Week 1

Why Privacy – Consumer:

- Economic loss / Identity theft / Fraud
- Dignity Loss/ Embarrassment
- Discrimination
- Control over information / Loss of Self Determination
- Confidence and trust

Why Privacy – business 3Rs:

Reputation: السمعة وثقة العملاء

Revenue:خسارة العملاء

Regulation:غرامات مالية

The Verizon Data Breach Investigations Report(DBIR):

يقدم تحليلات عن حوادث امن المعلومات

- Ransomware
- Human element/Social Engineering / Phishing
- Human Error
- Web application vulnerabilities
- Credentials/user-ids & passwords

BEC(business email compromise): تهكير الايميل

CDB(Computer Data Breach):اختراق بيانات الكمبيوتر من خلال الثغرات الأمنية

The California Consumer Privacy Act (CCPA)

Personal/Protected Information (PI): معلومات شخصية-محمية كالفرد واسرته

Identifies an individual or household

- Who they are
- Where they are
- What they are
- What they are doing

Includes:

Personally identifiable information(pii): معلومات تحددك كفرد في المجتمع كالاسم والميلاد والرقم التاميني والايميل

Protect health information(phi)

Cardholder data معلومات مالية

Browsing habits

Data life cycle:

1. Collection or Generation
2. Transmission
3. Processing
4. Storing
5. Sharing / Disclosure
6. Destruction

Risk management:

- Compliance: التأكد ان كل شي يسير بشكل سليم
- Security: العمليات والتكنولوجيا اللازمة للحماية
- Privacy: إبقاء المعلومات في سرية

data privacy: حماية المعلومات الشخصسة واستخدامها

cybersecurity: مفهوم أوسع غالبا في المعاملات التجارية ومثلا خسارة التوفر والنزاهة او خسارة جهاز او شبكة

cybersecurity hygiene: ممارسات (عادات) لحماية انفسنا الكترونيا

protecting yourself online:

Defeating Social Engineering

Think before you click

Trust your gut – Be a little skeptical

When in doubt, ASK

Multifactor Authentication (MFA)- Using at least two of the following, something you

Know (password)

Are (fingerprint, face, voice)

Have (smartphone, card)

Device Security:

- AntiVirus (AV) applications
- Patching and Updates
- Wireless (WiFi) Security - Home and Remote

Weak 2

Internet of things(IOT): أي حاجة متصلة بشبكة

The Cloud: enables systems, applications, and data to be reached from anywhere using almost any device

Cybersecurity involves the ability to understand past and current trends to understand the future better.

Security Trends:

- Phishing, Ransomware & Business Email Compromise
- Social Engineering & Scams
- Smart devices, IoT & Cloud Services
- More opportunities for cybersecurity professionals

The CIA Triad: يتضمن اهداف السايبر سيكيوريتي

Confidentiality: السرية وهي حماية المعلومات من غير المصرح لهم

Integrity: النزاهةو السلام وهي و ايمكانية التاكد من ان المعلومات دقيقة وصحيحة

Availability: ان تكون المعلومات متاحة عند احتياجها

Least privilege: عدم إعطاء سماح لاعضاء لاشياء لا يحتاجونها او غير ضرورية

To fail-safe: توقع كيف تسير الأمور علي شكل خاطي وان حدث التأكد ان تكون بامان وقتها

Defense in depth: using multiple layers at the same time to help keep data and systems safe from an attack

Layers of a computer system:

- Data is at the center.
- Outside of the data is the application that uses the data to provide services to us.
- When you open an application, it runs inside operating
- On the outside, it's the network that connects different devices to allow data-sharing.
- Surrounding each of the layers are humans that interact with them and enjoy the services.

Week 3

Security Principles

1. Economy of mechanism

- Keep things small and simple. Bigger is not better. Because Complex systems are harder to defend
- Fail-safe defaults (already mentioned)
- Least privilege (already mentioned)

2. Choke points

- Only one way in and one way out.
- Defense in depth (already mentioned)

3. Other principles

- Least common mechanism
- User-friendly interface
- Complete mediation
- Open design
- Separation of privilege

Governance: تنظيم كيفية ان يكون سيستمك بامان

Compliance: الامتثال لقواعد الجوفيرينس

Center for Internet Security control(CIS):

Best Practices:

CIS Benchmarks™: are guidelines to secure or lockdown operating systems, software, applications, and networks.

Critical Security Controls(CIS controls): activities for organizational security.

Implementation groups:

Basic controls:

1. **Inventory** and Control of **Hardware** Assets

2. **Inventory** and Control of **Software** Assets

3. Continuous **Vulnerability Management**

4. Controlled Use of **Administrative Privileges**

5. **Secure Configuration** for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

6. Maintenance, Monitoring, and Analysis of **Audit Logs**

Foundational controls:

7. Email and Web Browser Protections 8. Malware Defenses 9. Limitation and Control of Network Ports, Protocols, and Services (Firewall) 10. Data Recovery Capabilities 11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches 12. Boundary Defense 13. Data Protection

Orgnasational controls:

17. Implement a **Security Awareness** and Training Program

18. **Application** Software Security

19. **Incident Response** and Management

20. **Penetration Tests** and Red Team Exercises

Risk Management terms:

Risk management terms:

- Risk: موقف يتضمن التعرض للخطر
- Threat:المسبب في الخطر
- Vulnerability:(ثغرة) عيب غير مقصود بالسيستيم
- Asset: شي ذو قيمة
- Exploit: الهجوم الفعلي

Hacker mindset:

Ethical Hacking Lifecycle:

The Hacking Lifecycle

Week 4

Vulnerability management:

1. Identification
2. Analysis
3. Action

Examples of vulnerabilities in information technology:

- Code / Software apps
- Networks
- Unpatched systems

vulnerabilities Sources include:

- Vendors
- Vulnerability lists & databases
- Bug Bounties
- Security assessments

Zero-Day (0-Day) Vulnerabilities: ثغرات لم يتم معرفتها من قبل الشركة او الجمهور

Examples of threats with information technology

- Malicious hacker
- Disclosed passwords
- User error

Threat source: الشخص او الشي الي هيسبب ضرر

Threat vector: الطريقة الي بيها هيقدر الثريت سورس يسبب ضرر