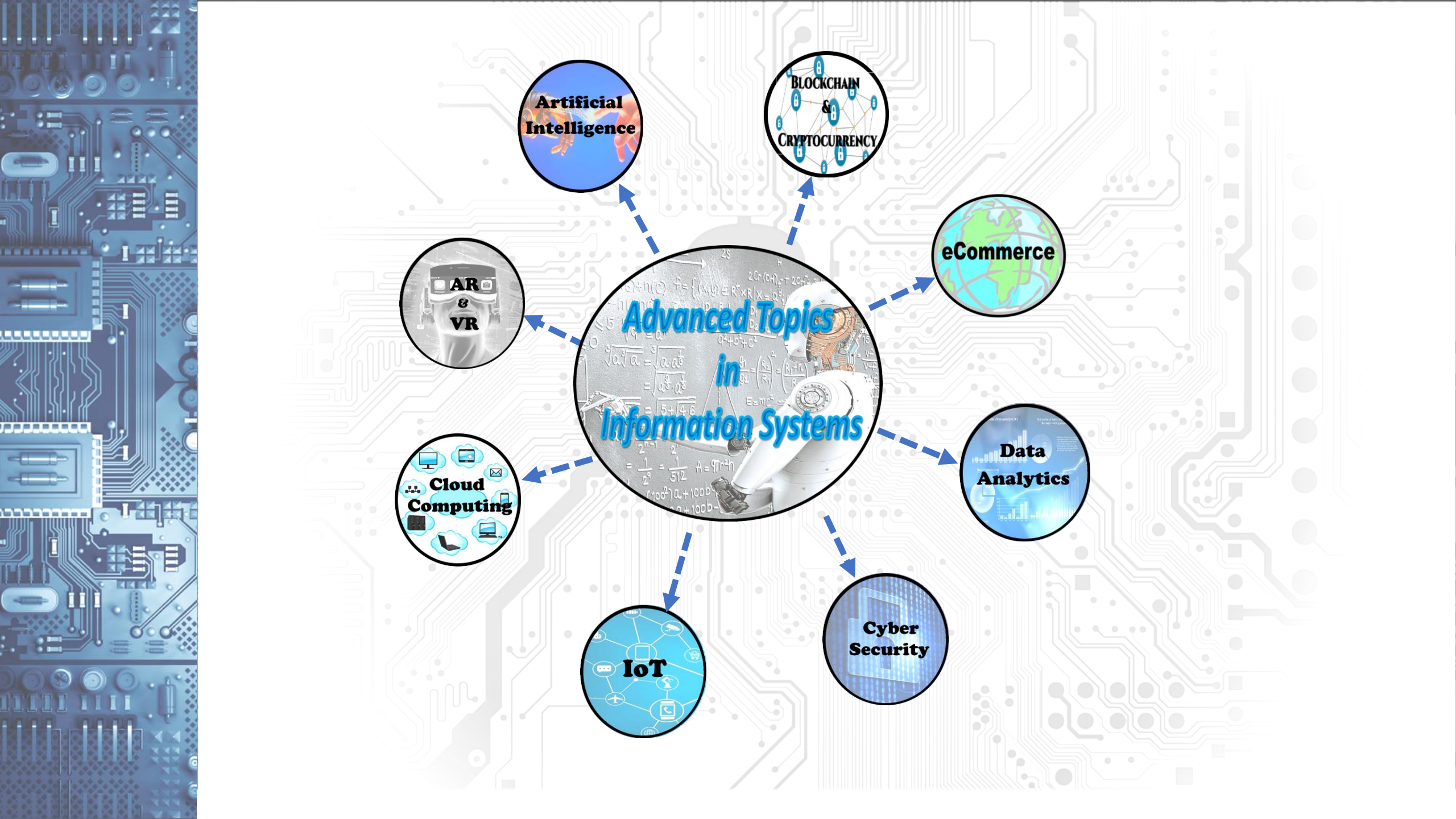
Advanced Topics in Information Systems

(FinTech)

CIS8690


Artificial Intelligence
Blockchain & Cryptocurrency
AR & VR
eCommerce
Advanced Topics in Information Systems
Cloud Computing
Data Analytics
IoT
Cyber Security

Why is Cybersecurity Important?

- Security threats are real…
- Certain aspects of their information must be protected
- We can’t keep our customers isolated from the INTERNET

Today's Cybersecurity Ecosystem

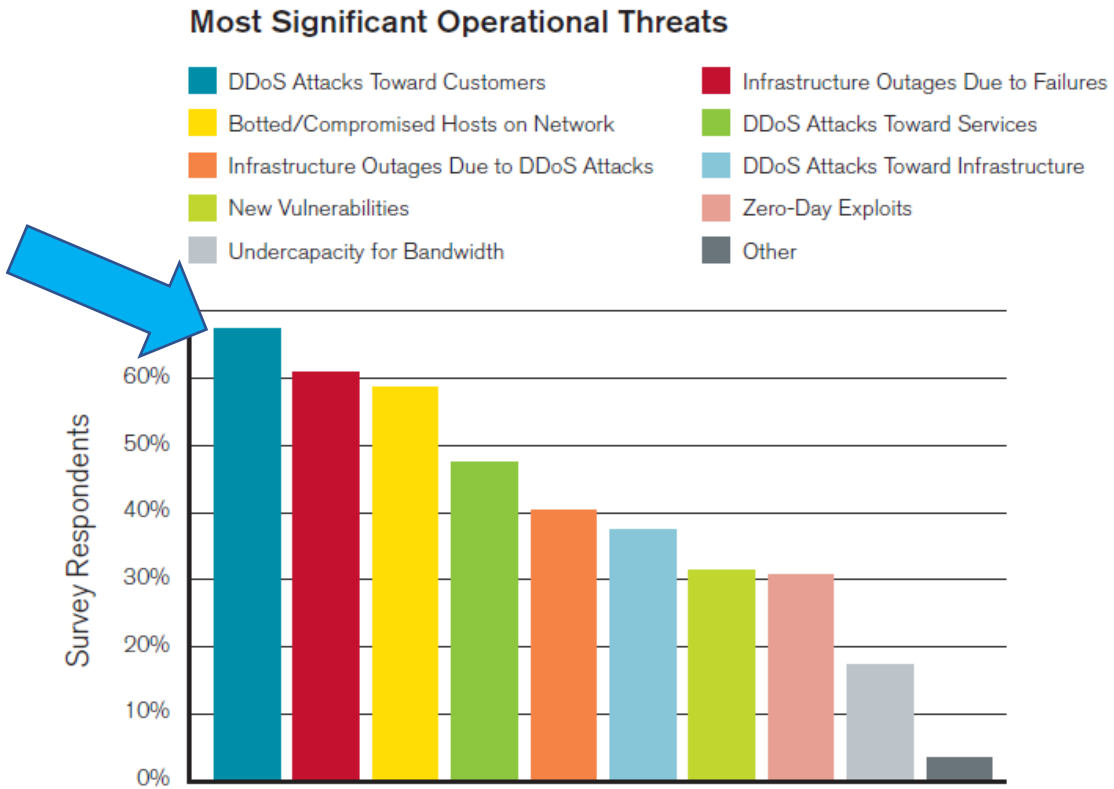
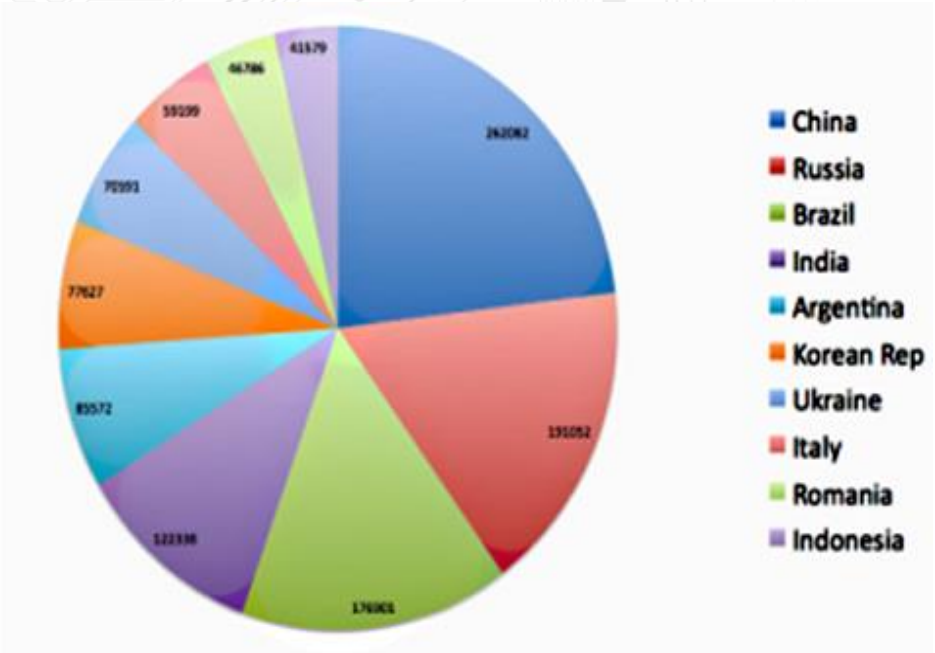


Figure 7
Source: Arbor Networks, Inc.



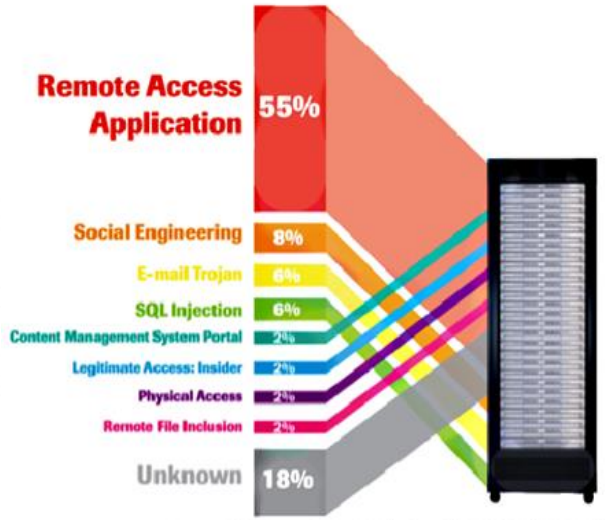
Most infrastructure attacks are unreported

Source: http://www.arbornetworks.com/report

Cyber Security

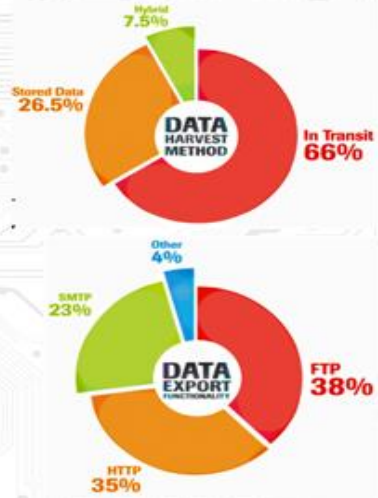
Breach Sources

Infiltration



Data infiltration is when new employees may bring in confidential **data** from outside source, and use their new employer's applications to store and share this confidential **data, but also brings in a virus in as well**.

Exfiltration



Data exfiltration occurs when malware **and/or** a malicious actor carries out an unauthorized **data** transfer from a computer.

Source: Trustwave Global Security Report
https://www.trustwave.com/global-security-report.php

Cyber Security

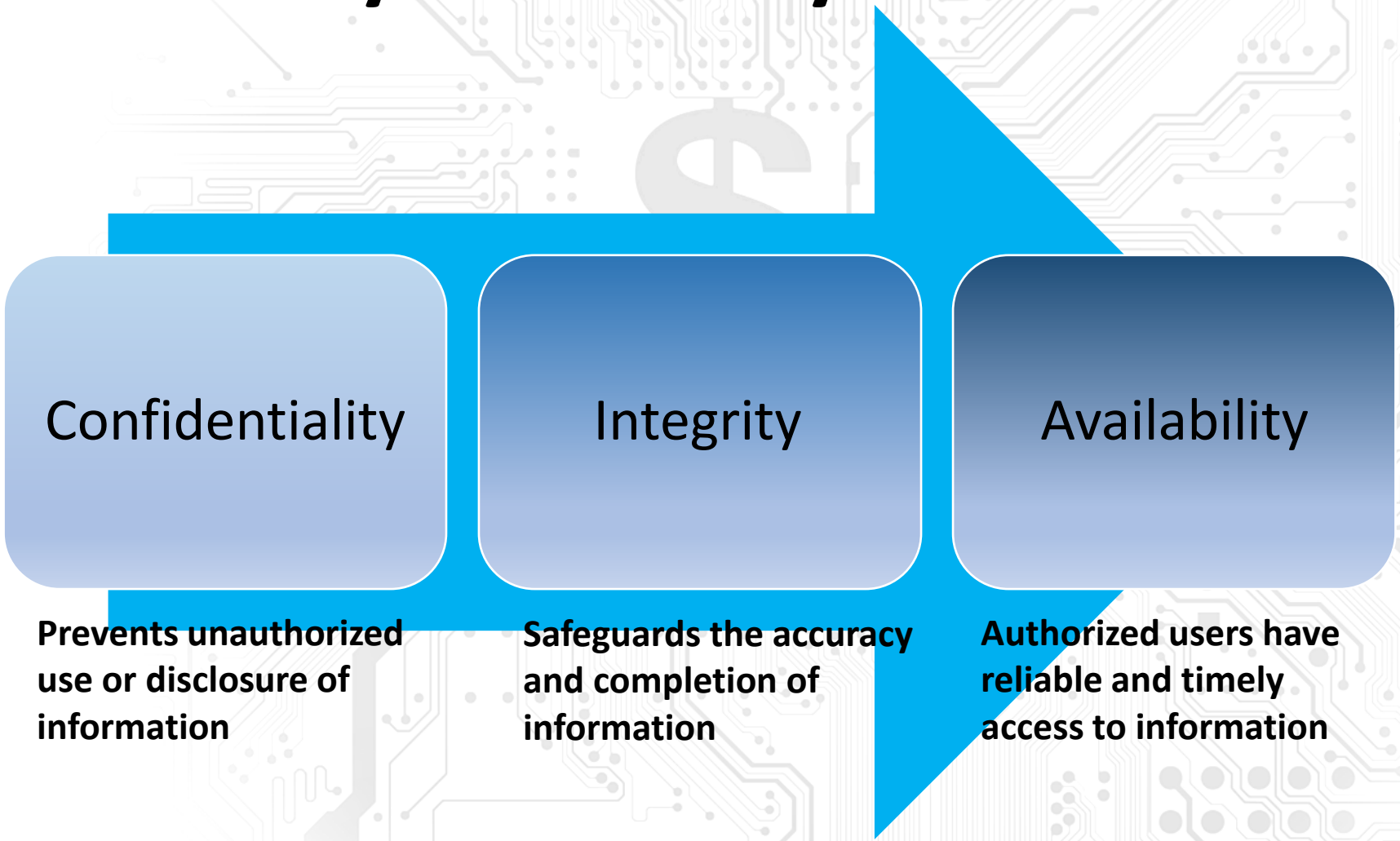
Tiers of Cybersecurity

Generic name for the collection of tools designed to protect data and to thwart hackers

Measures used to protect data during their transmission

Measures to protect data during their transmission over a collection of interconnected networks

Goals of Cybersecurity



Terminology

The ability to permit or deny the use of an object by a subject and provides 3 essential services:

1. **Identification** and authentication (Who can login)

1. **Authorization** (What authorized users can do)

2. **Accountability** (Identifies what a user can di

Cyber Security

Terminology

The possibility that a particular vulnerability will be exploited

3 step process of **Risk analysis:**

1. Identifying Security risks
2. Determining their impact
3. And identifying areas require protection

Cyber Security

Terminology

Any event with the potential to cause harm to a networked system

Examples:

1. **Denial of service**
   - Attacks make computer resources (i.e., bandwidth or disk space) unavailable to its intended users
2. **Unauthorized access**
   - Access without permission issues by a rightful owner of devices or networks
3. **Impersonation**
4. **Worms**
5. **Viruses**

Cyber Security

Risk management vs. Cost of Security

VS.

The process of selecting appropriate controls to reduce risk to an acceptable level

Determined by comparing the risk of security exposure to the cost of implementing and enforcing the security policy

Remember, NEVER spend more to protect something than it is worth

Cyber Security

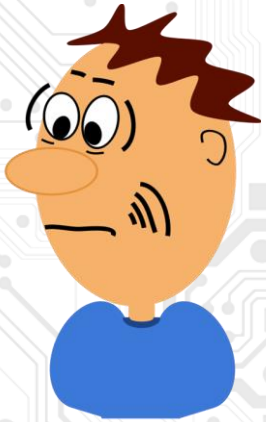
Attack Sources

Active

Writing data on the network
(like a virus)

Vs.

Passive

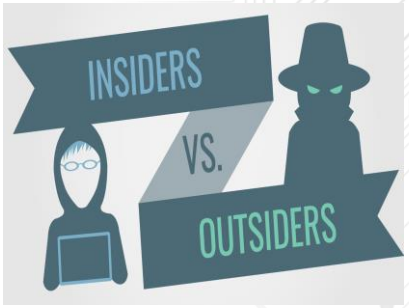


Reading data on the network
(like stealing PII)

Attack Sources

On-path vs. Off-path

- **On-path routers** (transmitting datagrams) can read, modify, or remove any data transmitted along the path
- **Off-path hosts** can transmit data that appears to come from any hosts but cannot necessarily receive data intended for other hosts
  - If attackers want to receive data, they have to put themselves on-path
- ***How easy is it to subvert network topology?***
  - **It is not easy thing to do but, it is not impossible**



Insider or outsider

- What is the definition of perimeter/border?

Deliberate attack vs. unintentional event

- Configuration errors and software bugs are as harmful as a deliberate malicious network attack

Cyber Security

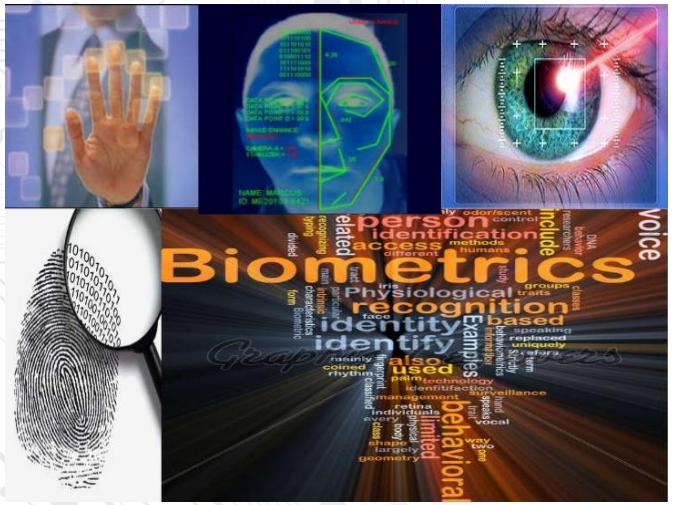
Common Fintech Methods of Preventative Security

1. **Biometrics**
2. Public Key Infrastructures
3. Certificates
4. Cryptographic Hash
5. Digital Signatures

Biometrics

- **Definition:** The study of **automated methods for uniquely recognizing humans, based on one or more intrinsic physical** or behavioral traits

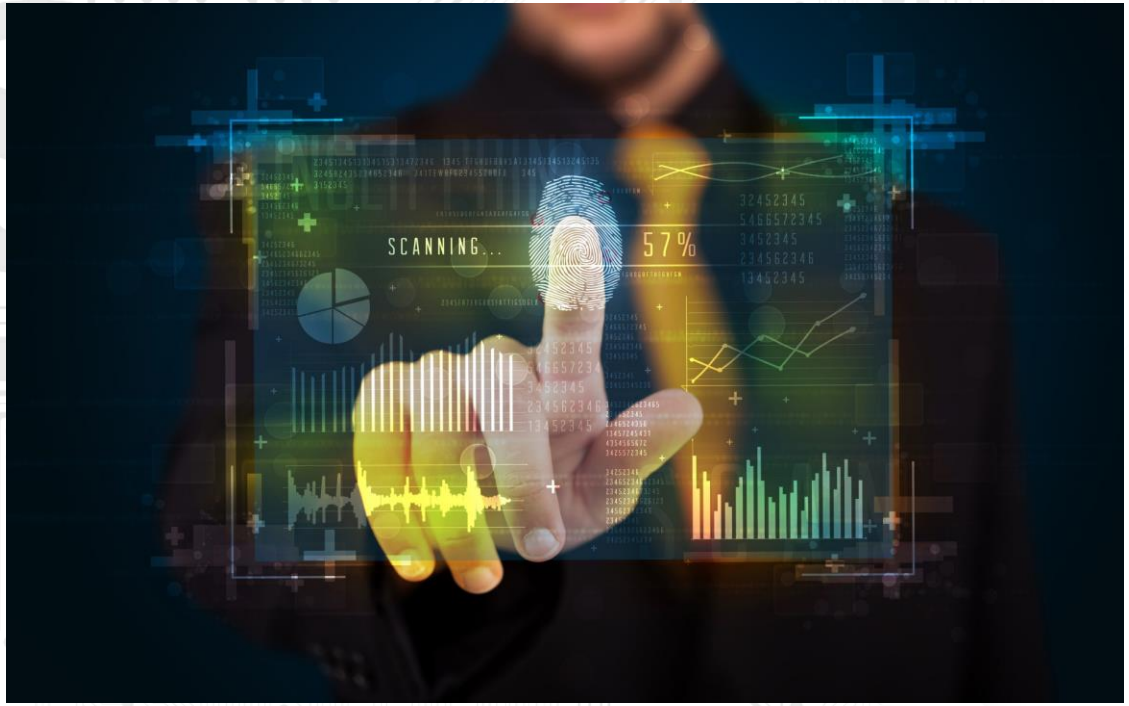
- ***Biometric Authentication***: **Technologies that measure and analyze human physical** and behavioral characteristics for authentication



Cyber Security

How Does Fingerprinting Work?

- **Fingerprint Capturing Technologies**
  - **Optical**
  - **Silicon**
  - **Ultrasound**



Iris Scanning

- The iris has a unique pattern from eye to eye and person to person
- Once fully formed, the texture is stable throughout lifetime of a person

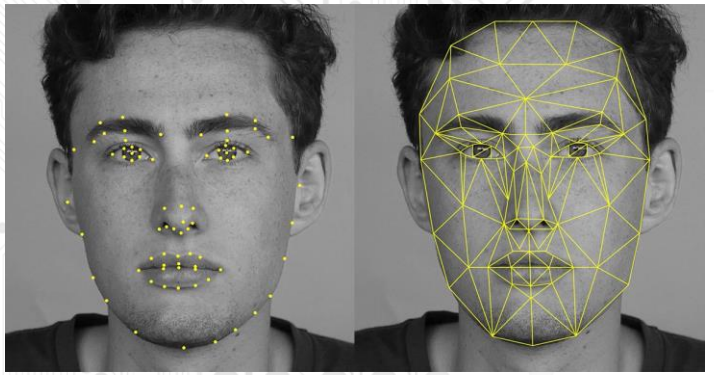
Iris Vs. Retina Scanning

- Retinal scans are an older technology
- People's retinas change as they age, which could lead to inaccurate readings
- Iris scanning is more precise and much faster

Cyber Security

Facial Patterns

- Nodal points - There are about 80 nodal points on a human face
- To prevent an image/photo from being used, systems will require the user to smile, blink, or nod their head
- Facial thermography can also be used to record the heat of the face (to stop mask frauds)



Cyber Security

How Do They Each Measure up?

BIOMETRTIC:	Uniqueness	Permanence	Collectability	Performance	Circumvention
Face	L	M	H	L	H
Fingerprint	H	H	M	H	H
Keystroke Dynamics	L	L	M	L	M
Iris	H	H	M	H	L
Retina	H	M	L	H	L
Signature	L	L	H	L	H
Voice	L	L	M	L	H
DNA	H	H	L	H	L

#1

H=High, M=Medium, L=Low

Cyber Security

Common Methods of Preventative Security

1. Biometrics
2. **Public Key Infrastructures (PKI)**
3. **Certificates**
4. Cryptographic Hash
5. Digital Signatures

What are Digital Certificates

A Digital Certificate is an "Electronic Password that allows a person or organization to exchange data securely using PKI

Where are Digital Certificates Used?

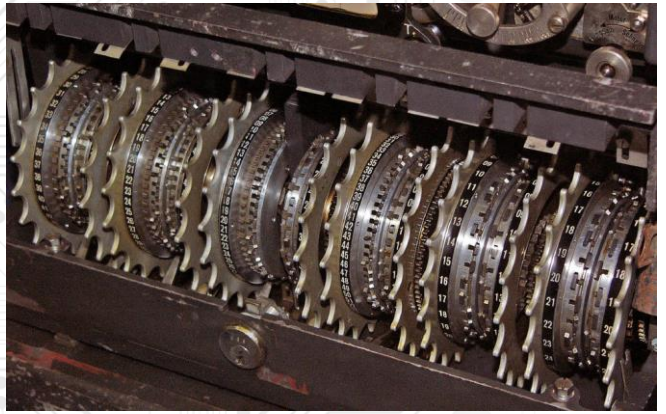
- In several Internet applications that include:
  1. Secure Socket Layer (SSL)
  2. Secure Multipurpose Internet Mail Extensions (S/MIME)
  3. Secure Electronic Transactions (SET)
  4. Internet Protocol Secure Standard (IPSec)

Common Methods of Preventative Security

1. Biometrics
2. Public Key Infrastructures
3. Certificates
4. **Cryptographic Hash**
5. **Digital Signatures**

What is Cryptographic Hash?

A **cryptographic hash function** is a mathematical algorithm that **maps data of arbitrary size to a bit string of a fixed size**



Definitions

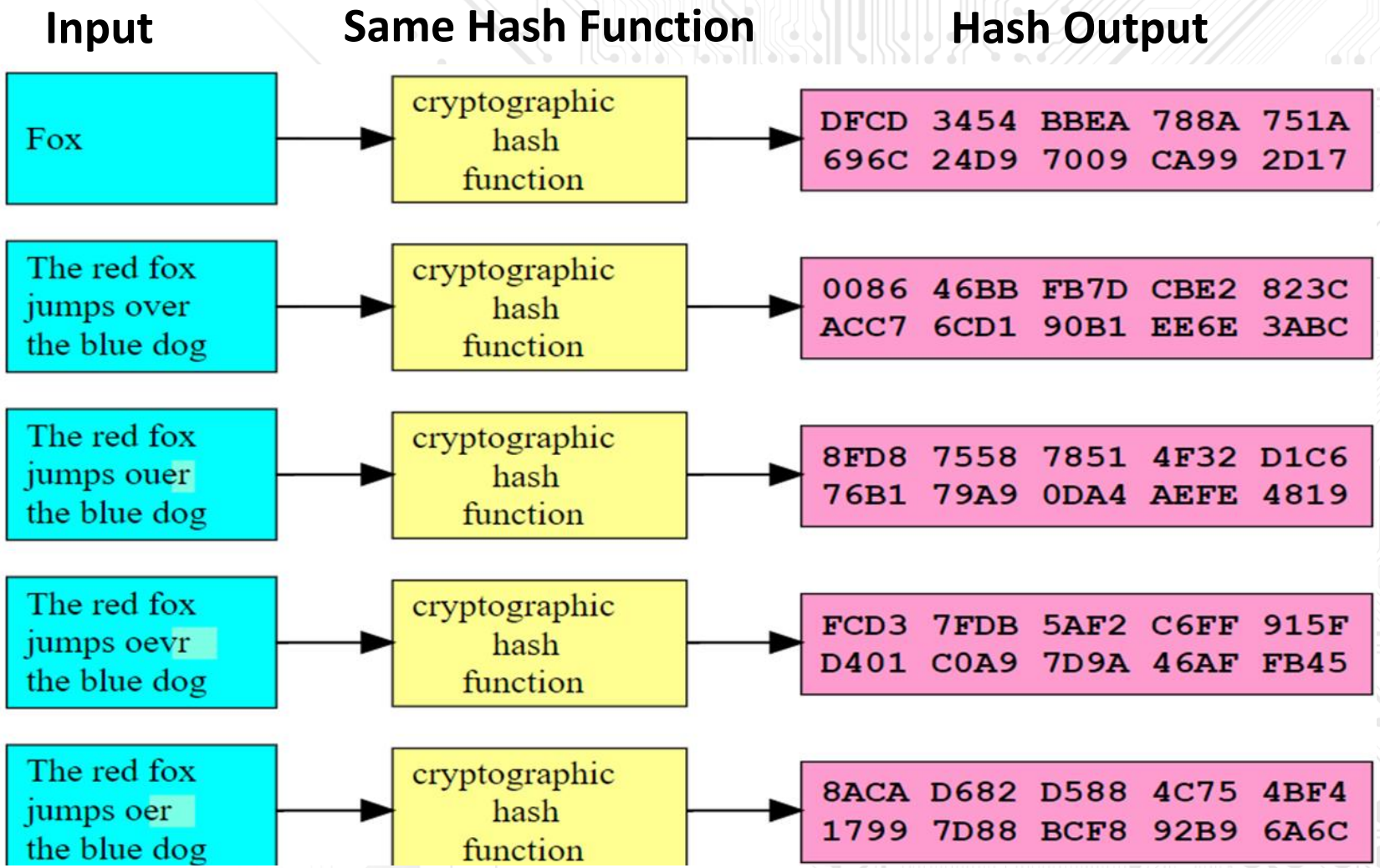
- **Cryptology** is about **constructing and analyzing methods to** prevent third parties or the public from reading private messages

- **Hash Function** is **any function that can be used to map data of arbitrary size onto data of a fixed size**.

Standard Algorithms are Incredibly Secure

- **128 bit key for a symmetric encryption algorithm has 2^{128} possible keys**
- Even with the endless computing resources **most of the software developers alive today will be dead before someone could break an encryption**
- Most security experts believe that **256-bit keys are good for the lifetime of the universe** (many billions of years).

Cryptographic Hash at Work



In looking at this diagram, you will notice a couple of things. First that all of the hash totals are using the same "Hash Function". Also that although the input increases in length, that the hash total remains the same!

Cyber Security

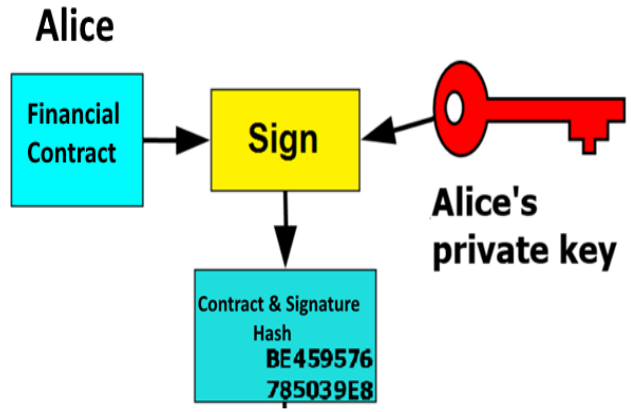
What is a Digital Signature

- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents
- A valid digital signature gives a recipient reason to believe:
  1. The message was created by a known sender (**authentication**)
  2. The sender cannot deny having sent the message (**non-repudiatio**n)
  3. The message was not altered in transit (**integrity**).

Cyber Security

Example

- Assume “Alice” wants financial advisor lawyer “Bob” in another country to receive her OK for a HUGE financial investment
- She wants to give Bob the assurance that the contract was unchanged and that it was really her that sent it!
  1. She copies and pastes the contract he sent her to review into an e-mail
  2. Using software on her device, she obtains a **message hash signature of the contract**
  3. **She uses a private key** that she obtained from a public-private key authority to encrypt the hash
  4. The **encrypted hash becomes her digital signature of the message** (*Note that it will be different each time you send a message)*



- **<u>At the other end, Bob (Financial Advisor) receives the message</u>**
  1. To make sure it's intact and from “Alice”, Bob use device software to **make a hash of the received message signature**
  2. Bob **then uses her public key to decrypt the message hash signature**
  3. **If the hashes match, the received message is valid**

Cyber Security

Mobile Security

Remember Fintech REQUIRES MOBILITY

Overview of Fintech Mobile Devices

- **Cisco: Over 10 billion mobile devices will be sold by 2020**
- **Fintech products must now connect to cellular networks**
- **Mobile *computers*:** Mainly smartphones, tablets, but with lot:
  - Sensors: GPS, camera, accelerometer, etc.
  - Computation: powerful CPUs (≥ 1 GHz, multi-core)
  - Communication: cellular/4G, Wi-Fi, near field communication (NFC), etc.

Cyber Security

Mobile Threats and Attacks in Fintech

- **<u>Mobile devices make attractive targets to Cyber Criminals:</u>**
  - People store personal info on them
  - Sensitive organizational info
  - Can fit in pockets, easily lost/stolen
  - Built-in billing system: in-app purchases

Mobile Device Loss/Theft

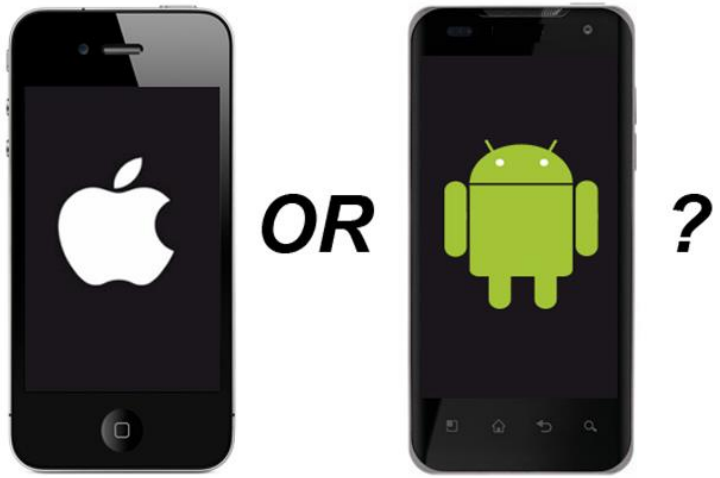
Many mobile devices lost, stolen each year

- 113 mobile phones lost/stolen every minute in the U.S.
- 56% of us misplace our mobile phone or laptop each month
- Lookout Security found $2.5 billion worth of phones in 2020 via its Android app
- Symantec found 50 “lost” smartphones throughout U.S. cities in just one scan
  - 96% were accessed by ‘***finders***’
  - **80% of finders tried to access “sensitive” data on phone**

Cyber Security

Mobile Device Malware

- Good news for Apple (iOS)
- Major increase in Android malware from 2017 to 2020
- Android malware growth keeps increasing exponentially



Mobile Device Search and Seizure Risk

- ***People v. Diaz (2011)*:**

  “ A Supreme Court of California case held that police are not required to obtain a warrant to search information contained within cell phone in a lawful arrest”

Location Disclosure

- Fintech Infrastructure will require mobile communication
- All device addresses are globally unique and identifiable
- ALL Peer-to-Peer mobile communications can be tracked

Fintech “Specific” Mobile Access Controls Needed

- Easy for attacker to control a mobile device if he/she has physical access
- Needed Fintech access controls for mobile devices
  - Authentication, authorization, accountability

Fintech Authentication Techniques

- **Authentication generally based on:**
  - **Something customer knows**
    - Password/passphrase
    - Unlock pattern
  - **Something customer has**
    - Magnetic key card
    - Smart card
    - Token device
  - **Something customer is**
    - Biometrics (Fingerprint, Retina Scan, etc.)

Cyber Security

Fintech Authentication: Comparison

	Passwords	Smart Cards	Biometrics	Pattern Lock
Security	Weak	Strong	Strong	Weak
Ease of Use	Easy	Medium	Hard	Easy
Implementation	Easy	Hard	Hard	Easy
Works for phones	Yes	No	Possible	Yes

- All of these authentication techniques have good and bad aspects!
- Passwords and Pattern Locks are the most widely used, but are the weakest form of protection.
- Therefore, many mobile devices are now “Biometric” enabled, which provides strong protection, but can be problematic in its usage

Bigger problem: mobile devices are designed with single-user assumption…

Payment Card Industry Data Security Standards

PCI DSS COMPLIANT

Protecting Cardholder Data with PCI Security Standards

- As of 2020 More than 300 million records with sensitive information have been breached in the U.S. alone
- Compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) helps to alleviate these vulnerabilities and protect cardholder data for Fintech customers.

But some businesses aren't helping!

Risky Behavior

A survey of businesses in the U.S. and Europe reveals activities that may put cardholder data at risk.

81% store payment card numbers

73% store payment card expiration dates

71% store payment card verifcation codes

57% store customer data from the payment card magnetic stripe

16% store other personal data

Source: Forrester Consulting: The State of PCI Compliance (commissioned by RSA/EMC)

THE THREE P'S of PCI

PII: Protected Identifiable Information

PCI: Protected Consumer Information

PHI: Protected Health Information

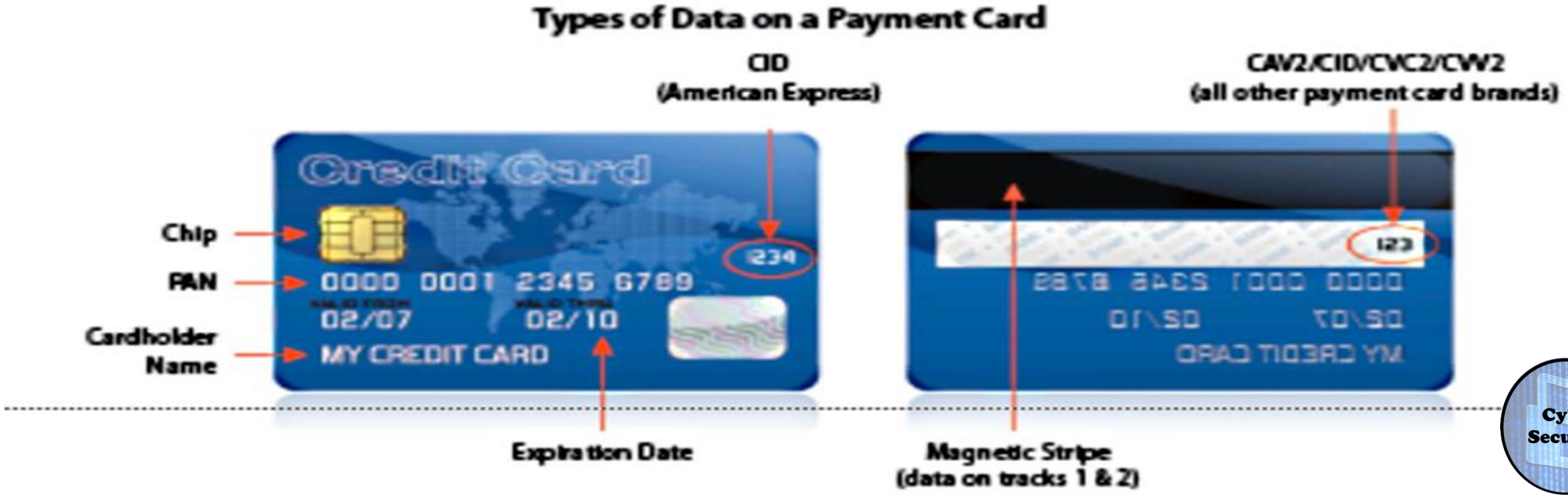
The levels of importance from a Security Perspective

- **PHI is the most important and most secure**. It is currently regulated by Federal Law (**HIPAA- Health Insurance Portability and Accountability Act**)
- **PHI>PCI>PII**
- **Both PCI and PHI contain a significant amount of PII**

WHAT IS PCI (Protected Consumer Information) DATA?

Cardholder data and sensitive authentication data are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

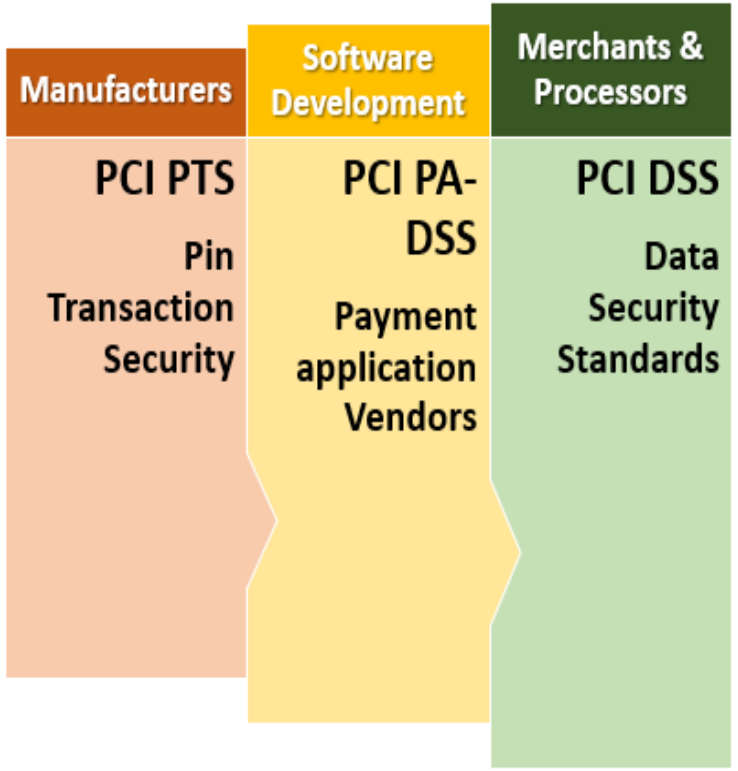


Cyber Security

Overview of PCI Security Requirements

- PCI security standards requirements set by the PCI Security Standards Council (PCI SSC)
- Applies to all organizations that store, process or transmit cardholder data
- Guidance for software developers, manufacturers of applications and devices used in those transactions
- The Council is responsible for managing the security standards
- Compliance standards is enforced by the founding members of the Council

<u>Payment Card Security Standards</u>



Cyber Security

Required *Fintech* PCI Controls

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

New World of Fintech Increases Risk

Data Privacy is Paramount in Fintech

Cyber Security

Data Privacy in an “Ethical” Fintech

Fintech New Markets Create New Cybersecurity Challenges