

IT Security Objectives by the example of Fun & Fitness, Inc.

Group 33 (Haddad et al.)

Introduction to the team

Haifa Haddad
MSc. Information Systems

Kevin Wamba
MSc.
Management
& Technology

Bahadur Ali
MSc.
Management
& Technology



Sebastian Zett
MSc.
Management &
Technology

Florence Koster
MSc.
Management &
Technology

Agenda for today's case study

1. Refresh lecture concepts
2. Give context about Fun & Fitness Inc.
3. Explain IT security objectives of the company & understand how the objectives would be violated
4. Give methods for ensuring Fun & Fitness security objectives



1. Refreshing lecture concepts

Refreshing lecture concepts

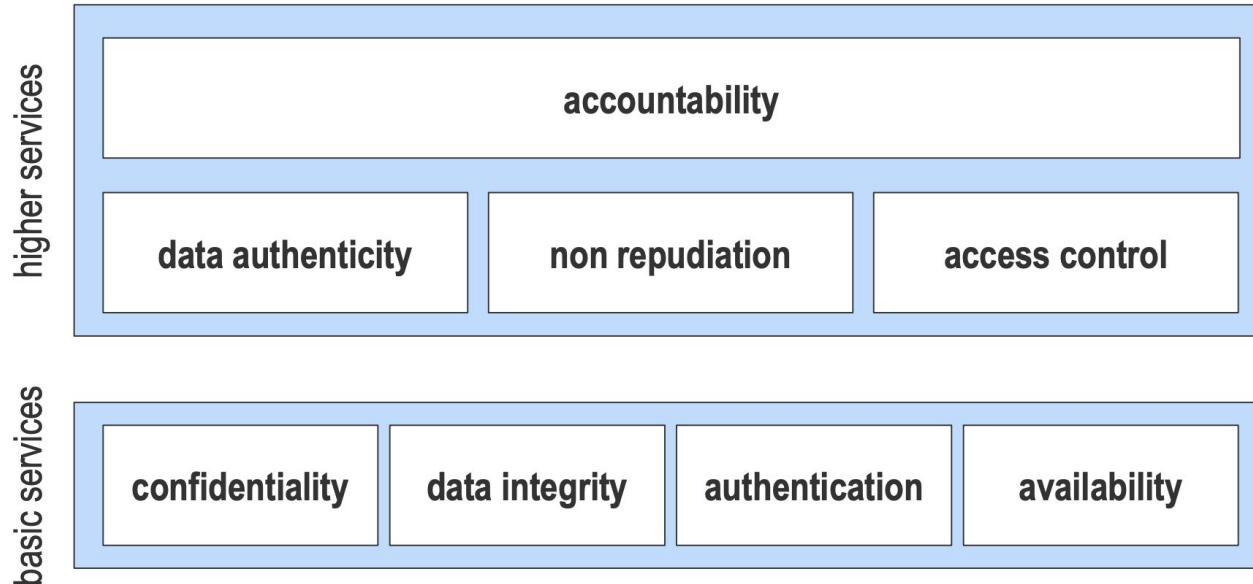
- **Security** = absence of unbearable risks
- **Risk** = probability of adverse future event multiplied by its magnitude
- **Information security** = practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Shared networks, distributed services (cloud computing) means organizations are even more vulnerable.

Security objective = goal you wish to achieve with respect to securing an information system.

Refreshing lecture concepts

IT Security Objectives



2. Context about Fun & Fitness Inc.

Fun & Fitness Inc.

- Fun & Fitness is a gym that offers **instructor-led classes**.
- Attendants of the classes may be **members** or **non-members**.
- Gym wants to optimize potential **revenues**: pay when registering for a class.
- Online payment done with a **credit card**.
- Verification and handling of transactions is done by an **external system**.



3. IT security objectives of Fun & Fitness

Deriving IT security examples along objectives

	Confidentiality	Integrity	Authentication	Availability
Credit card information				
Marketing promotion				
Exercise fitness class schedule				
Financial transaction				
Customer e-mail list				

Deriving IT security examples along objectives

	Confidentiality	Integrity	Authentication	Availability
Credit card information	Identity theft fraud discrimination loss of business	Changed credit card information	Credit card stolen	Internet connection failure inhibits check for correctness
Marketing promotion	Unreleased promotion can affect competitive advantage	(Unethical) competitor damaging promotion assets	Competitor hacks into marketing account	Loss of work effort when promotional campaign is unavailable
Exercise fitness class schedule	Personal schedule exposed	Schedule made unavailable	Unauthorized user accesses exercise classes	Server outage makes schedule unavailable for customers
Financial transaction	Personal information revealed	Falsify reported revenue	Password hacked	Unavailable log of financial transactions
Customer e-mail list	Unwanted spam e-mails	Competitor deleting customer list	Access to e-mail addresses breached	Unavailability prohibits sending marketing offers

Confidentiality: Credit card information

- Fun and Fitness must comply to the with **PCI DSS** that is associated with the goal to protect Cardholder data while stored or in transit.
- The confidentiality can be violated when the organization experiences a **data breach** involving personally identifiable information.
- In case the confidentiality of the cardholder data is violated, information restricted to only authorized people will be made available to to unauthorized people (**identity theft**).

Data integrity: Marketing Promotions



Completeness

Accuracy

Consistency

Authentication: Exercise Fitness Class Schedule

- Specialized exercise classes.
- Authentication ensures only **eligible members** can sign up for certain classes.

Without authentication:

- Non-eligible members can attend classes.
- May lead to insecurity of other attendants.






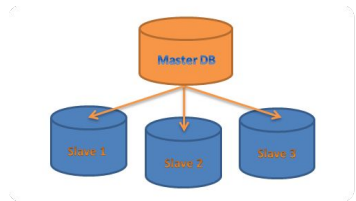
Availability: Financial transaction information

- Financial transaction data contains **personal information** about involved parties and payment flow
- It must be available permanently
- Availability can be violated by **server breakdowns**, **internet connection outages** or **power loss**
- In case data is not available:
 - Fun & Fitness can't document its payment flow for monthly business reports or audits
 - Customers cannot proof their payment
→ are charged twice / can't attend booked class



4. How to ensure Fun & Fitness Inc. security objectives

Fulfilling Fun & Fitness security objectives

Confidentiality	Integrity	Authentication	Availability
<p>Encryption (preferably asymmetric) for protecting data in transit → envelope encryption where master key is encrypted & safely stored</p> <p>Encryption & Decryption</p>  <p>The diagram shows a flow from a document icon labeled 'Plaintext' to a key icon labeled 'Encryption', then to a document icon with binary code and a lock labeled 'Ciphertext', then to a key icon labeled 'Decryption', and finally to another document icon labeled 'Plaintext'.</p>	<p>Hashing to verify that data hasn't been altered (i.e. authentic)</p> <p>Hashing</p>  <p>The diagram shows a flow from a document icon labeled 'Plaintext' to a box labeled '#SHA-2' (representing the Hash Function), and then to a document icon labeled 'Hashed text'.</p>	<p>All system users (e.g. members) have to authenticate using password.</p>  <p>The diagram shows a circular flow involving a user icon, a fingerprint icon, a server icon, and a checkmark icon, representing the authentication process.</p>	<p>Replication of the log of financial transactions</p> <p>Ensure consistency of the replicas upon writes</p>  <p>The diagram shows a central 'Master DB' icon with arrows pointing to three 'Slave 1', 'Slave 2', and 'Slave 3' icons, representing database replication.</p>

Thank You!

Suggested questions to guide the discussion

- To which basic security objective would you assign Fair Information Practices?
- Which objectives do you consider most important in the available case?
- How are higher services based on basic IT security objectives?