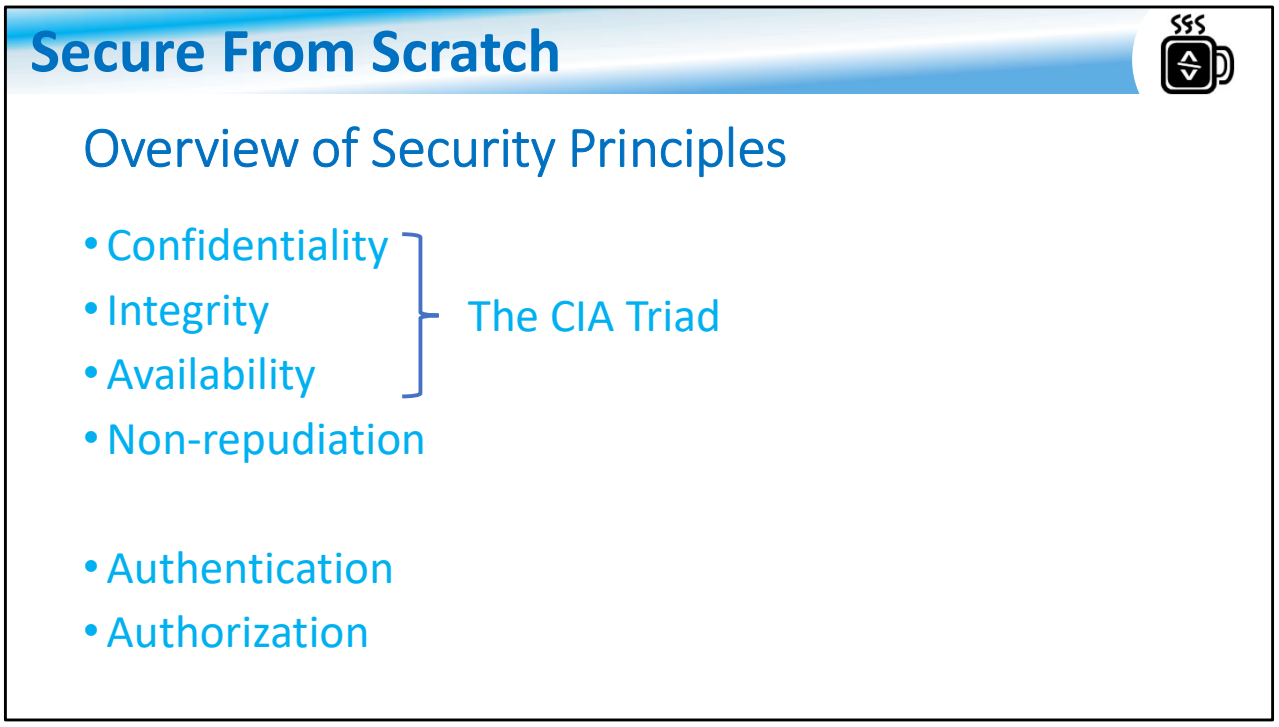
Security Breach Damage & Cost



- **CIA Triad:**
  - **Confidentiality:** Ensuring that information is only accessible to those authorized to view it.
  - **Integrity:** Protecting information from being altered by unauthorized parties.
  - **Availability:** Ensuring that information and resources are available to authorized users when needed.
- **Non-repudiation:** Ensuring that actions and transactions can be tracked to prevent denial of action.

Not so much security principles - but basis for security implementation:

- **Authentication:** Verifying the identity of users and systems.
- **Authorization:** Determining what resources and actions a user or system can access.

Secure From Scratch

Confidentiality
Integrity
Availability
Non-repudiation

When Security Principles Break…

We can *bypass* the security.

Exploit – bypassing security principles to make money/cause harm

Confidentiality Bypass: Data leaks

- Steal someone's identity
- Access military secrets
- Use credit cards

Examples of what happens if a security principle is not upheld:

- **Confidentiality:** Ensuring that information is only accessible to those authorized to view it.

Secure From Scratch

Confidentiality
Integrity
Availability
Non-repudiation

When Security Principles Break…

We can *bypass* the security.

Exploit – bypassing security principles to make money/cause harm

Integrity Bypass: Data manipulation

- Change product price
- Transfer money
- Encrypt database (Ransomware)

Examples of what happens if a security principle is not upheld:

- **Integrity:** Protecting information from being altered by unauthorized parties.

Secure From Scratch

Confidentiality
Integrity
Availability
Non-repudiation

When Security Principles Break…

We can *bypass* the security.

Exploit – bypassing security principles to make money/cause harm

Availability Bypass: Denial-of-Service attacks (DOS)

- Bring Amazon down
- Prevent Home Front Command from sending alerts
- Shutdown sea port

Examples of what happens if a security principle is not upheld:

- **Availability:** Ensuring that information and resources are available to authorized users when needed.

Secure From Scratch

Confidentiality
Integrity
Availability
Non-repudiation

When Security Principles Break…

We can *bypass* the security.

Exploit – bypassing security principles to make money/cause harm

Non-repudiation Bypass: Hide or fake activity

- Avoid capture
- Delay remediation

Examples of what happens if a security principle is not upheld:

- **Non-repudiation:** Ensuring that actions and transactions can be tracked to prevent denial of action.

Secure From Scratch

Damage from Security Breaches ==> Cost

Financial losses

Reputational damage

Legal consequences

Injury/Death

…

Secure From Scratch

IBM Report: Avg. Cost of Security Breaches 2024

- Average breach cost: $4.9 million
  - $150 per compromised record
- Impact of involving law enforcement: -$1 million in costs
- Average time to identify: 204 days
- Average containment period: 73 days
- Customer PII involvement: 46% of breaches
  - PII – Personally Identifiable Information

https://acsense.com/blog/ibm-2024-cost-of-data-breach-report/

Secure From Scratch

Cost of Security Breach - MOVEit

- 2023
- Product: *Secure* File Transfer
- $9,923,771,385
- 1000 organizations
- 60,144,069 individuals
- Root cause is SQL injection.
- Compromised Confidentiality

MOVEit has a group of products that offer secure and compliant ways to transfer sensitive data between partners, customers, users, and systems
. On may 2023 the vulnerability was disclosed by security firm and already exploited in the wild.
The mass-exploitation of MOVEit Transfer software has rapidly cemented itself as the largest hack of the year so far.
While the full impact of the attack will likely remain untold for months to come, there are now more than 1,000 known victims of the MOVEit breach, according to cybersecurity company Emsisoft.
This milestone makes the MOVEit breach not just the largest hack of 2023 — but also one of the largest in recent history.
The root cause of MOVEit mass-exploitation is sql injection.

Secure From Scratch

Cost of Security Breach - MGM

- 2023
- Product: Hotels & *Casino chain*
- $100,000,000
- Ransomware
- Compromised Availability

https://edition.cnn.com/2023/10/05/business/mgm-100-million-hit-data-breach/index.html

Secure From Scratch

Cost of Security Breach - Shirbit

- 2020
- Product: Insurance policies
- ₪1,200,000,000 in law suits
- Q4 ₪8,000,000 loss
  - Yearly profit down ₪79,000,000
- Potential sell price down ₪30-40,000,000
  - 60-70,000,000 instead of 100,000,000
- Now owned by Harel Insurance
- Compromised Confidentiality

https://www.calcalist.co.il/markets/articles/0,7340,L-3903028,00.html

Secure From Scratch

Cost of Security Breach – National Public Data

- Aug. 2024 (but started Dec. 2023)
- Product: Employee Background Checks
- 2,900,000,000 records
  - name, current and past addresses, birth date, phone number
- 272,000,000 Social security numbers exposed
- 17 lawsuits
- Filed for bankruptcy
- Compromised Confidentiality

Secure From Scratch

Equifax Data Breach

Equifax:

A Credit Bureau company

…. providing information on individuals' borrowing and bill-paying habits

WIKIPEDIA

Secure From Scratch

Equifax Data Breach

Compromised data: private records of 147.9 million Americans along with 15.2 million British citizens and …

Undetected for 76 days.

WIKIPEDIA

Secure From Scratch

Equifax Data Breach

Equifax shares dropped 13% in early trading the day after

Sep. 7th 2017 close: 142.72

Sep. 8th 2017 open: 121.82

Sep. 19th 2017 open: 92.5

----------> Jul. 29th 2019 close: 142.72

yahoo!finance WIKIPEDIA

It took almost 2 years for Equifax's stock price to return to its previous value.

Secure From Scratch

Equifax Data Breach

On July 22, 2019, Equifax agreed to a settlement:

- $300 million to a fund for victim compensation,
- $175 million to the states and territories in the agreement,
- $100 million to the CFPB in fines

WIKIPEDIA

Secure From Scratch

Viasat Outage

Internet broadband satellite

24/2/2022 – on Russia's invasion of Ukraine

Attack on the modems

WIKIPEDIA

Secure From Scratch

Viasat Outage - Method

Entered company intranet via poorly configured VPN

Issue flash overwrite command to all modems

➔ Wipe modem configuration

➔ No configuration – no satellite connection

WIKIPEDIA

Secure From Scratch

Viasat Outage – Impact

Internet outage in Ukraine and Europe

- European internet provider - ~13000 subscribes
- France – 9000 subscribes
- Ukraine – several thousands

5800 Wind Turbines (loss of remote control)

Time to fix – upto 2 weeks

WIKIPEDIA