asset : tài sản

stakeholder : các bên liên quan

thrive : phát triển

triad : bộ ba

integrity : toàn vẹn/chính trực

availability :sẵn có

pace : nhịp độ

mitigate : giảm nhẹ

start over: bắt đầu lại

glossaries: từ điển thuật ngữ

assess : đánh giá

reside: cư trú

breach: xâm phạm

-------------------------

confidentiality: bí mật

exploitation : bóc lột

compromise: thỏa hiệp|xâm phạm

compromised kɑːm.prə.maɪz: bị xâm phạm

vendor: nhà cung cấp

abuse: lạm dung

------------------------

-Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.

-Security controls are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture(tình trạng)

Security posture is an organization’s ability to manage its defense of critical(chỉ trich/then chốt) assets(tài sản) and data and react to change. A strong security posture leads to lower risk for the organization.

mitigate: giảm nhẹ

compliance kəmˈplaɪ.əns: tuân thủ

-Compliance is the process of adhering(tham gia vào) to internal standards and external regulations(quy định) and enables organizations to avoid fines and security breaches

A threat actor, or malicious(độc hại) attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.

At times: đôi khi

accidental ˌæk.səˈden.t̬əl: tình cờ

regulatory: quy định

fines: tiền phạt

audits: kiểm toán/kiểm tra

obligation : nghĩa vụ

fraud : lừa đảo

manifest : biểu hiện

evole : tiến hóa

penetration: thâm nhập

proactive: chủ động

passive : bị động

conduct periodic security audit

conduct : chỉ đạo

periodic [ˌpɪr.iˈɑː.dɪk] : định kì

audit : kiểm toán|| kiem tra

examine : nghiên cứu

phishing : lừa đảo

terminology: thuật ngữ

---------------

confidentiality : bí mật, integrity: toàn vẹn, and availability

staying informed : cập nhật thong tin

------------

interpreting : phiên dich

forensic: pháp y

preserve : bảo tồn

meet : đáp ứng

compromise: thỏa hiệp

event management (SIEM) tools

Intrusion : sự xâm nhập

Intrusion detection systems (IDSs)

mutual : cộng đồng

vital : thiết yếu

variant: biến thể

emerge ɪˈmɝːdʒ: xuất hiện

expose :lộ ra

infer : suy luận

strict : chặt chẽ

biometric : sinh trắc học

fraud : gian lận

impersonating : mạo danh

Digital forensic investigators identify, analyze, and preserve criminal evidence within networks, computers, and electronic devices.

crawl: thu thap

tally: kiểm đếm

credential : thông tin xác thực

social engineering : thao tác kĩ thuật khai thác lỗi con người để lấy thông tin

trade-off : đánh đổi

evolve: phát triển

shift: thay đổi

phishing : giao tiếp digital để lừa mọi ng tiết lộ data

infiltrated : xam nhap

settled : giai quyet

--------------------------------------------------------------

Ransomware : phần mềm tống tiền

Intimidation : đe dọa

impersonate : mạo danh

Consensus : đồng thuận

Scarcity : sự khan hiếm

imply : ám chỉ

exploited : khai thác

- Spear phishing lừa đảo trực tuyến : A malicious email attack targeting a specific user or group of users that appears to originate from a trusted source

- phishing : The use of digital communications to trick people into revealing sensitive data or deploying malicious software

- Whaling : A form of spear phishing during which threat actors target executives(giám đôc) in order to gain access to sensitive data

- Business email compromise (BEC) :An attack in which a threat actor impersonates a known source to obtain a financial advantage

- Vishing : The exploitation(khai thác lien tuc) of electronic voice communication to obtain sensitive information or to impersonate a known source

Watering hole attack : An attack in which a threat actor compromises(xâm phạm) a website frequently visited by a specific group of users

Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor(người bán ) to obtain unauthorized access to a physical location

pirated : lậu

outcry : phản ứng , chống đối

evolve : tiến hóa

involve : có liên quan

----------------------

8 DOMAINS

mitigation : giảm nhẹ

retention : giu lai

=========================================

\*security and risk management : Quản lý rủi ro, chính sách bảo mật, tuân thủ pháp lý, quản trị doanh nghiệp, và quản lý khủng hoảng

\*Asset security: luu tru, duy tri ,retention: giu lai, pha huy data

\*security architechture and engineering : lam viec voi firewall,Thiết kế và bảo mật hệ thống, các mô hình bảo mật, và đánh giá các yếu tố bảo mật.

\*communication and network : lam viec voi mang vat ly va khong day ,Bảo mật mạng, thiết kế kiến trúc mạng, và quản lý các biện pháp bảo mật mạng.

\*identity and access management : giữ cho dữ lieejeu được bảo maajt, đảm bảo người dùng tuân theo chính sách để đảm bảo và control tài sản vật lý vd mạng hoặc appications(keycard access)

\*security assessment(đánh giá) and testing : tiến hành điều khiển ktra, thu thập, phân tích dữ lieu , tien hanh kiem tra bao mat de theo doi rui do , moi de doa , khả năng tổn hại

\*security operations : conducting investigations and implementing preventative measures

\*software development security

========================================

- password attack types : Brute force, Rainbow table

- Password attacks fall under the communication and network security domain.

Social engineering attack : Phishing,Smishing,Vishing,Spear phishing,WhalingSocial media phishing,Business Email Compromise (BEC),Watering hole attack,USB (Universal Serial Bus) baiting,Physical social engineering

fall under : thuoc cai gi do

- Social engineering attacks are related to the security and risk management domain

- Physical attacks fall under the asset security domain: Malicious USB cable,Malicious flash drive,Card cloning and skimming

- Adversarial artificial intelligence falls under both the communication and network security and the identity and access management domains.

- Supply-chain attack

- Cryptographic(mật mã) attacks fall under the communication and network security domain(An attack that affects secure forms of communication between a sender and intended recipient): Birthday,Collision,Downgrade

------------------------------

ATTACKER

patents: bằng sáng chế

Sabotage: phá hoại

Espionage : gián điệp

intellectual : thuộc về trí tuệ

Demonstrations: biểu tình\trình diễn\bày tỏ\thuyết minh

Propaganda : tuyên truyền

adhere : tuân theo

confidential : bảo mật

agenda : chương trình nghị sự

audit : kiểm tra

agenda vɪdʒ.əˈlæn.t̬i : cảnh giác

\*Advanced persistent threats

\*Insider threats

\*Hacktivists

--------------------------------------------

sought-after : được săn đón

inadvertently : vô tình

-----------------------------------------

security framework:

protecting pii

securing financial infor

identify security weakness

nmagnae organization risk

align security business goal

vital : thiết yếu

mandatory : bắt buộc

CIA triad (condidencialy – integrity -avilability ): mâu giúp cho doanh nghiệp xem xét tới rủi ro khi setup hệ thống hoặc chính sách

**Security frameworks** are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:

1. Identifying and documenting security goals
2. Setting guidelines to achieve security goals
3. Implementing strong security processes
4. Monitoring and communicating results

NIST cybersecurity framewok (CSF) : cái doanh nghiệp sử dụng để phòng chống rủi ro

Compliance : tuân thủ

Regulations: quy định

Obligation : nghĩavụ

Unbiased: 0 thiên vị

Entrusted : giao phó

Privilege : đặc quyền