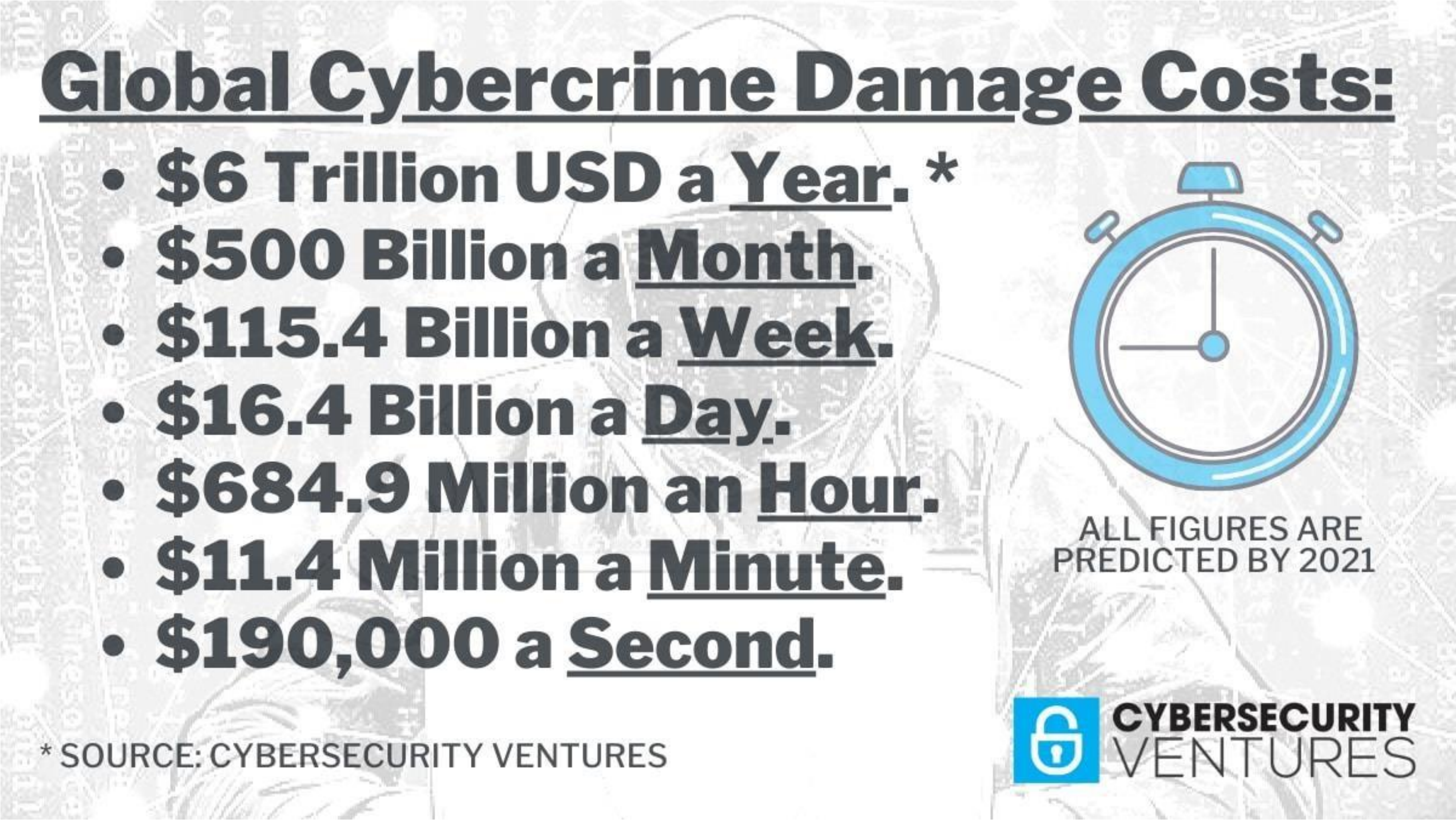
Cyber Security

Subject Code:-102045607

Unit-1 Introduction

Largest economy in world

- USA
- China



Global Cybercrime Damage Costs:

- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

ALL FIGURES ARE
PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY
VENTURES

Importance of Cyber Security

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium safe, buried in a solid bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

- ***Professor Gene Spafford***

In security matters:

- There is nothing like absolute security
- We are only trying to build comfort levels, because security costs money and lack of it costs much more
- Comfort level is a manifestation of efforts as well as a realization of their effectiveness & limitations

Importance of Cyber Security

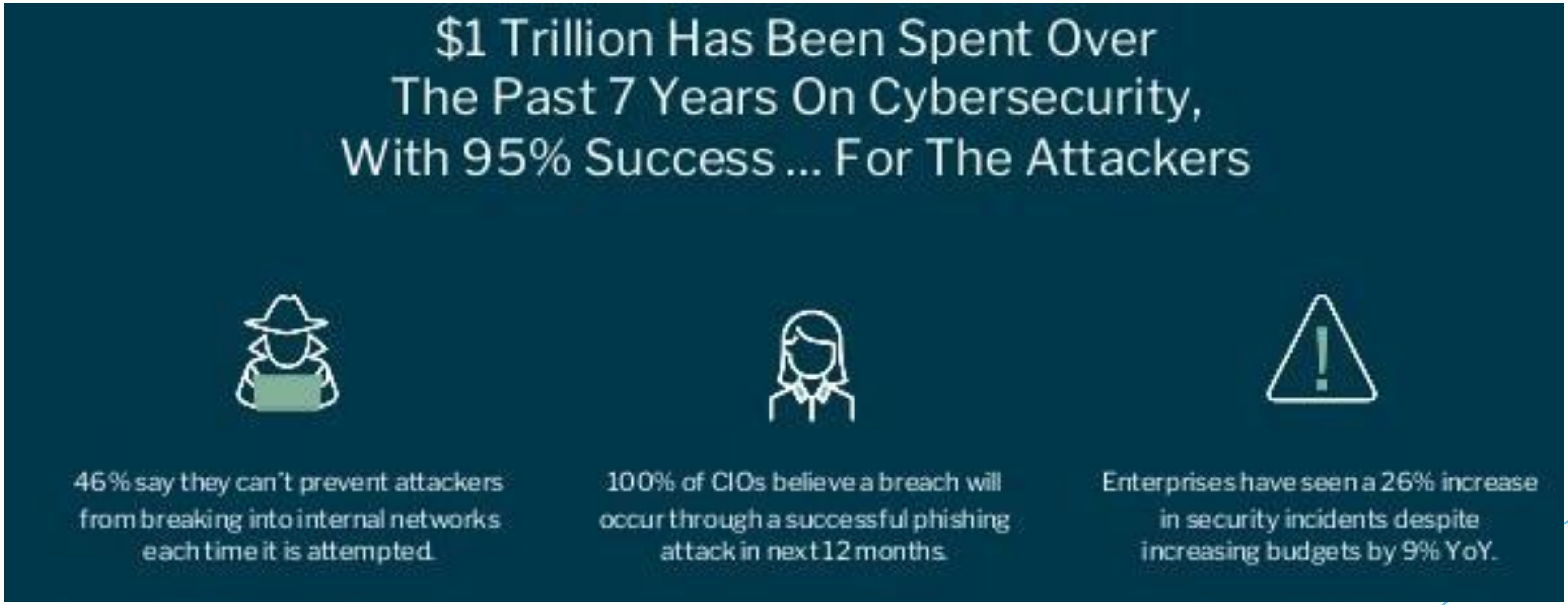
- The Internet allows an attacker to work from anywhere on the planet.

- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Consequences (for yourself and your organization)
  - Sanctions or termination if policies are not followed

- According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
  - Web Browser
  - IM Clients
  - Web Applications
  - Excessive User Rights

Cyber Security

- Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.



$1 Trillion Has Been Spent Over The Past 7 Years On Cybersecurity, With 95% Success ... For The Attackers

46% say they can't prevent attackers from breaking into internal networks each time it is attempted.

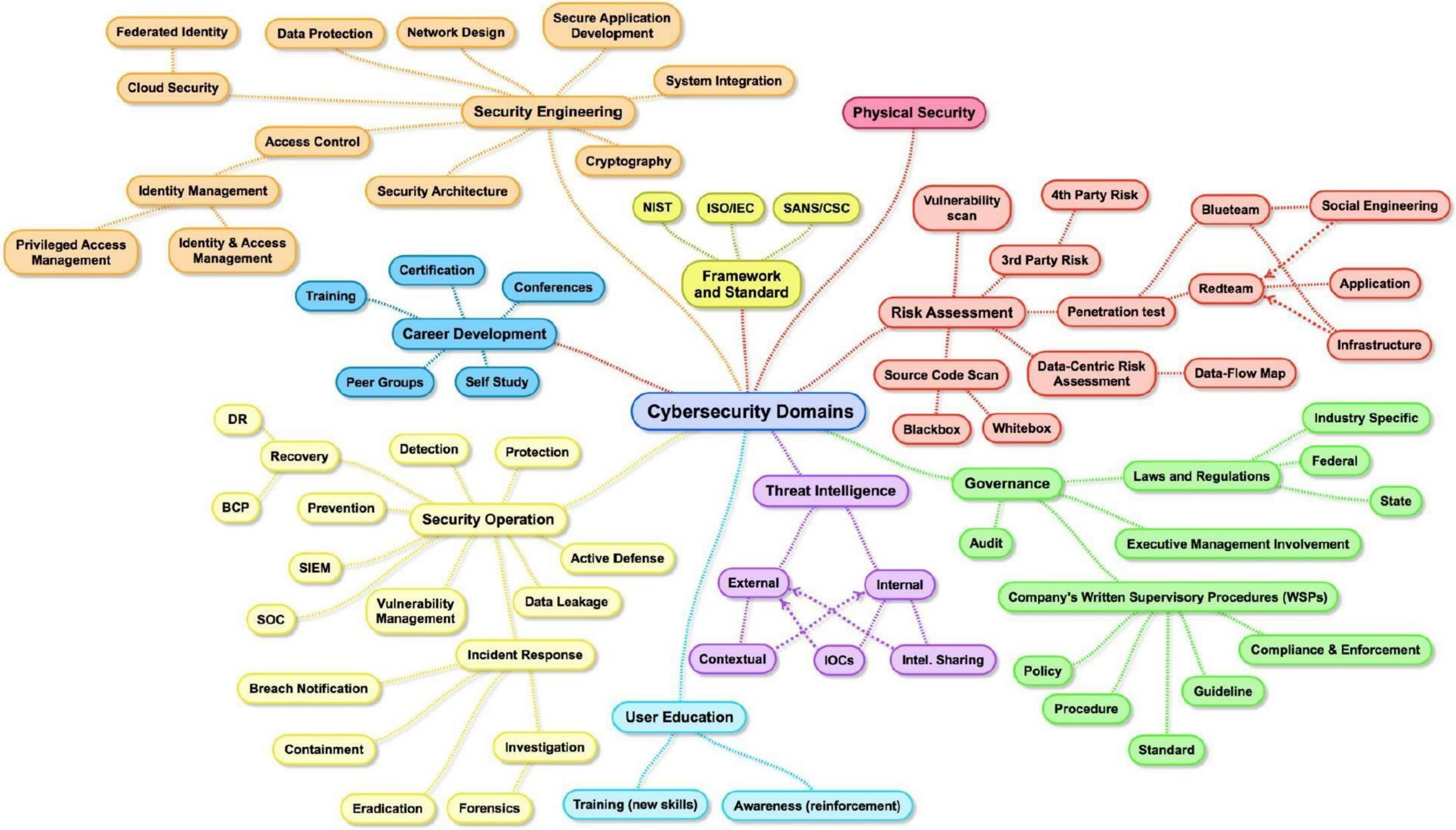
100% of CIOs believe a breach will occur through a successful phishing attack in next 12 months.

Enterprises have seen a 26% increase in security incidents despite increasing budgets by 9% YoY.

Cyber Security is Safety

- Security: We must protect our computers and data in the same way that we secure the doors to our homes.
- Safety: We must behave in ways that protect us against risks and threats that come with technology.

Cyber Security Domains



Cybersecurity Domains

- Security Engineering
  - Federated Identity
  - Cloud Security
  - Data Protection
  - Network Design
  - Secure Application Development
  - System Integration
  - Cryptography
  - Security Architecture
  - Access Control
    - Identity Management
      - Privileged Access Management
      - Identity & Access Management
- Physical Security
- Framework and Standard
  - NIST
  - ISO/IEC
  - SANS/CSC
- Career Development
  - Training
  - Certification
  - Conferences
  - Peer Groups
  - Self Study
- Risk Assessment
  - Vulnerability scan
  - 3rd Party Risk
    - 4th Party Risk
  - Penetration test
    - Blueteam
      - Social Engineering
    - Redteam
      - Application
      - Infrastructure
  - Source Code Scan
    - Blackbox
    - Whitebox
  - Data-Centric Risk Assessment
    - Data-Flow Map
- Governance
  - Laws and Regulations
    - Industry Specific
    - Federal
    - State
  - Audit
  - Executive Management Involvement
  - Company's Written Supervisory Procedures (WSPs)
    - Policy
    - Procedure
    - Standard
    - Guideline
    - Compliance & Enforcement
- Threat Intelligence
  - External
  - Internal
  - Contextual
  - IOCs
  - Intel. Sharing
- User Education
  - Training (new skills)
  - Awareness (reinforcement)
- Security Operation
  - Detection
  - Protection
  - Prevention
  - Recovery
    - DR
    - BCP
  - Active Defense
  - SIEM
  - SOC
  - Vulnerability Management
  - Data Leakage
  - Incident Response
    - Breach Notification
    - Containment
    - Eradication
    - Forensics
    - Investigation

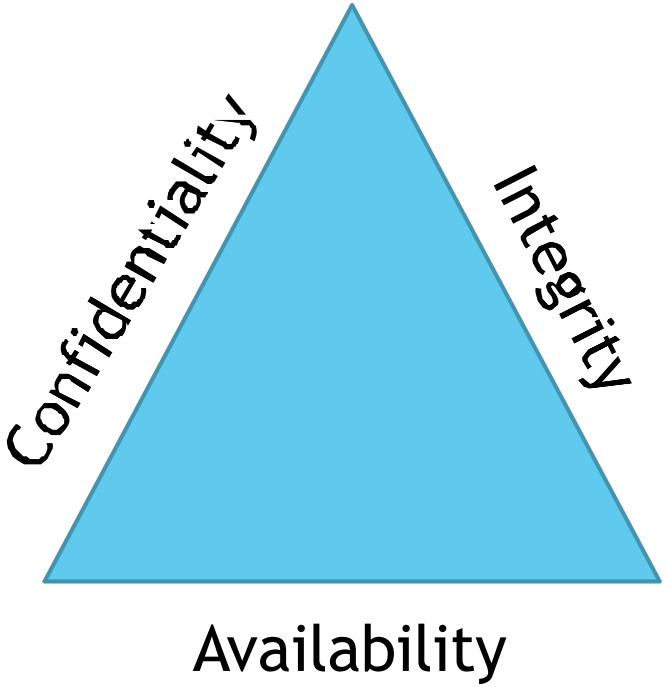
Cyber Security Types

- **Network Security**
- **Application Security**
- **Information or Data Security**
- **Identity management**
- **Operational Security**
- **Mobile Security**
- **Cloud Security**
- **Disaster Recovery and Business Continuity Planning**
- **User Education**

False Sense of Security?

JEWELRY
EVEN THE BEST SECURITY SYSTEM
Only functions when it is activated
motifake.com

What is a Secure System? (CIA Triad)



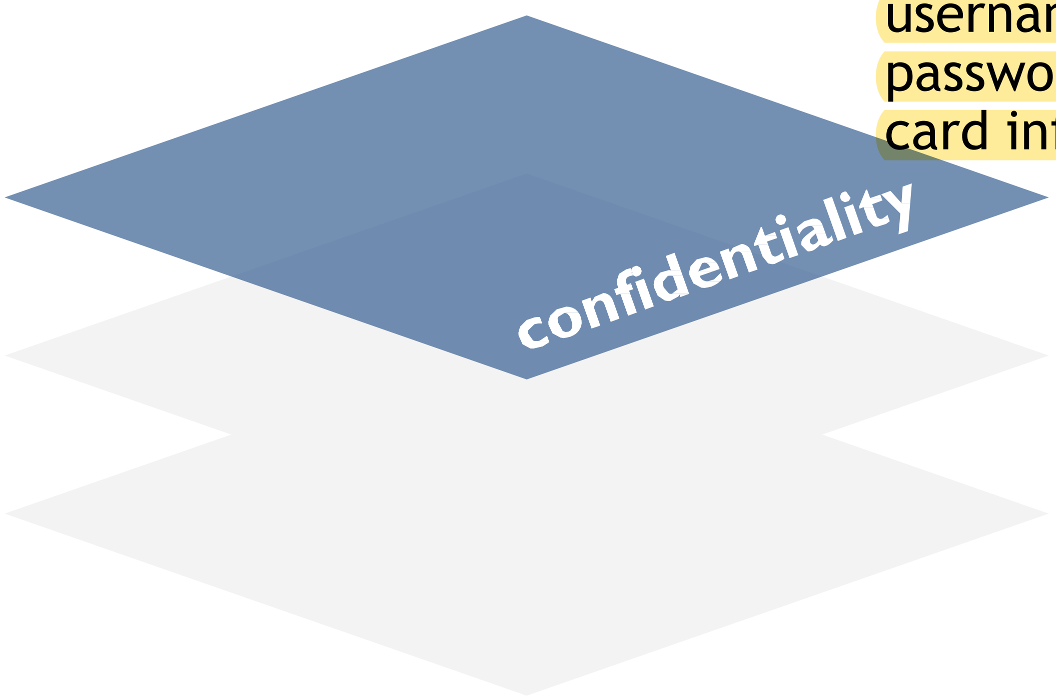
- ***Confidentiality*** – restrict access to unauthorized individuals
- ***Integrity*** – data has not been altered in an unauthorized manner
- ***Availability*** – information can be accessed and modified by authorized individuals in an appropriate timeframe

CIA Triad

Confidentiality

Example:

Criminal steals customers’ usernames, passwords, or credit card information

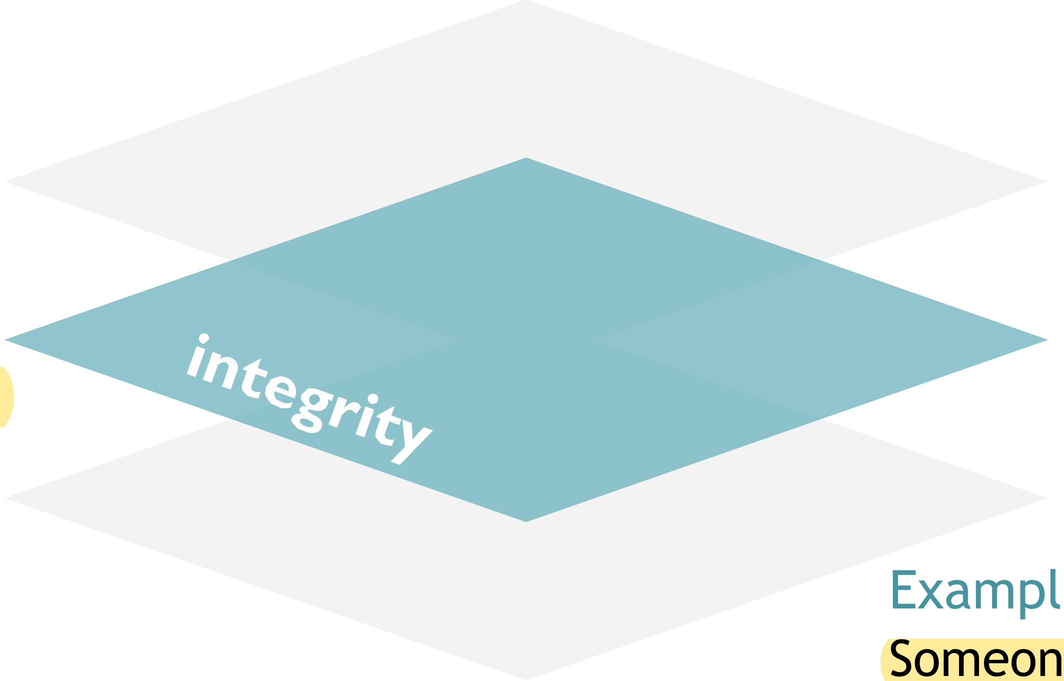


Protecting information from unauthorized access and disclosure

CIA Triad

Integrity

Protecting information from unauthorized modification



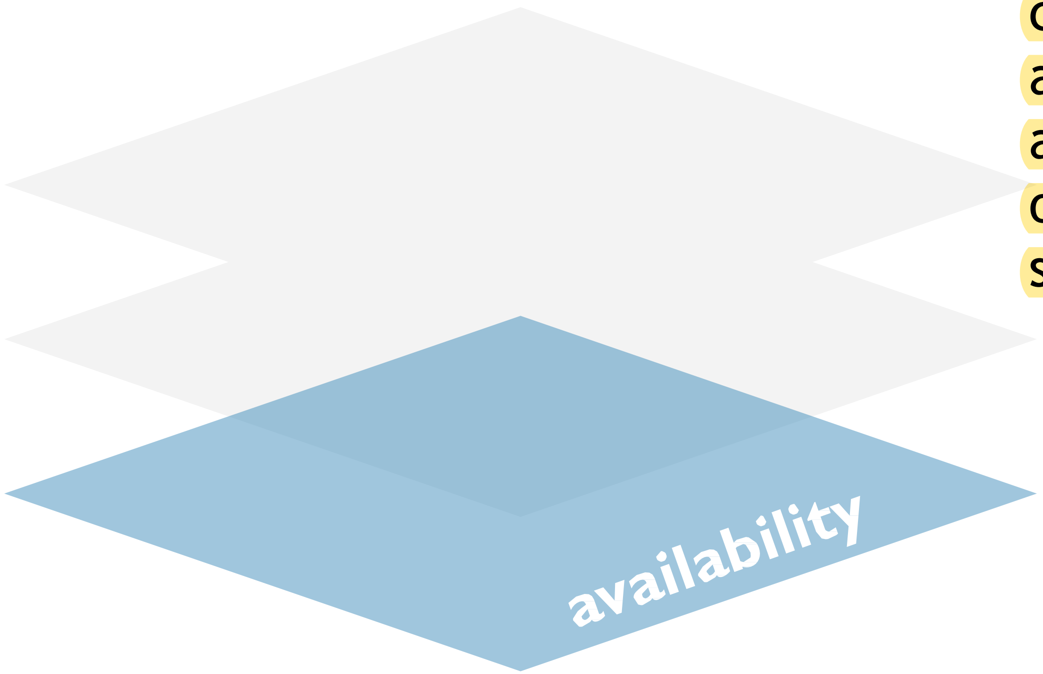
Example:

Someone alters payroll information or a proposed product design

CIA Triad

Availability

Preventing disruption in how information is accessed



Example:

Your customers are unable to access your online services

CIA Triad

- **Confidentiality** is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts.
- It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands.

CIA Triad

- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.
- Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

CIA Triad

- **Availability** means information should be consistently and readily accessible for authorized parties.
- This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

CIA Triad

Putting Confidentiality into Practice:

- Data encryption is one way to ensure confidentiality and that unauthorized users cannot retrieve data for which they do not have access.
- Access control is also an integral part of maintaining confidentiality by managing which users have permissions for accessing data.

CIA Triad

Putting Integrity into Practice:

- Event log management within a Security Incident and Event Management system is crucial for practicing data integrity.
- Implementing version control and audit trails into your IT program will allow your organization to guarantee that its data is accurate and authentic.

CIA Triad

Putting Availability into Practice:

- Employing a backup system and a disaster recovery plan is essential for maintaining data availability should a disaster, cyber-attack, or another threat disrupt operations.
- Utilizing cloud solutions for data storage is one way in which an organization can increase the availability of data for its users.
- As the reliance on data analytics expands, the need for data to be available and accessible grows for sectors like financial services and life sciences.

Challenges in Cyber Security

#1. Increase in Cyberattacks

#2. Supply Chain Attacks Are on the Rise

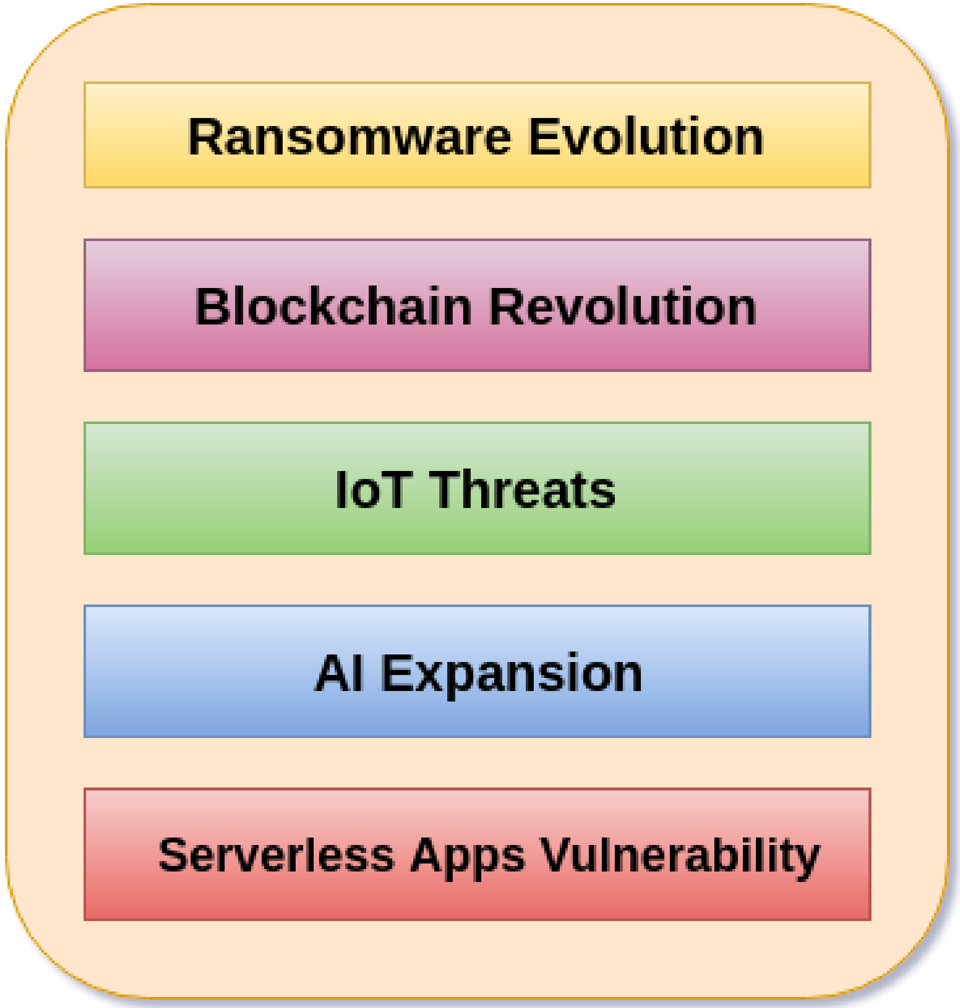
#3. The Cyber Pandemic Continues

#4. Cloud Services Are A Primary Target

#5. Ransomware Attacks Are on the Rise

#6. Mobile Devices Introduce New Security Risks

……………..



Ransomware Evolution

Blockchain Revolution

IoT Threats

AI Expansion

Serverless Apps Vulnerability

Cyber Security Challenges

Cyberspace

Definition:-A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

- Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.
- Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

Threats and Vulnerabilities

- What are we protecting our and our stakeholders information from?
- **Threats:** Any circumstances or events that can potentially harm an information system by destroying it, disclosing the information stored on the system, adversely modifying data, or making the system unavailable
- **Vulnerabilities:** Weakness in an information system or its components that could be exploited.

Cyber Threats

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber threats can originate from various factors, including corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers.

Types of Cyber Security Threats

1. Malware

Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software.

2. Denial of Service

A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS.

Types of Cyber Security Threats

3. Man in the Middle

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

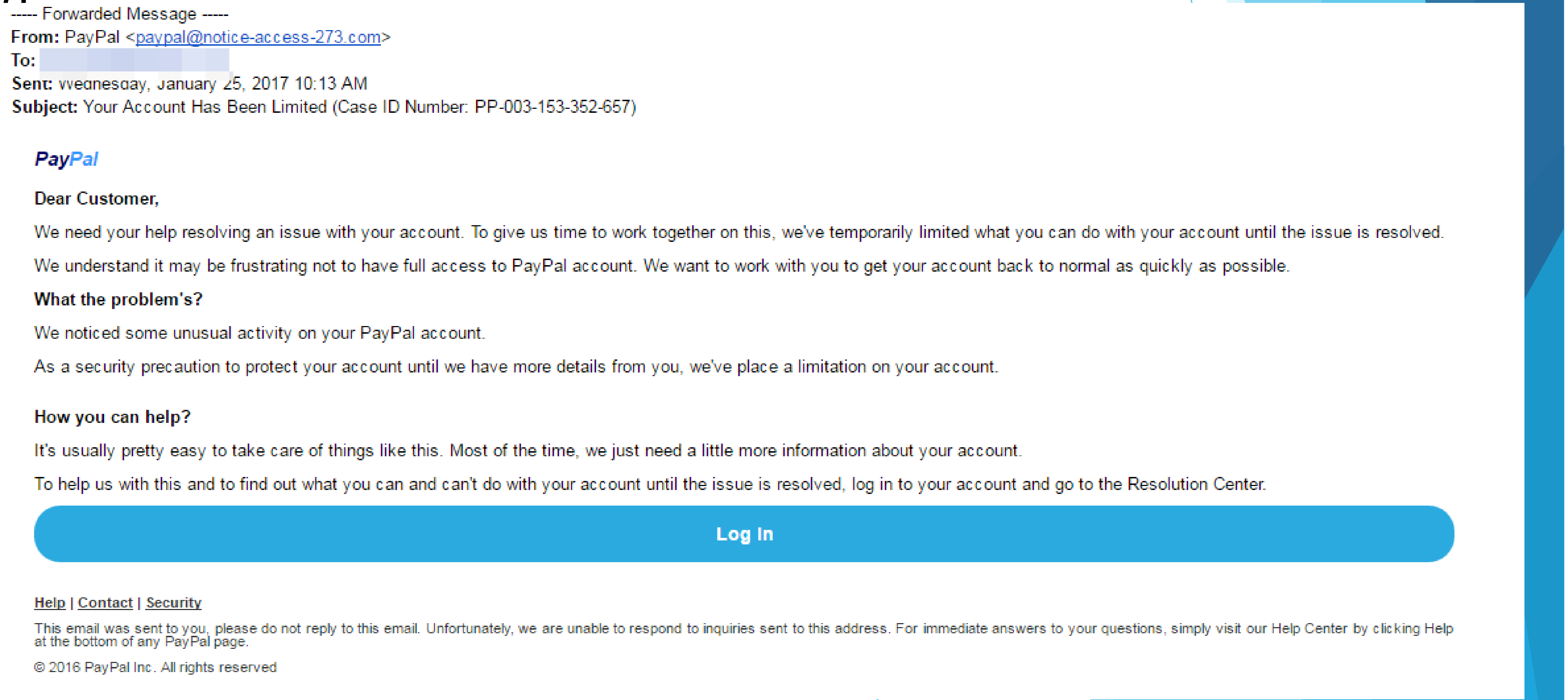
Types of Cyber Security Threats

4. Phishing

Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. “The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine,” Cisco reports.

Types of Cyber Security Threats

4. Phishing



----- Forwarded Message -----

From: PayPal <paypal@notice-access-273.com>

To: [redacted]

Sent: Wednesday, January 25, 2017 10:13 AM

Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

Types of Cyber Security Threats

5. SQL Injection

A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

Types of Cyber Security Threats

6. Password Attacks

With the right password, a cyber attacker has access to a wealth of information. Social engineering is a type of password attack that Data Insider defines as "a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices." Other types of password attacks include accessing a password database or outright guessing.

Types of Cyber Security Threats

7. Emotet

The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware."

Cyber Warfare

Cyber Warfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks.

What Does Cyber Warfare Look Like?

Cyber warfare can take many forms, but all of them involve either the destabilization or destruction of critical systems. The objective is to weaken the target country by compromising its core systems.

This means cyber warfare may take several different shapes:

- Attacks on financial infrastructure
- Attacks on public infrastructure like dams or electrical systems
- Attacks on safety infrastructure like traffic signals or early warning systems
- Attacks against military resources or organizations

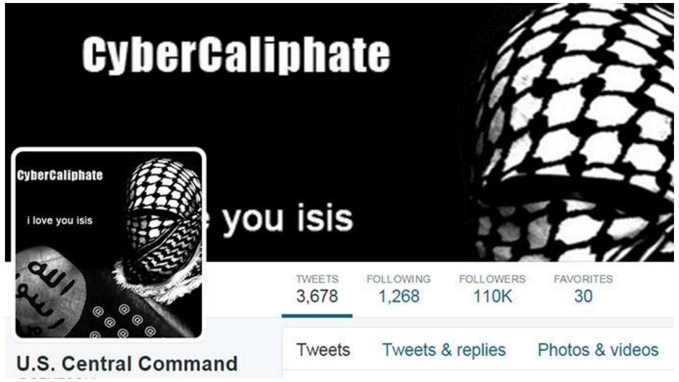
Cyber Terrorism

Cyber - Anything that involved computer resources and information.

Terrorism - An act of violence.

Cyber Terrorism

History Of Attacks



CyberCaliphate

e you isis

CyberCaliphate

i love you isis

TWEETS	FOLLOWING	FOLLOWERS	FAVORITES
3,678	1,268	110K	30

Tweets Tweets & replies Photos & videos

U.S. Central Command

BREAKING NEWS

BRUSSELS AIRPORT ROCKED BY EXPLOSIONS

Subway station also attacked, system shut down

Cyber Terrorism

Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents. - by TechTarget

The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives. - Wikipedia

Motivations of Cyber-Terrorists

There are various reasons why cyber attacks are an attractive choice for terrorists.

Few of them are:

- *No need to cross physical barrier.*
- *Identity is kept a secret.*
- *Easy to attack.*
- *Fast flow of information.*
- *Little or no regulation.*
- *Huge audience.*

Cyber Security of Critical Infrastructure

- Chemical Sector.
- Commercial Facilities Sector.
- Communications Sector.
- Critical Manufacturing Sector.
- Dams Sector.
- Defence Industrial Base Sector.
- Emergency Services Sector.
- Energy Sector.

The Cybersecurity Implications of Infrastructure Modernization

The adoption of new technologies in oil and gas facilities is a dual-edged sword. On one side, there are the obvious benefits of implementing industrial internet of things (IIoT) devices to improve efficiencies and reduce operational costs. On the other side, there are inherent risks associated with upgrading systems and with the cybersecurity infrastructure.

Thank you!