(week 13) Cybersecurity and data privacy

What is meant by cybersecurity?

Cybersecurity is about protecting technology, but it is also about protecting information that information can include data about your behaviors such as: What you do? Where you go? What you buy? What you eat? Which websites you visit?

Consumer privacy strategies?

- be open and honest about consumer data
- protect consumer data by default
- Have clear and concise communication about privacy

Defining privacy:-

- the right to be left alone (beeing free from unwantes or undue intrusion or disturbance in one's private life or affairs)
- the state of being apart from other people or concealed from their view
- freedom from intursion, interference, scruting or surveillance

Data/information privacy:-

- the right to have some control over you personal information (Activity, identity, about you)
- How, when, where and why it is collected and used
- only used for it's intended purpose

Why privacy-consumer :-

- economic loss/identity theft / fraud meaning someone takes your personal information and use it to steal from you
- Dignity loss / Embarrassment that sould someone find out the website you may be viewing at home
- Discrimination is another potential privacy concern if someone learns about your political views and disagree
- Control over information / logs self determination. individuals should have control over their information and know how it may be used, shared and stored
- Confidence and trust. if you feel your privacy has been violated. you have less trust in that insistution

Why privacy-Business (3Rs)

- Reputation السمعة
- Revenue الربح
- Regulation الأنظمة

verizon Data Breach investigations Report (DBIR)

- Ransomware
- Human element / social engineering / phishing
- Human error
- Web application vulnerabilities
- Credentials / user-ids and passwords

the (DBIR):-
is an annual publication that analyzes information security incidents with a specific focus on data breaches
What is personal/protected information (PI)?
identifies an individuals or household
- Who they are like (full name, paspore number, tek no dote of birth)
- Where they are phisicolly located overen logecly on the internet
- what they are (finger print, facial recognation)
- What they are doing (personal info such as web viewing and other source of habits)

What is personally Identifiable Information (PII)?
is information that find you or an individuale and include your name, address, number
What is protect Health Information (PHI)
is all individualy identifiable health information, including demographic data, medical histories, test results and other information used to identify a patcint or provide health care services

protected data life cycle and data processing stages

- It starts with collection or generation for example when I sign up on a new site with my demograph information it can also be generated from other data. think of this as the birth of the data element in your system
- once the data is initiated, it is transmitted across networks. for example. from the website to a backend database
- processing is the next stage in the data life cycle Data is used within computer applications to complete a task, such as credit card processing or validating my identity
- protected data is often stored for future use this storage can take a few seconds to confirm a valid credit card purchase for too many years to meet data retention regulation
- Another possible stage in data's life cycle is sharing with other validated parties and disclosure to the individual this may be required by regulation
- the last stage is destroying the data when it is no longer required

(Week 14) Cybersecurity

Internet of things (IOT) :-
refers to any thing connected to a network, such as computers, laptops and desktop computers as well as those we don't see in our cars, TVs, speakers the clouds - which enables systems, applications, and data to be reached from anywhere using almost any device. All these devices require security to ensure they are only being used for their intendy purpose.

What is cyber security?
it is the practice of protecting critical systems and sensitive information from digital attack
eg: Company's valuable digital sets such as costumers information and the code files can be targeted and attack by malicious actors
to safeguard these digital assets the company must leverage tools techniques and policies to actively protect the asset from thes attacks

The 3 key matras of a security mindset?
1- trust. but verify (check everything you do)
2- stop. think. connect (take a few seconds to think)
3- if you see something. say something (make report)

Security trends:-

How:- phishing - ransomware - bussiness email compromise

No.1 way for scams:- social engineering

New ways:- smart devices - IOT - cloud services

More opportunities:- Cybersecurity professionals

phishing variations:-

- spear phishing
- whaling
- SMS-ishing (smishing)
- vishing (voice mail)
- instant message (chat)

Ransomware:-

- Malicious software
- Block access to computer system
- often accept Bitcoin as payment

Business Email compromise (BEC):-

- Access to a business email account
- imitates the owners identity
- Defraud the company and its employees, customrs or partenrs

social engineering and scams:-

An attemp to trick someone into revealing info like pass that can be used to attack system

Smart devices, IOT and cloud services :-

security challenges :-

- only authorized people and systems have access
- used in ways they were intended

The CIA traid :-

- Confidentiality that means to protect the info from unauthorized users (No one can see your private information)
- integrity which means make sure the data is reliable and accurate (No one has modifies your accounts)
- Availability which means ensure the data and system is available when needed (you can get to your money when you need it)

the principles of least privilege :-

is all about controlling who can or cannot gain access to something such as a database or a device It involves giving people the minimum privileges or permissions needed to do their job

To fail safe :-

means to anticipate how things can go wrong and to ensure when it does thing are in a safe state and the safe state should be default

7k layers that protecting data:- (protections)

Data → Application → Host → Network →

policies, procedure, Awars ← physical ← perimeter

Defense in depth examples:-

- encryption
- malware protections
- Host and network fire walls
- multi factor authentication

(week 15) security controls, risk mangmnt and the hacked minds of

- security principles :-

① economy of mechanism
  - keep thing small and simple.
  - Bigger is not better. it just means there is more to protect and complexity is an enemy of security.
  - complex systems are harder to defend bec you need to understand all of the ways to access them and how processes can be broken to allow unauthorized activities.

- fail-safe defaults :-
ensure a safe state by default when it fails
-fail smart (fail open)
  - walk in freezer; power goes out (fail) door open by default (safe)
  - internet website; firewall fails website shut by default (safe) (fail shut)

- Least privilege :-
only have the access you need
  - employee badges
  - administrator rights

• choke points and defense in depth :-
• choke point - only way in or out
• defense in depth - layers of security
• Gorerance :-
process to meet business goals and objectives
• Compliance :-
following established rules
G → is having a framwork for structuring how your system and data are secured gorernace helps with processes when it comes to meeting bussiness
C → the process of meeting a third party's requirments for digital security with the aim of enabling business operations in a particular market or with a particular customer.
CIS cybersecurity Best practices
CIS means :- (center of internet security)
• CIS controls
• CIS Benchmarks
* Cis Controls :-
implementation steps :-
• 20 actions in order of priority
• provide defense in depth

- three levels :-
  a. Basic controls
  b. foundational controls
  c. organizaton controls

Basic controls :- (controls that should done every organizt)
1- inventory and control of Hardware assets
2- inventory and control of software assets
3- continuous vulnerbility mangrement
4- controlled use of administrative privileges
5- secure configuration for hardware and software on mobile devices, laptops, servers
6- maintenance, monitoring and analysis of Audit logs

foundtional Controls :- (add additional sec layers)
1- email and web browser protections
2- malware defence
3- limitation and control of network ports protocols and services (firewall)
4- data recovery capabilities
5- secure configuration for network devices such as firewalls, Routers, switches
6- Boundary defense
7- data protection

8- controlled Access based on the need to know
9- wireless access control
10- account monitoring and control
Organizational controls :-
1- implemnt a security awareness and training program
2- application software security
3- incident Response and mangment
4- pentration tests and Red team exercises
Risk mangement :-
is identifying potential risks in advance, analzing them, and taking precautionary steps to reduce risk the risk mangement process includes :-
1- Risk identification
2- Risk analysis
3- develop Risk Response plan
Risk = exposure to danger
threat = potential damage
vulnerability = unintended flaw
Asset = has value
exploit = attack
pentration testing = test methodology which mostly under

Hacker process :-

- goal / target
- learn it
- explore it
- break it
- explore it

Ethical hacking life cycle :-

1- A target or goal : understand why you are assessing its security

2- learn it : learn as much as you can about it.

4- Break it :- understand the target's weaknesses or vulnerabilities

3- explore it :- is understanding how it works and what others know about it. this is known as (reconnaissance)

5- fix it :- secure operating system, applications, and networks

6- make it better :- figure out a better way to secure the asset

7- tell others :- tell others what you find, it called (ethical disclosure)

What is the difference between hacking and ethical hacking?

Ethical hacking (hakers) help an organization find weakness so that they can be known and fixed. but hackers find these

penetration testing = A test methodology in which assessors, typically working under specific constains, attempt to circumvent or defeat the security features of an information system