



UNIVERSITY
OF TRENTO - Italy




**Cyber Security Risk Assessment
Spring 2018**


*Lecture 01 – Introduction to the course
Prof. Fabio Massacci*

*[https://securitylab.disi.unitn.it/doku.php?
id=security_engineering](https://securitylab.disi.unitn.it/doku.php?id=security_engineering)*

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




UNIVERSITY
OF TRENTO - Italy




The “Usual” Course

- ***The usual lectures/labs***
 - Prof. does theory + Assistant does exercises
 - Prof. does technique + Assistant does programs
 - Prof+Assist = Oracles resolving all doubts
- ***The usual exam***
 - Prof gives well defined problem,
 - Students mirroring exercises/code solutions
- ***The usual project***
 - Developing a project (i.e. code)
 - Prof. knows exactly requirements
- ***This course is not a “Usual” course***

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




UNIVERSITY OF TRENTO - Italy




Why I don't want to teach a "usual" course

- **Reality is very different from the usual course**
 - Problem is not well defined
 - Already a big step if customers realize they have a problem
 - Customers don't know the solution
 - Otherwise they won't be paying you in the first place
 - Decision must be justified and understood by them
 - They won't pay just because you found a solution in a book
 - They don't read code. They pay you for that.
 - Security gets in the way of the business
 - Except when there is an incident → your successor will get attention
- **The course's idea**
 - Teach you cyber security risk assessment with a process as close as possible to real life including presenting and justifying your choices

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




UNIVERSITY OF TRENTO - Italy




Why you don't want me to teach a "usual" course

- **If you can only write programs → you're done for**
 - You must also be able to make decisions and communicate them to upper management
- **Italian Industry Assoc. ICT Salary (24-30 yrs old)**
 - Web Developer/ IT/Network Admin. – 21-26K€
 - Programmer/Analyst – 29-41K€
 - Sys Engineer/Architect – 31-44K€
 - Sw Project Leader/IS Manager – 47-78K€
 - CIO – 98K€/year
- **So, write a management report explaining why you do what you do → at least once**

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




UNIVERSITY
OF TRENTO - Italy




Course principles

- **Objective:**
 - Learn how to assess the risks in a real life problem from high-level controls down to security architecture
- **Methodology**
 - Lecturers present methodology in class
 - Students apply it on various industrial case studies
- **What do you have to prepare**
 - Presentations justify the solution to the customers
 - And they are never happy (but you get early feedback)
 - Deliverable is an executive report to justify your choices
 - You submit it into installments as in real life (here to get feedback)
 - Only at the end you get the money
- **This year “final” customer**
 - UTC - United Technologies: Large Multi-national, research center in Trento and a larger one in Rome (from building sensors to aircraft jets)

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



UNIVERSITY
OF TRENTO - Italy



Cognitive Levels: why the course is tough

- **Knowledge**
 - Recall things by memory (eg repeat a proof from a book)
- **Comprehension ← Most theory course stops here**
 - Justify methods and procedures
- **Application ← Most design courses stops here**
 - Apply concepts and principles to new situations
- **Analysis**
 - Understanding relationships between parts (content & structure)
- **Synthesis ← This course**
 - Ability to put parts together to form a new whole
- **Evaluation ← The best should arrive here**
 - Conscious ability to judge the value of material

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

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Pre-requisites

- ***You must have successfully attended***
- ***Either last semester or in your bachelor***
 - Introduction to Computer and Network Security or
 - Cryptography and
 - Security Testing
 - Attending Network Security in parallel might be an asset
- ***This was not specified in the past, now it is!***

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

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

What Students Think

- ***Pre-prequisite?***


– ++No	0	0	8
– +No, -Yes	8	4	8
– +No, +Yes	12	17	15
– ++Yes	7	20	6
– Score:	70%	90%	97%
– DISI	78%	84%	74%
- ***Material is enough?***

– ++No	1	0	2
– +No, -Yes	8	2	8
– +No, +Yes	13	18	13
– ++Yes	5	21	9
– Score:	67%	95%	66%
– DISI	82%	82%	74%
- ***Effort wrt ECTS?***


– ++No:	2	1	0
– +No, -Yes:	7	5	1
– -No, +Yes:	13	16	22
– ++Yes:	15	19	6
– Score:	67%	85%	97%
– DISI	78%	84%	74%
- ***Satisfied with course?***

– ++No:	2	0	2
– +No, -Yes:	7	3	11
– -No, +Yes:	13	21	12
– ++Yes:	15	17	4
– Score:	52%	93%	55%
– DISI	78%	81%	69%

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




UNIVERSITY OF TRENTO - Italy




What Students Think II

- **Prof is motivating?**
 - ++No 0 0 1
 - +No, -Yes 8 0 7
 - +No, +Yes 12 16 15
 - ++Yes 7 25 6
 - Score: 81% 100%72%
 - DISI 85% 87% 74%
- **Prof is clear?**
 - ++No: 0 0 0
 - +No, -Yes: 3 0 6
 - -No, +Yes: 18 18 15
 - ++Yes: 6 23 6
 - Score: 89% 100%79%
 - DISI 87% 87% 76%

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




UNIVERSITY OF TRENTO - Italy




Make up your grade

- **Step-by-Step Qualitative RA Exercises during the course (up to 16/30)**
 - Industrial Cases:
 - Remote Virtual Control Tower (RTV)
 - Building Automation by UTC (UTC)
 - Identify Assets, Threats, Pre and Post Controls
 - Being able to defend your ideas in class is an important part of the evaluation
 - if you cannot explain why you chose something you get a negative vote
- **Assess Vulnerabilities Exercise (Up to 6/30)**
 - CVSS (Common Vulnerabilities Scoring System), world standard
 - Identify risk from description “as they arrive” in a CERT Bulletin
 - Identify risk as they “apply to you” on your security architecture
- **Final Project (Up to 12/30)**
 - Draft a complete detailed, quantitative, risk assessment of the industrial automation case study security architecture
 - Evaluation by Industry experts of UTC

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




UNIVERSITY
OF TRENTO - Italy




Planned Discussions in Class

- **March**
 - 3 (Assets RVT),
 - 10 (Threats RVT),
 - 17 (PreControls RVT)
- **April**
 - 7 (PostControls RVT),
 - 14 (CVSS Exercise),
 - 21 (CVSS Environmental),
 - 28 (Assets UTC)
- **May**
 - 5 (Threats UTC),
 - 12 (PreControls UTC),
 - 19 (Post Controls UTC),
 - 26 (Environmental UTC) <- to be confirmed
 - 28 (Quantitative UTC) <- to be confirmed
 - Depends whether we need NDA or not

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




UNIVERSITY
OF TRENTO - Italy




The 1° “Exercise” Case study

- **The Business Case**
 - At Airports there is control tower to guide airplanes in landing and take-off
 - Personnel is very expensive as needs to have turns, good training, etc. etc.
 - But some airport have very few flights
- **The Solution**
 - Remote and Virtual Control Tower
 - Move everything into a centralized location and replace the “Over the Window” view with fully virtualized centers with sensors etc.
 - Obviously security is kind of a problem...

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




UNIVERSITY
OF TRENTO - Italy




The “On-Going” Methodology

- **SESAR SECARAM**
 - Methodology developed by SESAR Project (Open Sky) specifically to address the case study
- **EuroControl Catalogue**
 - Specifically targetted to provide a first set of threat and corresponding security
 - It is confidential, so you will have to sign a Non-Disclosure Agreement
 - Every student will have his/her own catalogue **on paper and watermarked**
 - **If you don’t return it, you don’t pass the exam**
 - (and I will make sure you don’t graduate either)

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




UNIVERSITY
OF TRENTO - Italy




How to report your work: Report

- 1. Structure of the report**
 1. Target of Evaluation
 2. Threats and Risk Assessment
 3. Pre-Controls
 4. Post-Control
 5. Summary of Recommendations
- 2. Delivery**
 1. In installment during Exercises
 2. In single shot for final report

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




UNIVERSITY OF TRENTO - Italy




Rule of the game

- **On “I took this text from a colleague of mine”**
 - Remember I have been a student myself, thinking “he is not going to find it” is going to disappoint you
- **IF**
 - you are able to have people working for you and you can sell their work as yours as if they didn’t exist → Great, you’re the next Steve Jobs → 30 cum Laude is deserved
- **ELSE**
 - That’s called plagiarism and is forbidden.
 - You will fail the class and that’s it.
- **Statistics is against you on the IF clause**

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



UNIVERSITY OF TRENTO - Italy



Rules of Engagement

- **Asking questions in class is always the best policy**
 - Your colleagues may be interested in the answer
 - Things are easier to explain
 - The prof gets hundreds email per day...
 - Today before 10:30 (... emails and counting)
- **Do your homework first**
 - “I can’t bother to find the answer, I will ask the prof.”
 - Q: “I don’t remember to whom the deliverable should be submitted”
 - A: “read my slides”
- **Write with “[CybRisk]” in the subject**
 - “important” is a no go
 - “urgent” is not better

[A!A] Fw: important

eleonora_lanave <giacomelli@mediavoice.it>
a mediavoice, alicia, sales, mediavoice.it, Andrea, angela, Barbara, Carmela, comunicazioni

Categorizza questo messaggio come: Forum

Hello!

Check it out <http://u20980.netangels.ru/impossible.php>

eleonora_lanave

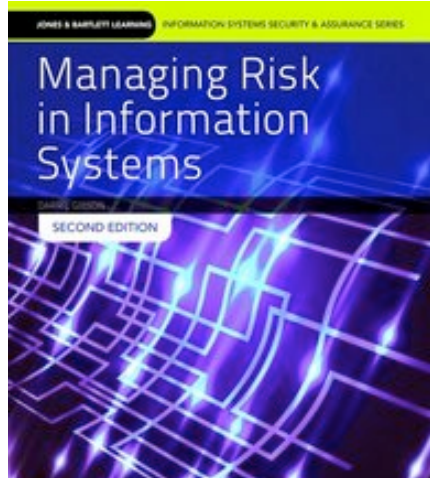
21/02/18 Fabio Massacci - Cyber Security Risk Assessment 16

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Textbook

- Darril Gibson. Managing Risk in Information Systems, 2nd edition.
- <http://www.jblearning.com/catalog/9781284055955/>



21/02/18

Fabio Massacci - Cyber Security Risk Assessment

17

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Reading Materials




ACM DL DIGITAL LIBRARY

Google scholar

Fabio Massacci - Cyber Security Risk Assessment

▶ 18

21/02/18