



UNIVERSITY  
OF TRENTO - Italy




**Cyber Security Risk Assessment**  
**Spring 2018**

*Lecture 02 – Terminology*  
*Fabio Massacci*

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 1




UNIVERSITY  
OF TRENTO - Italy




**What is a...**

- **Asset**
  - Something of value for your stakeholders
- **Threat**
  - circumstance, capability, event, action that could breach security and cause harm to an asset
- **Threat Agent**
  - the entity carrying out a threat
- **Vulnerability**
  - A flaw or weakness in a system's design, implementation, operation, management that could be exploited by a threat
- **Risk**
  - An expectation of loss expressed as the probability that a threat occurs and the harmful result

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 2




UNIVERSITY  
OF TRENTO - Italy




## What is an asset?

- **Primary asset**
  - Intangible function, service, process or information
  - Part of the system within the scope of the project
  - Valuable to the stakeholders
- **Supporting (or tangible) assets**
  - “Actual” entities which enable the primary assets.
  - Typically supporting assets possess the vulnerabilities that are exploitable by threats aiming to impair primary assets

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 3



UNIVERSITY  
OF TRENTO - Italy



## What's a supporting “tangible” asset?

- **Hardware**
  - computer systems, data storage, data communication devices
- **Software**
  - operating systems, system utilities, applications, services
- **Data**
  - files and databases
- **Communication Lines**
  - local and wide area network communication links, router, gateways an so on
- **They are “supporting” asset → they have very limited value by themselves**

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 4




UNIVERSITY  
OF TRENTO - Italy




## Why this distinction?

- ***What is really of value***
  - Information and Values
  - Business Processes
  - Company Reputation
- ***In most cases the “tangible” assets by themselves are not really what you care about***
  - Customer List of 10M Records → priceless
  - DBMS managing the DB → buy & install new for 20K
  - 1TB Hard disk storing DBMS files → buy new for 2K

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 5



UNIVERSITY  
OF TRENTO - Italy



## Historic Threats to Tangible Assets

- ***Hardware***
  - Desktop computer stolen at Sutter Physicians Services and Sutter Medical Foundation, which contained about 3.3 million patients' medical details stored in unencrypted format in 2011
- ***Software***
  - Phishing attack to PayPal stealing customers' credit card details in 2006
- ***Data***
  - Data breaches (passwords), stemming from attacks that compromised Sony PlayStation Network, Sony Pictures in 2011, Target, OPM etc. etc.
- ***Communication Lines***
  - Kevin Poulsen was a teenage telephone hacker who hacked the phone lines to win a Porsche in a radio contest in 1990


21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 6

UNIVERSITY OF TRENTO - Italy 

## Intangibles are What Really Matter


- **Personal Information protected by law**
  - Sutter Physicians Services 3.3 million patients' medical details
- **Payment Information usable for frauds**
  - PayPal customers' credit card
  - Target customers' credit card
- **Governmental Information**
  - OPM Information of US federal employees
- **Reputation with business values**
  - Sony Pictures executives' confidential opinions and strategies
- **Fairness of Contests**
  - Radio contest
- **Remember we only worry on the intangible!**
  - Desktop computer was worth few Ks

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 7


UNIVERSITY OF TRENTO - Italy 

Unintentional Threats	Intentional Threats
<b>Environmental:</b> <ul style="list-style-type: none"> <li>▪ Fire, wind</li> <li>▪ Lighting, flooding</li> <li>▪ Accident</li> <li>▪ Equipment failures</li> </ul>	<b>Individuals or Organizations:</b> <ul style="list-style-type: none"> <li>▪ Hackers</li> <li>▪ Criminals</li> <li>▪ Disgruntled employees</li> </ul>
<b>Human:</b> <ul style="list-style-type: none"> <li>▪ Keystroke errors</li> <li>▪ Procedural errors</li> <li>▪ Programming bugs</li> </ul>	

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 8




UNIVERSITY  
OF TRENTO - Italy




## Intentional Threat Types

- **Active Attacks**
  - Aim to modify system's assets or to affect their operation
  - Preventing them is harder than detecting them
  - e.g reply attack, SQL injection
- **Passive Attacks**
  - Aim to learn or make use of information that not affect the system's assets
  - Detecting them is harder than preventing them
  - e.g traffic analysis

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 9



UNIVERSITY  
OF TRENTO - Italy



## Threat Agents

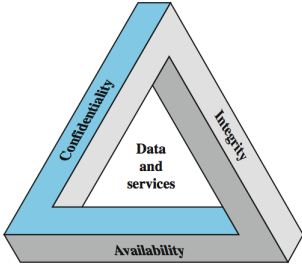
- **Insider Attacks**
  - The threat agent is a legitimated user of the system who oversteps his/her authorization
  - Frequent vector for large companies
- **Outsider Attacks**
  - The threat agent is an unauthorized user of the system or illegitimate user to the system
- **Both can be prevented and detected up to a certain level**

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 10

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## Threats Impact Security Properties

- **Confidentiality**
  - preventing unauthorized disclosure of information
- **Integrity**
  - preventing unauthorized modification of information
- **Availability**
  - preventing of unauthorized withholding of information or resources




21/02/18
Fabio Massacci - Cyber Security Risk Assessment
► 11

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


## Tangible Assets & Threats Impact on Security Properties

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled	Hardware trojan sends data out	EM field changes data
Software	Programs are deleted	Unauthorized copy of the software	Working program is modified
Data	Files are deleted	Unauthorized read of data	Existing files are modified or new files are fabricated
Communication Lines	Messages are deleted, Communication lines make unavailable	Messages are read. The traffic pattern of messages are observed	Messages are modified or fabricated

21/02/18
Fabio Massacci - Cyber Security Risk Assessment
► 12



UNIVERSITY  
OF TRENTO - Italy



## A “Pre-requisite” property

- **Authenticity**
  - property of an entity of being “genuine” and verified
  - origin authenticity, data authenticity
- **Authenticity is a pre-requisite property of all security properties**
  - If you cannot tell who is Fabio Massacci, how can your system ever assure that data is only read by him (confidentiality), only modified by him (integrity) or always accessible to him (availability)?

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 13




UNIVERSITY  
OF TRENTO - Italy




## Illustrating its importance

- **Identity theft in the US (2012)**
  - Population: 314.100.000
  - Identity Theft: 16.600.000
- **Identity theft in Italy (2012)**
  - Population: 59.500.000
  - Identify Theft: 24.000
- **Why so few Italian IT Thefts?**
  - After all Italy invented the mafia and exported it to the world

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 14




UNIVERSITY OF TRENTO - Italy




## Illustrating its importance... cont

- **Identity theft in the US (2012)**
  - Population: 314.100.000
  - Credit cards: 600.000.000
  - Identity Thefts: 16.600.000
- **Identity theft in Italy (2012)**
  - Population: 59.500.000
  - Credit cards: 61.000.000
  - Identify Thefts: 24.000
- **So there are**
  - 5 USA residents vs 1 Italian resident
  - 10 USA credit cards vs 1 Italian credit card
  - 691 USA ID thefts vs 1 Italian ID theft
- **Why no 10 US ID Thefts vs 1 Italian fraud or even more?**
  - What are these Italian mafia guy doing? Lagging behind?

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 15



UNIVERSITY OF TRENTO - Italy




## The BIG US mistake: Auth vs Ident

- **Identification (Oxford dictionary)**
  - “The action or process of identifying someone or something or the fact of being identified.”
- **Authentication (ibidem)**
  - “The process or action of proving or showing something to be true, genuine, or valid”
- **Can you discover my social security number?**
  - Very easy
- **What can you do with it?**
  - Very little
- **Why?**
  - It is just an unique identifier, not a unique authenticator.


VALUTAZIONE COMPARATIVA PUBBLICA PER N  
[web.poliba.it/.../k05a10...](http://web.poliba.it/.../k05a10...) ▼ Translate this page Polytechnic University of Bari ▼  
 Mar 20, 2000 - Massacci Fabio. 12. Milano Michela. 13. ... Massacci Fabio. 10. Milano Michela ... Massacci Fabio nato a Cagliari il 19/6/1967; Milano Michela ...

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 16






UNIVERSITY  
OF TRENTO - Italy




## The CIA Triad: Confidentiality

- **Data Confidentiality**
  - protecting private and sensitive data from access and disclosure by unauthorized individuals
- **Unlinkability**
  - Two items of interest are unlinkable if an attacker can't determine that they are related to each other
- **Anonymity**
  - A subject (a user) is anonymous if an attacker cannot be distinguish him/her in the anonymity set of subjects

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 17




UNIVERSITY  
OF TRENTO - Italy




## The CIA Triad: Integrity

- **Data Integrity:**
  - data are not modified by unauthorized individuals
- **System Integrity:**
  - system performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 18




UNIVERSITY  
OF TRENTO - Italy




## The CIA Triad: Availability

- **Availability**
  - ensuring that a resource is accessible and usable by an authorized entity
  - It concerns intentional failures caused by a human
- **Reliability**
  - It concerns accidental software, hardware, communication failures

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 19



UNIVERSITY  
OF TRENTO - Italy



## Other Properties

- **Accountability**
  - the property of tracing security related actions/events to the responsible entity
- **Non-repudiation**
  - the property of having unforgeable evidence that an event/action has occurred
  - non-repudiation of origin, non repudiation of delivery
- **“Privacy” (Often grouped with confidentiality)**
  - the right of an individual to control what data are collected and stored by who and to whom are disclosed

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 20

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## What can you do without...

	Confidentiality	Integrity	Availability	Accountability	Non-repudiation	Privacy
No Confidentiality		15 No- Yes 0	Yes	Yes	Yes	No
No Integrity	If auth is compromise No, Depends		Depends	No	No	Depends
No Availability	Yes	Yes		Yes (NO as well see NR)	Yes No if the NR service is the one to fail	Yes


21/02/18 Fabio Massacci - Cyber Security Risk Assessment 21

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


## What can you do without... (2015, 2016)

	Confidentiality	Integrity	Availability	Accountability	Non-repudiation	Privacy
No Confidentiality		10/10	15/8	6/7	6/4	Not really
No Integrity	12		Kind Yes/ No	?/No	No/No	Kind not/ no
No Availability	Yes	Yes		Kind of	Same	

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 22




UNIVERSITY OF TRENTO - Italy




## Unwanted Consequences

- **Unauthorized disclosure**
  - Exposure, Interception, Inference, Intrusion
- **Deception**
  - Masquerade, Falsification, Repudiation
- **Disruption**
  - Incapacitation, Corruption, Obstruction
- **Usurpation**
  - Misappropriation, Misuse

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 23




UNIVERSITY OF TRENTO - Italy



## Which incident does affect...


	Unauthorized disclosure	Deception	Disruption	Usurpation
Confidentiality	Yes	Possibly if impersonation	Not really	Yes
Integrity	No	Yes	Yes	Yes
Availability	No	If limit on services	All the times	If able to shutdown

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 24

UNIVERSITY OF TRENTO -  **Which incident does affect... (2015, 2016)**

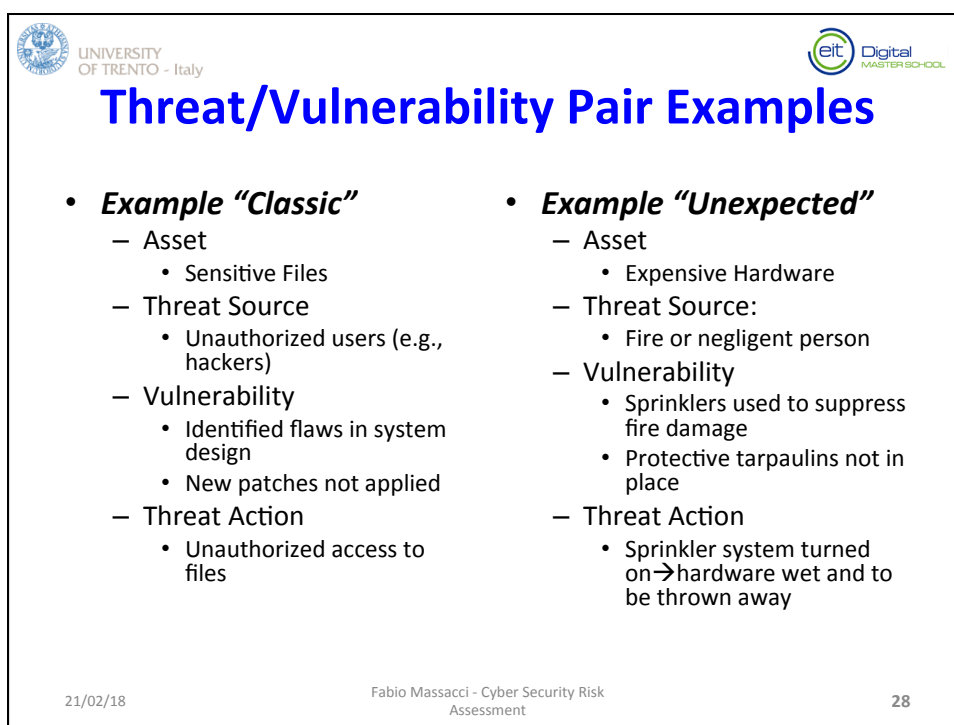
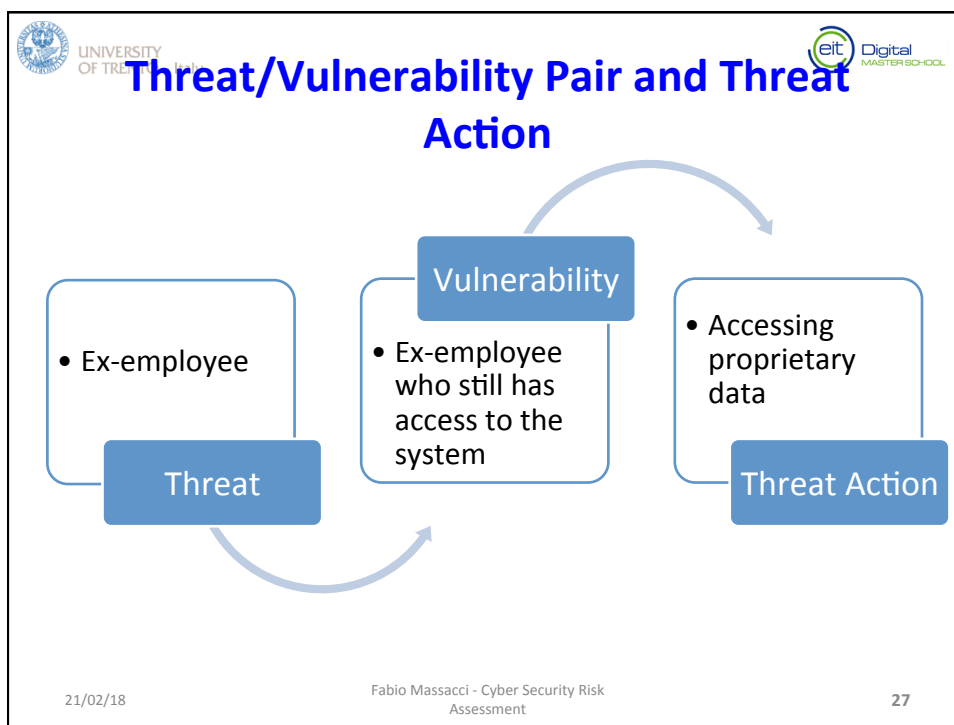
	Unauthorized disclosure	Deception	Disruption	Usurpation
Confidentiality	No/yes	No/No but can lead to a later compromise	Yes/No	kind of/yes
Integrity	Yes/No	No/yes	Yes/Yes if data is compromised	Not really/yes
Availability	No	Kind of/No but can lead to a later compromise	Yes	No/Maybe depends on context of implementation

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 25

UNIVERSITY OF TRENTO - Italy  **Threat/Vulnerability Pair**

- **Unwanted Incidents**
  - Occurs when a threat exploits a vulnerability
- **A vulnerability provides a path for the threat that results in a harmful event or a loss**
  - Both the threat and the vulnerability must come together to result in a loss
- **Vulnerabilities are easier to manage than threats**
  - Threats can't be entirely eliminated → are always present.
  - Can (try to) reduce the potential for a threat to occur.
  - Can (try to) reduce the impact of a threat → prevent the vulnerability or control the effects of the exploitation

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 26



UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

## What is a security control?

- ***an action, device, a procedure or technique that ...***
- ***reduces a threat, a vulnerability, or an attack by ....***
- ***eliminating it,***
- ***minimizing the harm it causes, or***
- ***discovering and reporting it so that corrective action can be taken***


21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 29

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


## What Can Controls Do?

- ***Countermeasures reduce risk and loss***
  - Reduce Threats
  - Reduce vulnerabilities
  - Reduce impact of loss

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 30




UNIVERSITY  
OF TRENTO - Italy




## When they can be applied?

- **Preventive**
  - Measures that prevent your assets to be affected
- **Detective**
  - Measures that allow to detect when an assets has been affected, how it has been affected, and by who
- **Reactive**
  - Measures that allow to recover your assets or (partially) restore operation from damage to your assets

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 31



UNIVERSITY  
OF TRENTO - Italy




## Which control does protect...


	Preventive	Detective	Reactive
Confidentiality			
Integrity			
Availability			

21/02/18 Fabio Massacci - Cyber Security Risk Assessment 32






UNIVERSITY OF TRENTO - Italy




## Types of Security Controls

- **Management Controls**
  - Awareness and Training
  - Security policy and practices
  - Audit and Accountability
  - Risk-assessment
  - Contingency Planning
- **Technical Controls**
  - Identification and authentication
  - Access and authorization
  - Encryption
  - Digital Signature
  - Privacy-enhancing technologies

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 34



UNIVERSITY OF TRENTO - Italy




## Where security controls should be placed?


- **You need to find**
  - right layer for each security control
  - right security control for each layer
- **Usually three levels**
  - Users
  - Applications
  - Infrastructure

Applications
Services
Operating System
OS Kernel
Hardware

21/02/18 Fabio Massacci - Cyber Security Risk Assessment ▶ 35



UNIVERSITY  
OF TRENTO - Italy



## Additional Readings

- **Textbook** –
  - Chapter 1, Chapter 2
- **Additional Readings**
  - Chapter 1, Ross Anderson. Security Engineering
  - Chapter 2, Dieter Gollmann. Computer Security
- **Insight**
  - D. Sterne: On the Buzzword 'Security Policy', IEEE Symposium on Research in Security and Privacy 1991
  - K. Thomson. Reflection on trusting trust. Turing Award Lecture.
- **Fact finding**
  - Reports on ID Theft in the US and Italy

21/02/18 Fabio Massacci - Security Engineering 36