ALL TOGETHER

Securing Your Data

Chris Sealey, Data and Analytics Department

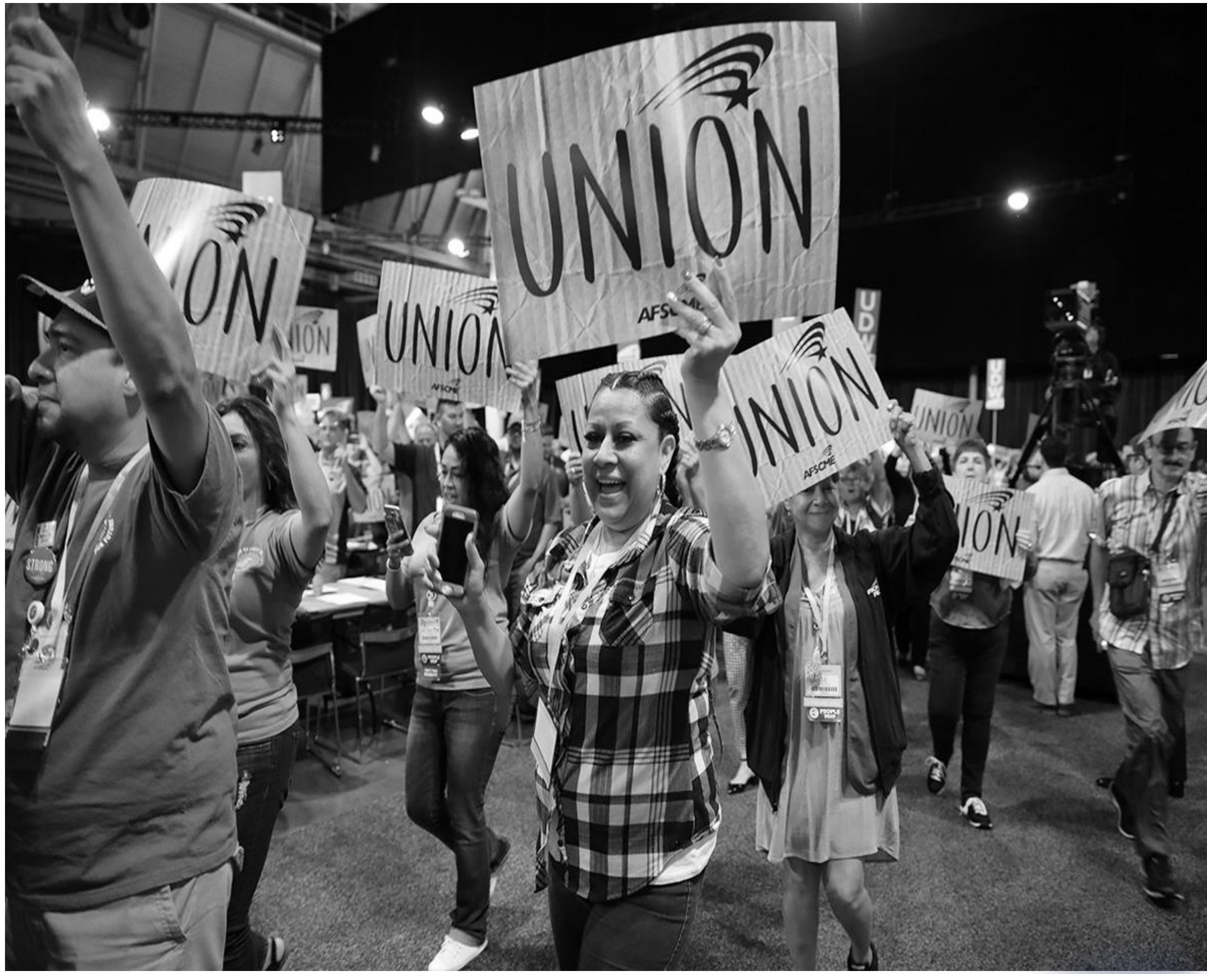
Securing Your Data

The business value of data has never been greater than it is today.

- What is data security
- Why is data security important
- Steps to secure your data

What is data security?

- Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.



Why is data security important/

Costs, Fines, and Reparations

In 2021, the combined cost of global data breaches reached $6 trillion annually.

Reputational Damage / Trust

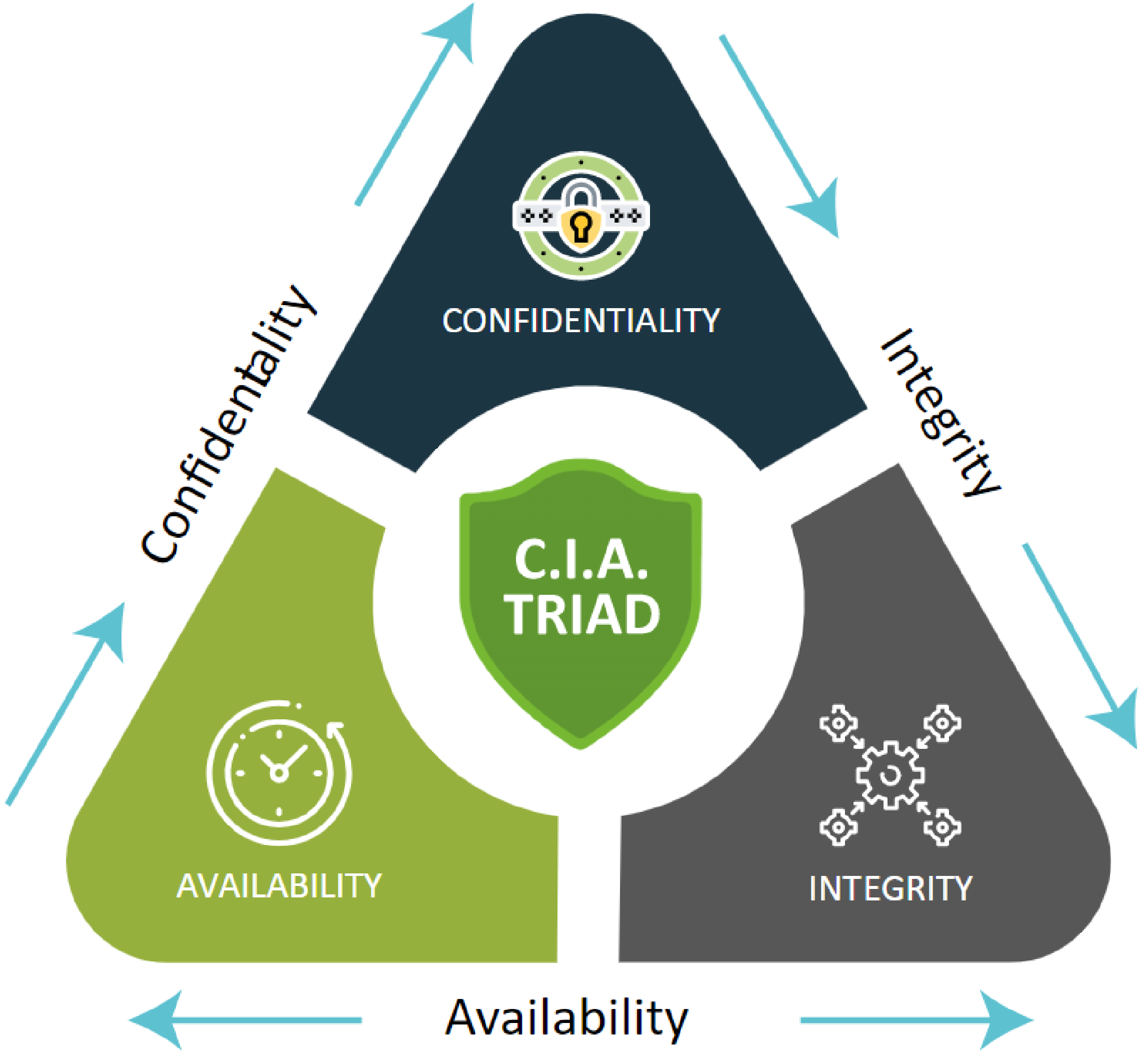
The Equifax data breach in 2017 was $87.5 million. Almost two years after the breach, the company was still suffering the negative after-effects of their data mistakes.

Job Losses

In high-profile cases, top-level executives at Target, Yahoo and Equifax have paid for security breaches with their jobs.

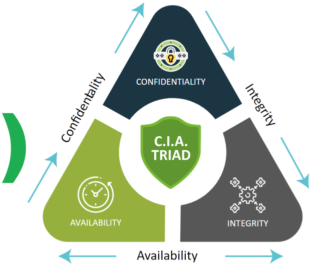
ALL TOGETHER

Steps to Secure Your Data



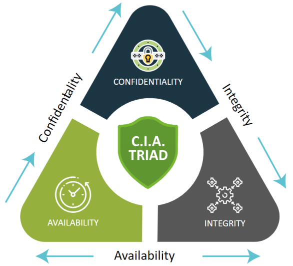
ALL TOGETHER

Confidentiality (Steps to Secure Your Data)



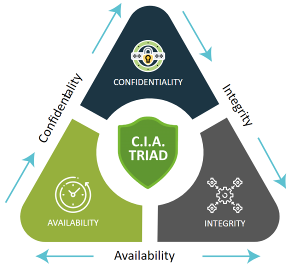
1) Protect sensitive, private information from unauthorized access.
2) Segregate data based on the criticality of the information and set parameters to limit who can access certain types of information.
3) Consider implementing **R**ole-**b**ased **A**ccess **C**ontrol (**RBAC**).

Integrity (Steps to Secure Your Data)



1) Ensure the data is correct, authentic, and reliable.
2) Data must be protected while it is in use, in transit, and when it is stored.
3) Consider the use of encryption, hashing, digital signature, digital certificate, intrusion detection systems, auditing, version control, authentication, and access controls.

Availability (Steps to Secure Your Data)



Ensure that critical systems, applications, and data are available and accessible to authorized users when they need them

When CIA Fails

1) **Disclosure** – Unauthorized entity gets access to your information.
2) **Alteration** – Data is unexpectedly modified or changed.
3) **Destruction** – Data systems or applications are destroyed or rendered inaccessible (for ex. ransomware attacks).

What You Can D0

1. Protect data at your workspace.

2. Dispose of data properly.

3. Be aware of phishing schemes.

4. Educate your peers/employees.

What You Can Do...

5. Encrypt sensitive data

6. Protect all portable devices and beware of public wi-fi

7. Verify before providing any info.