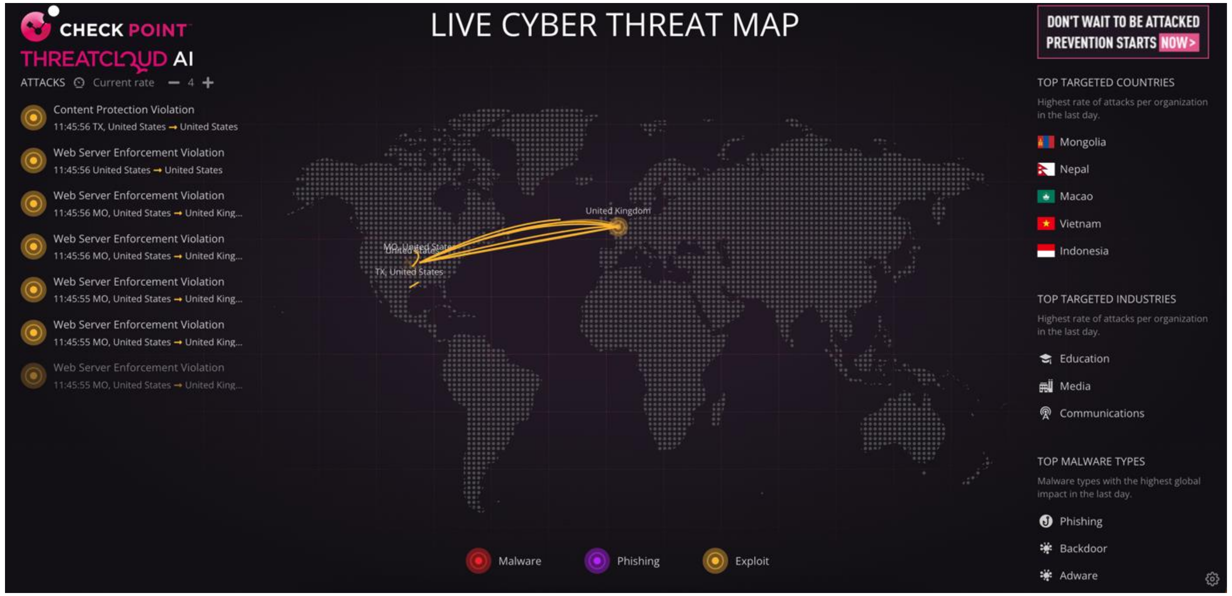


Image Source: ZyBooks

Threat map

- A threat map shows active attacks across the world. Debate surrounds the usefulness of threat maps for understanding cyberattacks. However, most threat maps include additional useful information.
- *Check Live Threat Map:*
- https://threatmap.checkpoint.com/
- [*https://www.digitalattackmap.com/*](https://www.digitalattackmap.com/)
- [*https://cybermap.kaspersky.com/*](https://cybermap.kaspersky.com/)



CHECK POINT
THREATCLOUD AI

LIVE CYBER THREAT MAP

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>

ATTACKS Current rate − 4 +

Content Protection Violation
11:45:56 TX, United States → United States

Web Server Enforcement Violation
11:45:56 United States → United States

Web Server Enforcement Violation
11:45:56 MO, United States → United King...

Web Server Enforcement Violation
11:45:56 MO, United States → United King...

Web Server Enforcement Violation
11:45:55 MO, United States → United King...

Web Server Enforcement Violation
11:45:55 MO, United States → United King...

Web Server Enforcement Violation
11:45:55 MO, United States → United King...

TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Macao
- Vietnam
- Indonesia

TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.

- Education
- Media
- Communications

TOP MALWARE TYPES
Malware types with the highest global impact in the last day.

- Phishing
- Backdoor
- Adware

5W1H framework (Who, What, When, Where, Why, and How)

1. What

•What is cybersecurity?

- The practice of protecting systems, networks, programs, and data from digital attacks, unauthorized access, and damage.
- Involves tools, processes, and practices to defend against threats such as malware, ransomware, phishing, and social engineering.

2. Who

•Who is involved in cybersecurity?

- **Users:** Individuals, businesses, and organizations using technology.
- **Cybersecurity professionals:** Analysts, engineers, and IT teams responsible for securing systems.
- **Threat actors:** Hackers, cybercriminals, and nation-states attempting to breach systems.
- **Regulatory bodies:** Organizations setting compliance and security standards, such as GDPR or HIPAA.

3. When

- **When is cybersecurity needed?**
  - Always. As long as digital systems, data, and networks exist, they require continuous protection.
  - **Specific scenarios:**
    - During software development (DevSecOps).
    - When deploying new systems or updates.
    - After a data breach or incident to mitigate damage.

4. Where

- **Where is cybersecurity applied?**
  - Across all sectors and environments:
    - **Personal devices**: Smartphones, computers, IoT devices.
    - **Business systems**: Servers, databases, cloud platforms.
    - **Critical infrastructure**: Power grids, water systems, transportation networks.
    - **Online platforms**: Websites, social media, and e-commerce platforms.

5. Why

- **Why is cybersecurity important?**
  - **Protect sensitive information**: Personal, financial, and organizational data.
  - **Prevent financial loss**: From fraud, theft, and operational disruptions.
  - **Ensure continuity**: Keep businesses and services running without interruptions.
  - **Maintain trust**: Secure systems foster customer confidence.
  - **Compliance**: Meet legal and regulatory requirements.

6. How

- **How is cybersecurity implemented?**
  - **Technical measures**: Firewalls, encryption, intrusion detection systems, and endpoint protection.
  - **Policies and procedures**: Incident response plans, access control policies, and regular audits.
  - **Training and awareness**: Educating employees and users about best practices and threats.
  - **Monitoring and response**: Using tools like Security Information and Event Management (SIEM) systems.
  - **Development practices**: Integrating security into development of software and services

Reading

- Why Cybersecurity Is Important Now More Than Ever

https://www.edoxi.com/studyhub-detail/why-cybersecurity-is-important-now

- Why is software security a bigger problem now than in the past?

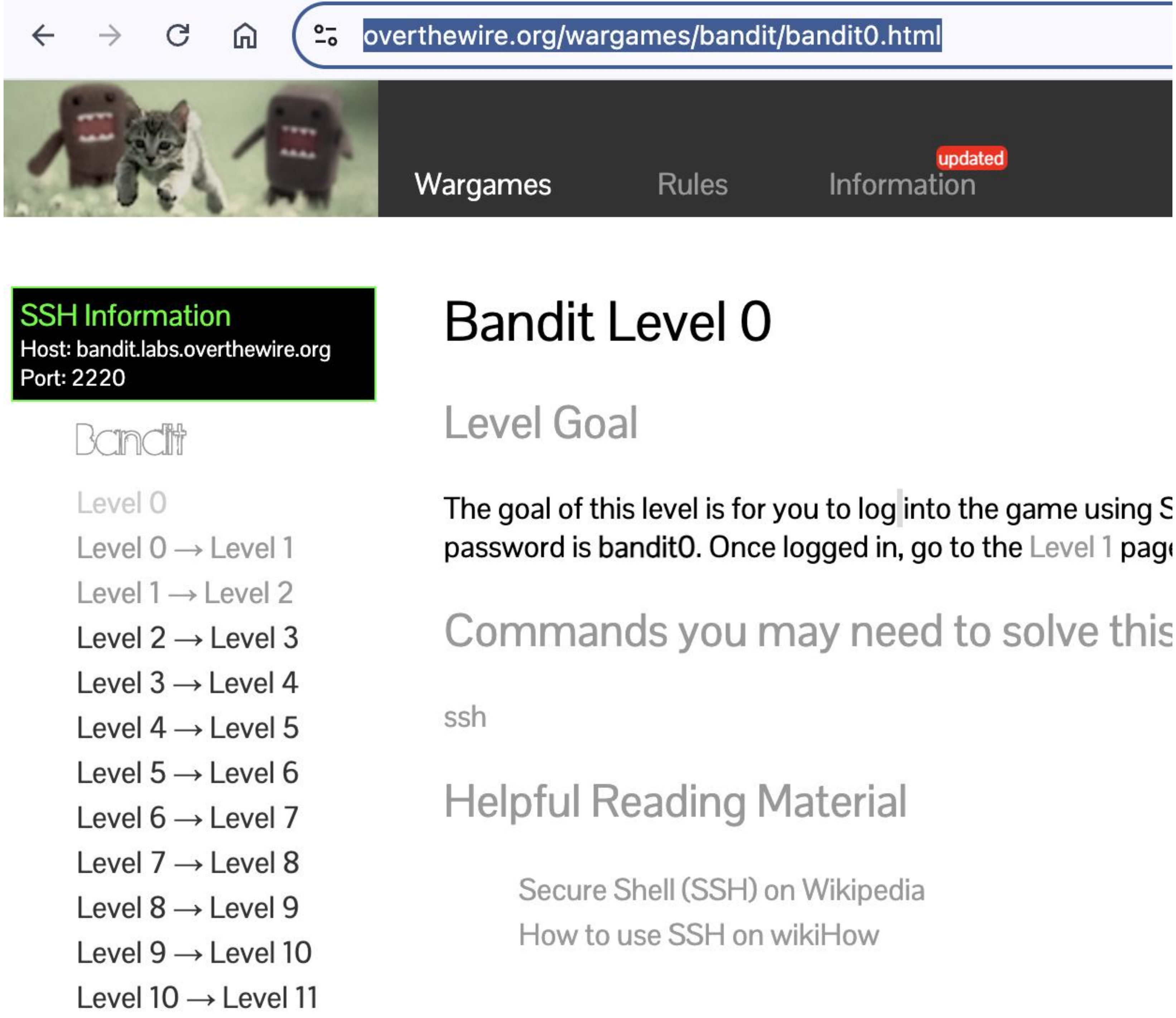
https://freedom-to-tinker.com/2006/02/15/software-security-trinity-trouble/

- National Vulnerability Database https://nvd.nist.gov/

- Security+ Study Guide, Chapple and Seidl, Exam SY0-701, Chapter 1 and 2

Summary

- Security Introduction
- CIA Triad
- Cybersecurity Vocabulary
- Vulnerability
- Threat and Threat actors
- Threat Maps



SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit Level 0

Level Goal

The goal of this level is for you to log into the game using S
password is bandit0. Once logged in, go to the Level 1 pag

Commands you may need to solve this

ssh

Helpful Reading Material

- Secure Shell (SSH) on Wikipedia
- How to use SSH on wikiHow