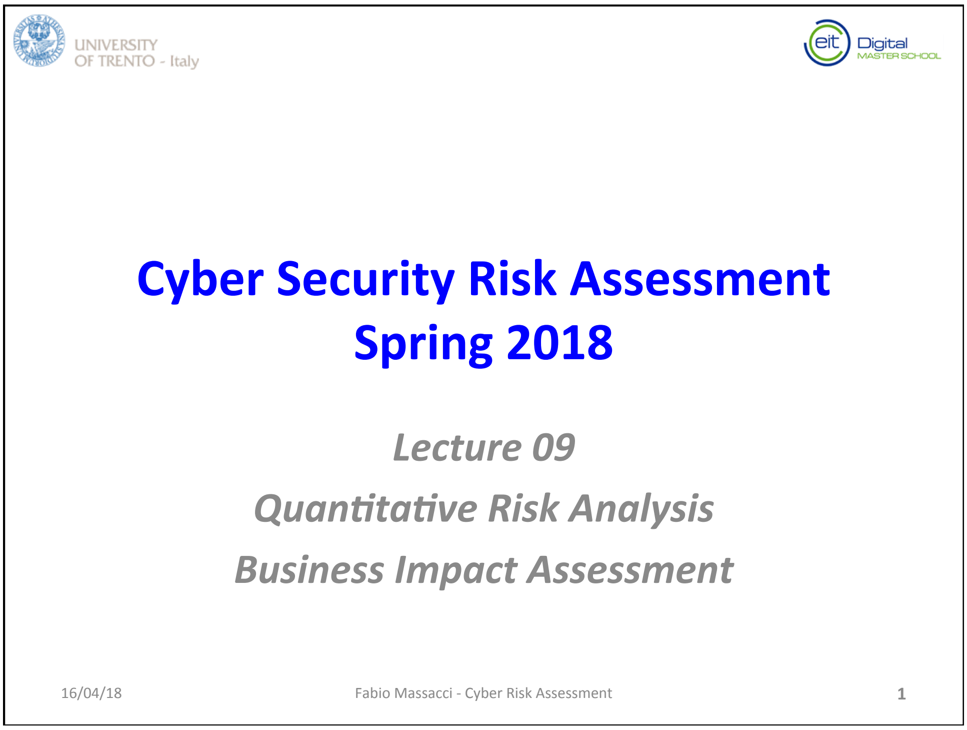
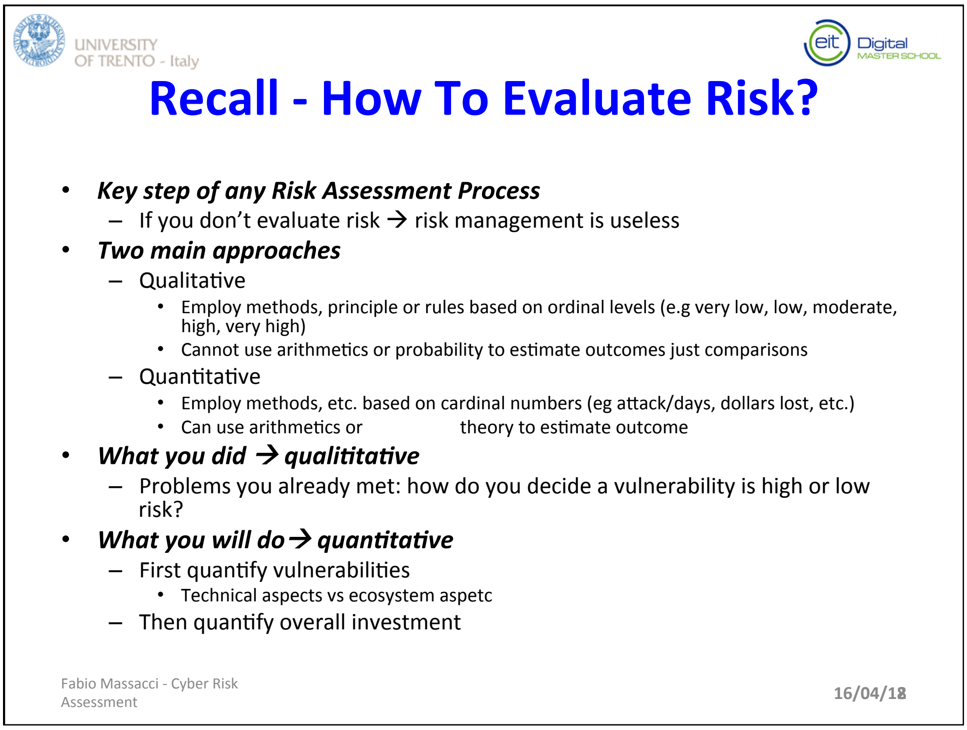


Cyber Security Risk Assessment Spring 2018

Lecture 09

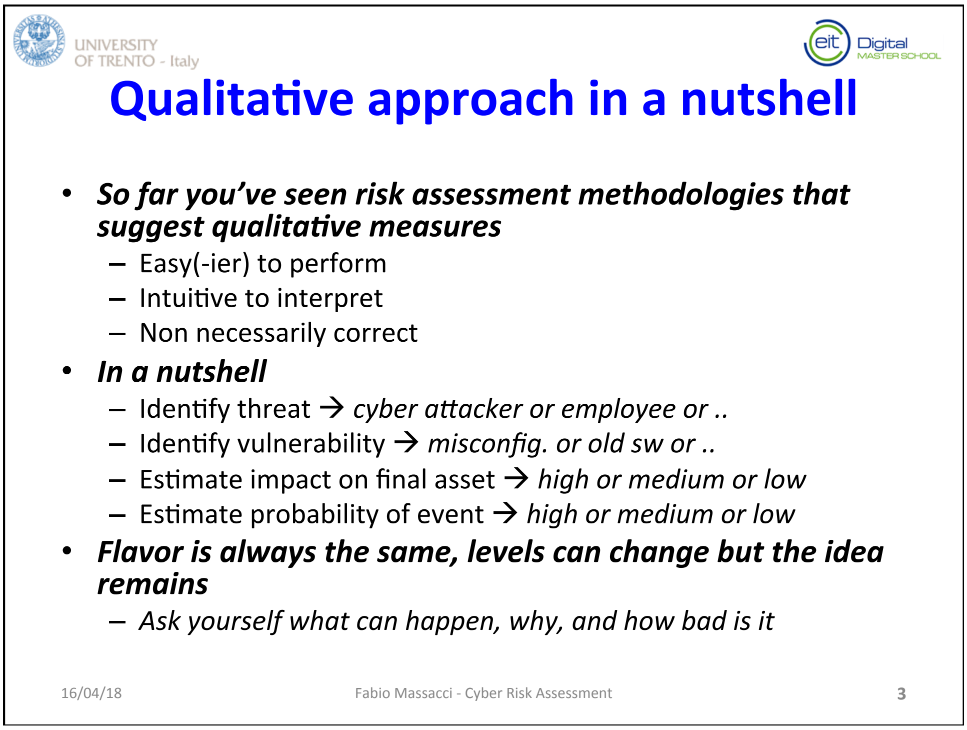
Quantitative Risk Analysis

Business Impact Assessment



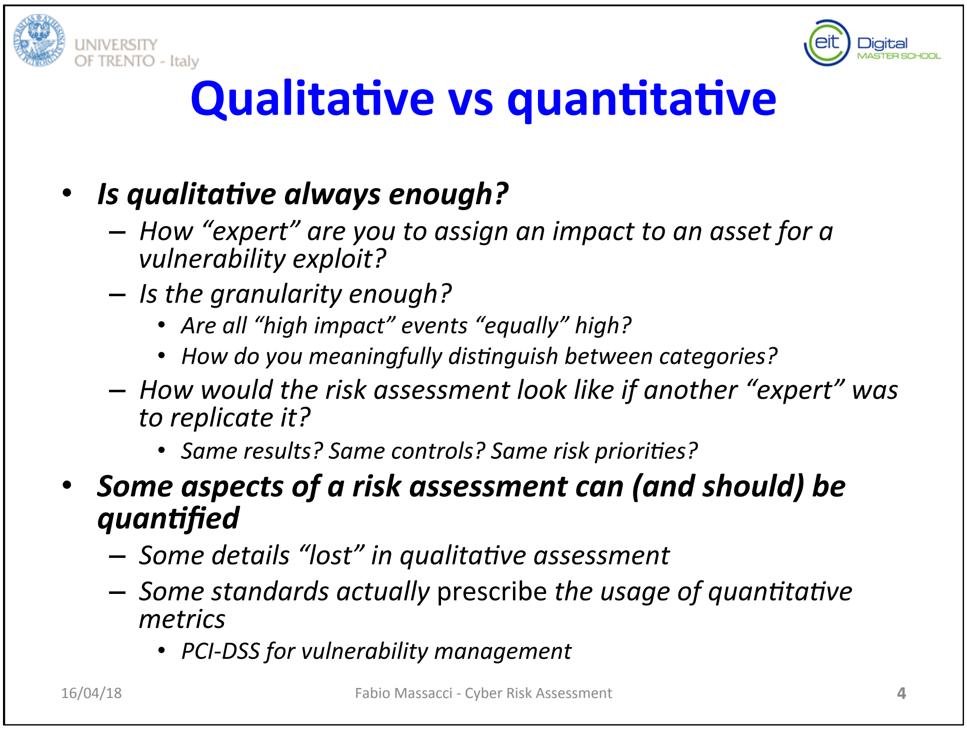
Recall - How To Evaluate Risk?

- ***Key step of any Risk Assessment Process***
  - If you don't evaluate risk → risk management is useless
- ***Two main approaches***
  - Qualitative
    - Employ methods, principle or rules based on ordinal levels (e.g very low, low, moderate, high, very high)
    - Cannot use arithmetics or probability to estimate outcomes just comparisons
  - Quantitative
    - Employ methods, etc. based on cardinal numbers (eg attack/days, dollars lost, etc.)
    - Can use arithmetics or theory to estimate outcome
- ***What you did → qualititative***
  - Problems you already met: how do you decide a vulnerability is high or low risk?
- ***What you will do→ quantitative***
  - First quantify vulnerabilities
    - Technical aspects vs ecosystem aspetc
  - Then quantify overall investment



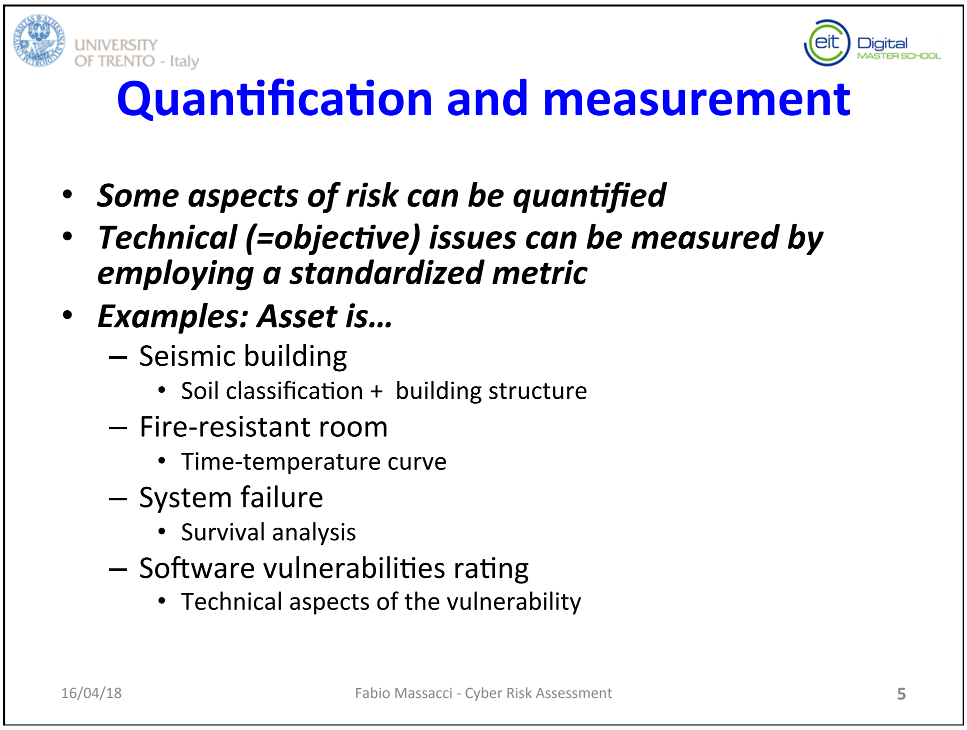
Qualitative approach in a nutshell

- ***So far you've seen risk assessment methodologies that suggest qualitative measures***
  - Easy(-ier) to perform
  - Intuitive to interpret
  - Non necessarily correct
- ***In a nutshell***
  - Identify threat → *cyber attacker or employee or ..*
  - Identify vulnerability → *misconfig. or old sw or ..*
  - Estimate impact on final asset → *high or medium or low*
  - Estimate probability of event → *high or medium or low*
- ***Flavor is always the same, levels can change but the idea remains***
  - *Ask yourself what can happen, why, and how bad is it*



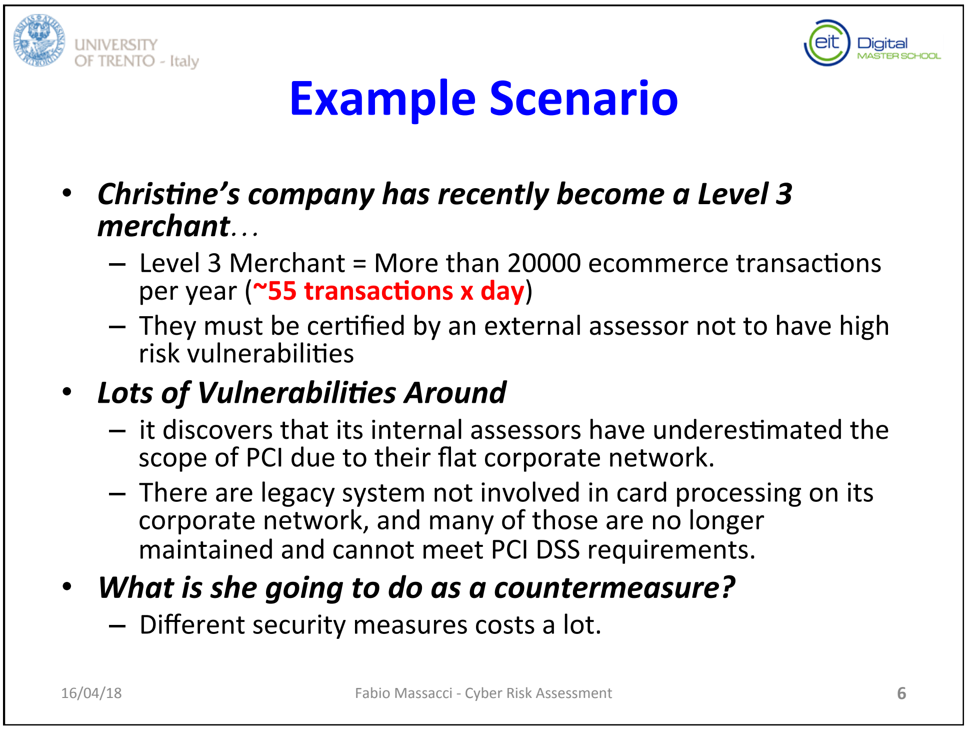
Qualitative vs quantitative

- ***Is qualitative always enough?***
  - *How "expert" are you to assign an impact to an asset for a vulnerability exploit?*
  - *Is the granularity enough?*
    - *Are all "high impact" events "equally" high?*
    - *How do you meaningfully distinguish between categories?*
  - *How would the risk assessment look like if another "expert" was to replicate it?*
    - *Same results? Same controls? Same risk priorities?*
- ***Some aspects of a risk assessment can (and should) be quantified***
  - *Some details "lost" in qualitative assessment*
  - *Some standards actually* prescribe *the usage of quantitative metrics*
    - *PCI-DSS for vulnerability management*



Quantification and measurement

- ***Some aspects of risk can be quantified***
- ***Technical (=objective) issues can be measured by employing a standardized metric***
- ***Examples: Asset is…***
  - Seismic building
    - Soil classification + building structure
  - Fire-resistant room
    - Time-temperature curve
  - System failure
    - Survival analysis
  - Software vulnerabilities rating
    - Technical aspects of the vulnerability



Example Scenario

- ***Christine's company has recently become a Level 3 merchant***…
  - Level 3 Merchant = More than 20000 ecommerce transactions per year (**~55 transactions x day**)
  - They must be certified by an external assessor not to have high risk vulnerabilities
- ***Lots of Vulnerabilities Around***
  - it discovers that its internal assessors have underestimated the scope of PCI due to their flat corporate network.
  - There are legacy system not involved in card processing on its corporate network, and many of those are no longer maintained and cannot meet PCI DSS requirements.
- ***What is she going to do as a countermeasure?***
  - Different security measures costs a lot.

Example of qualitative vs quantitative

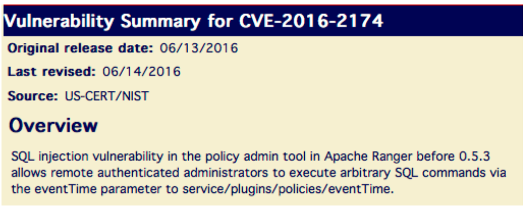
From lecture 05, slide 25

Threat Source	Threat Event	Impact
Alice	Install Malware	Moderate
Outsider	SQL Injection	High

- ***Qualitative assessment***
  - Malware has a lower impact than SQLi → assigned based on expert judgment
- ***Result:***
  - First fix SQL injection because it has a high impact
    - Confidentiality and Integrity impacts on data
  - Then add controls for malware (update AV, data caps policies,..)
    - Worrisome but moderated impact
    - Disclosure of only some data/compartmentalization

Example of qualitative vs quantitative

- ***Is this always reasonable?***
  - Should Christine Patch ALL SQLi vulnerabilities on ALL software?
  - Can not know without a technical/objective analysis of the vulnerability/threat



Vulnerability Summary for CVE-2016-2174

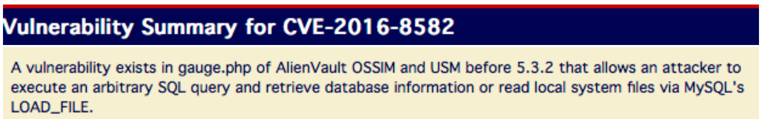
Original release date: 06/13/2016

Last revised: 06/14/2016

Source: US-CERT/NIST

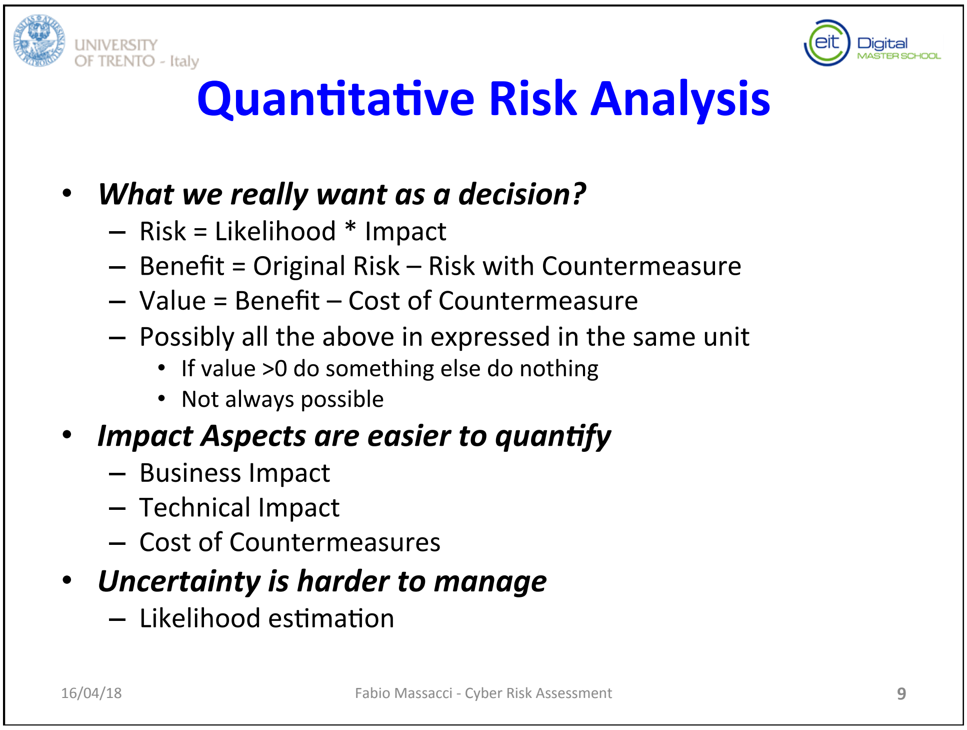
Overview

SQL injection vulnerability in the policy admin tool in Apache Ranger before 0.5.3 allows remote authenticated administrators to execute arbitrary SQL commands via the eventTime parameter to service/plugins/policies/eventTime.



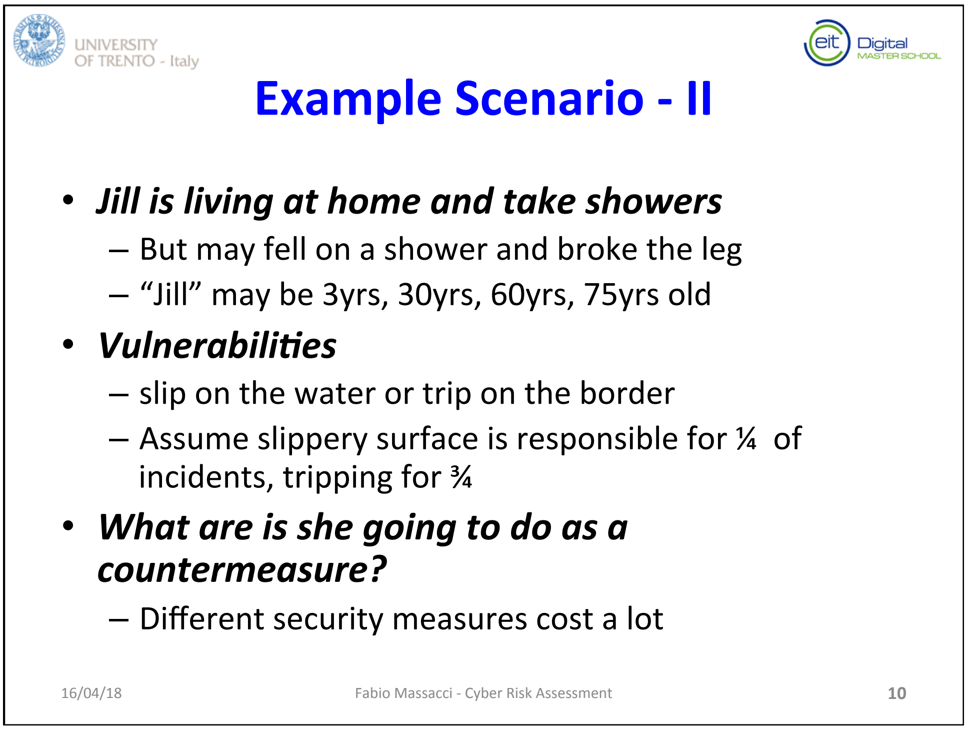
Vulnerability Summary for CVE-2016-8582

A vulnerability exists in gauge.php of AlienVault OSSIM and USM before 5.3.2 that allows an attacker to execute an arbitrary SQL query and retrieve database information or read local system files via MySQL's LOAD_FILE.



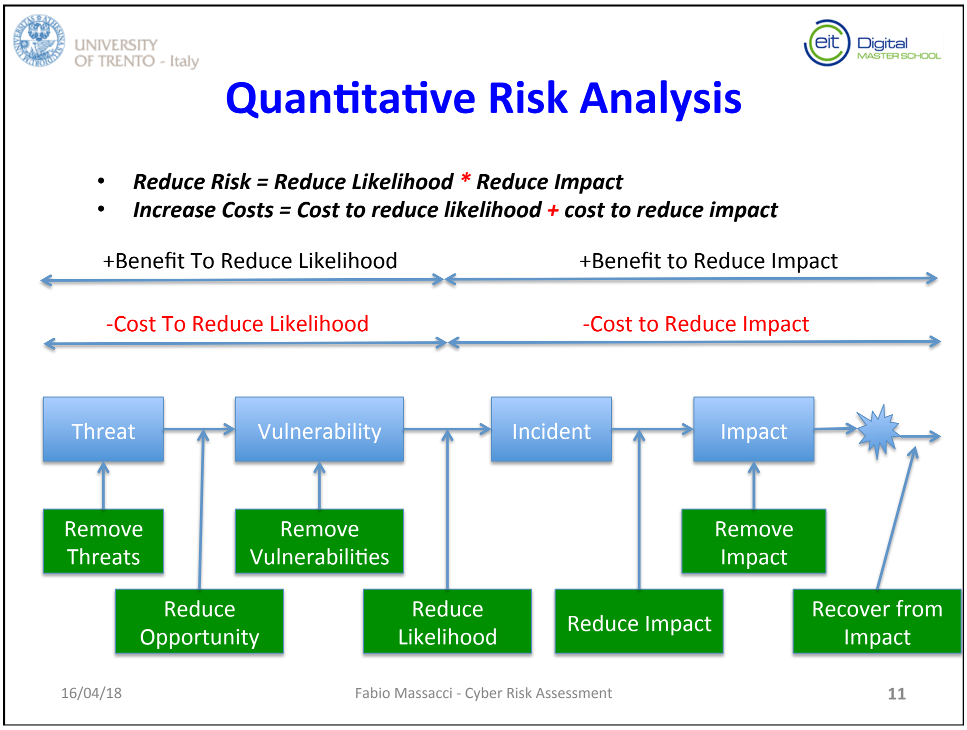
Quantitative Risk Analysis

- ***What we really want as a decision?***
  - Risk = Likelihood * Impact
  - Benefit = Original Risk – Risk with Countermeasure
  - Value = Benefit – Cost of Countermeasure
  - Possibly all the above in expressed in the same unit
    - If value >0 do something else do nothing
    - Not always possible
- ***Impact Aspects are easier to quantify***
  - Business Impact
  - Technical Impact
  - Cost of Countermeasures
- ***Uncertainty is harder to manage***
  - Likelihood estimation



Example Scenario - II

- ***Jill is living at home and take showers***
  - But may fell on a shower and broke the leg
  - “Jill” may be 3yrs, 30yrs, 60yrs, 75yrs old
- ***Vulnerabilities***
  - slip on the water or trip on the border
  - Assume slippery surface is responsible for ¼ of incidents, tripping for ¾
- ***What are is she going to do as a countermeasure?***
  - Different security measures cost a lot



Quantitative Risk Analysis

- *Reduce Risk = Reduce Likelihood* * *Reduce Impact*
- *Increase Costs = Cost to reduce likelihood* + *cost to reduce impact*

+Benefit To Reduce Likelihood

+Benefit to Reduce Impact

-Cost To Reduce Likelihood

-Cost to Reduce Impact

Threat

Vulnerability

Incident

Impact

Remove Threats

Remove Vulnerabilities

Remove Impact

Reduce Opportunity

Reduce Likelihood

Reduce Impact

Recover from Impact

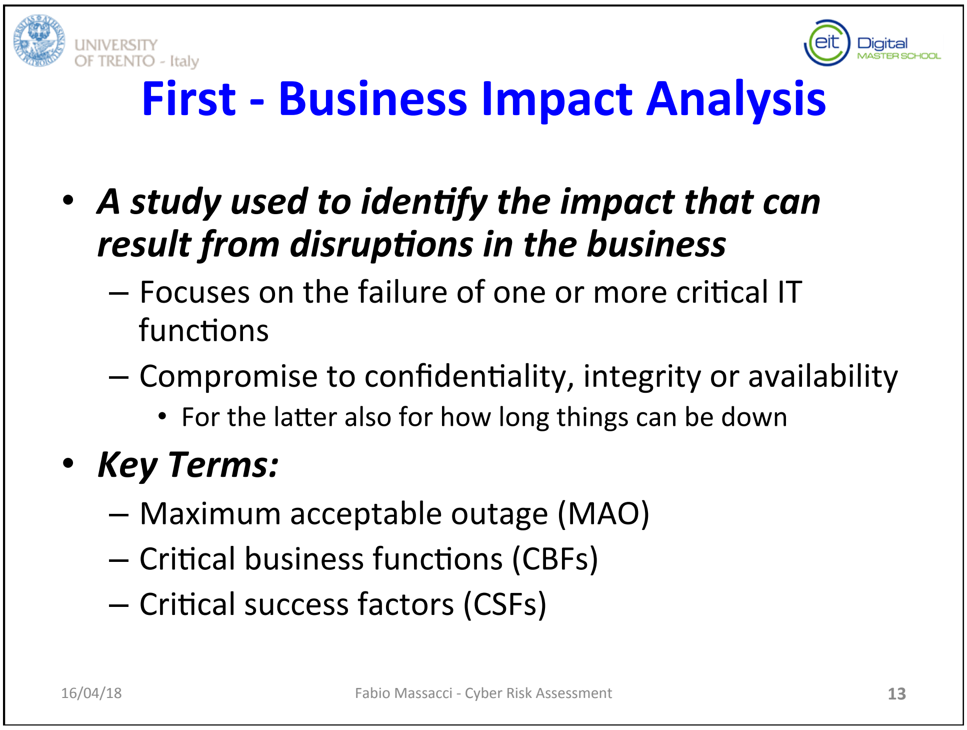
16/04/18 Fabio Massacci - Cyber Risk Assessment 11

How we are going to do that?

- ***Step 1 - Understand Technical Metrics***

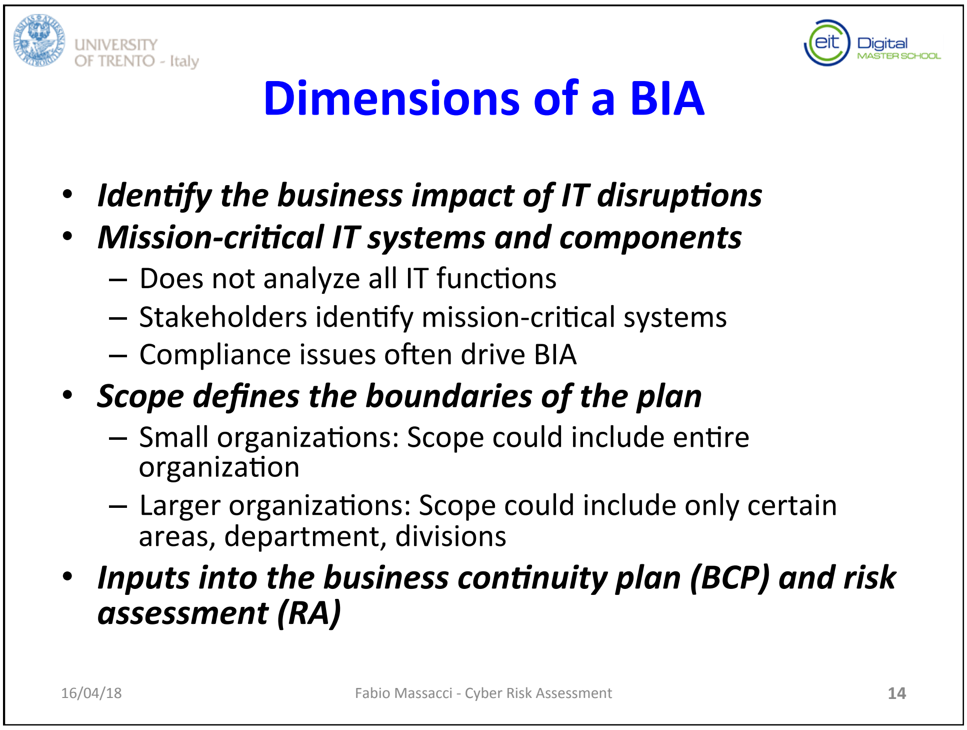
  Technical Measurements of Vulnerabilities
  - Business Impact of Vulnerabilities
- ***Step 2 – Understand Financial and Temporal Metrics***
  - Financial Impact
  - Likelihood
- ***How this is done in industry?***

16/04/18 Fabio Massacci - Cyber Risk Assessment 12



First - Business Impact Analysis

- ***A study used to identify the impact that can result from disruptions in the business***
  - Focuses on the failure of one or more critical IT functions
  - Compromise to confidentiality, integrity or availability
    - For the latter also for how long things can be down
- ***Key Terms:***
  - Maximum acceptable outage (MAO)
  - Critical business functions (CBFs)
  - Critical success factors (CSFs)

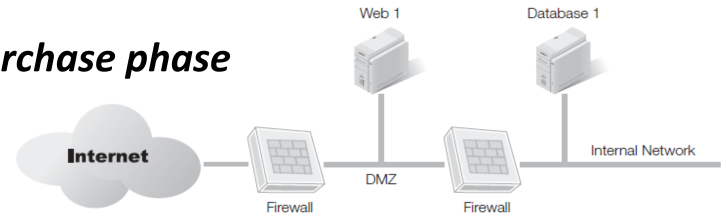


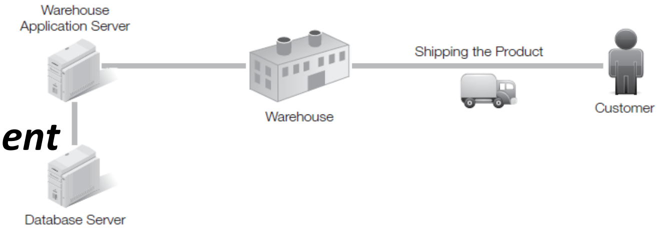
Dimensions of a BIA

- ***Identify the business impact of IT disruptions***
- ***Mission-critical IT systems and components***
  - Does not analyze all IT functions
  - Stakeholders identify mission-critical systems
  - Compliance issues often drive BIA
- ***Scope defines the boundaries of the plan***
  - Small organizations: Scope could include entire organization
  - Larger organizations: Scope could include only certain areas, department, divisions
- ***Inputs into the business continuity plan (BCP) and risk assessment (RA)***

Defining Scope of a BIA

- ***E.g. Purchase phase***

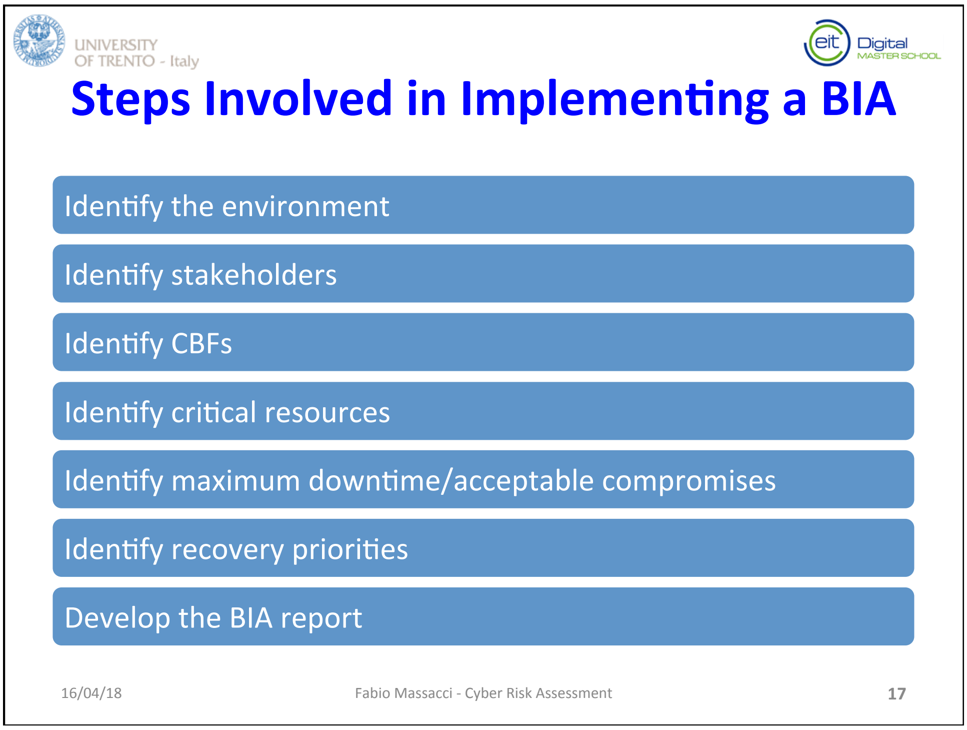




- ***E.g. Shipment phase***

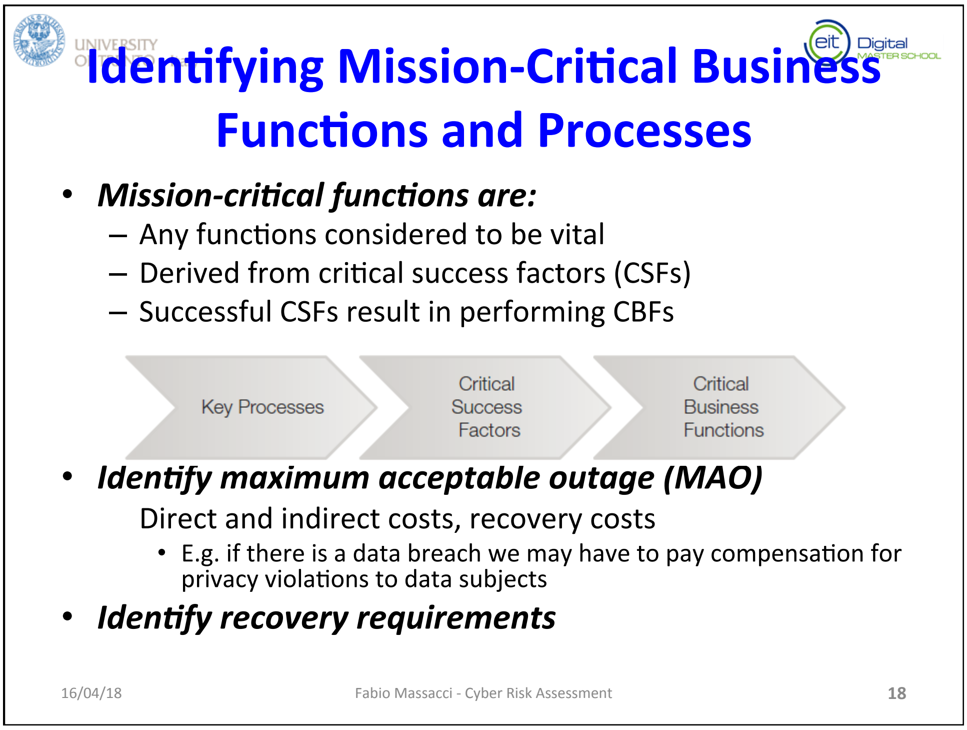
Segregating the Scope

- ***What is in scope?***
  - “Everything” on which CBF depend…
- ***Limiting the Scope is important***
  - it avoids that to achive the CBF “have a relaxed holiday trip” you need to deploy the preventive control “Ensure world peace” which is significantly more complex than “buy travel insurance”
- ***But can be misleading***
  - You can leave out key important details that can compromise the security



Steps Involved in Implementing a BIA

- Identify the environment
- Identify stakeholders
- Identify CBFs
- Identify critical resources
- Identify maximum downtime/acceptable compromises
- Identify recovery priorities
- Develop the BIA report



Identifying Mission-Critical Business Functions and Processes

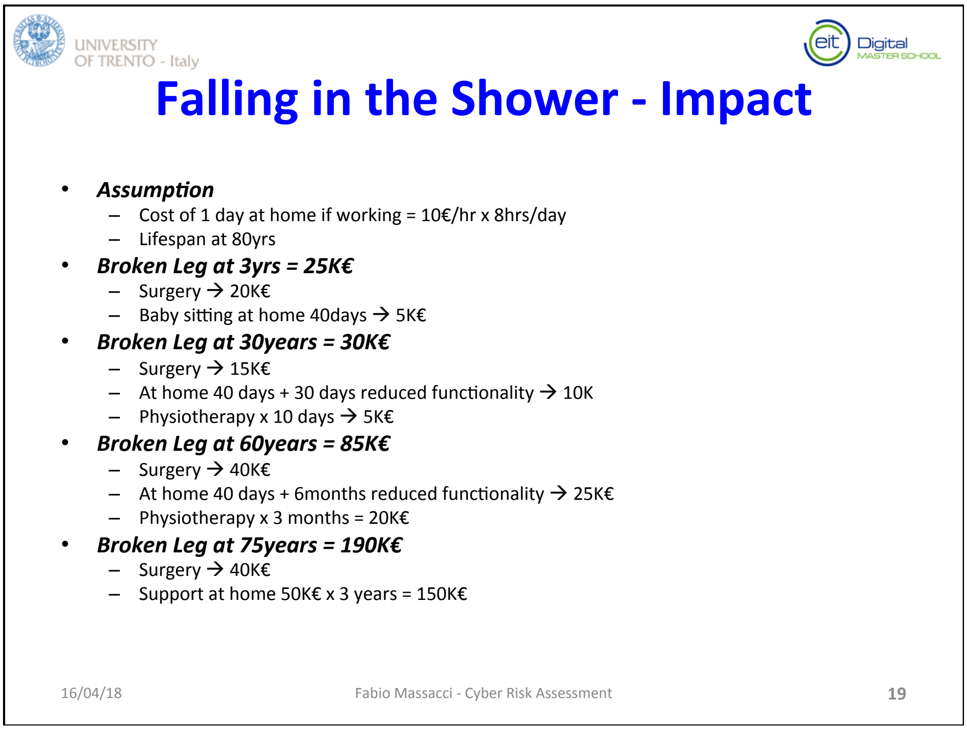
- ***Mission-critical functions are:***
  - Any functions considered to be vital
  - Derived from critical success factors (CSFs)
  - Successful CSFs result in performing CBFs

Key Processes → Critical Success Factors → Critical Business Functions

- ***Identify maximum acceptable outage (MAO)***

  Direct and indirect costs, recovery costs

  - E.g. if there is a data breach we may have to pay compensation for privacy violations to data subjects
- ***Identify recovery requirements***



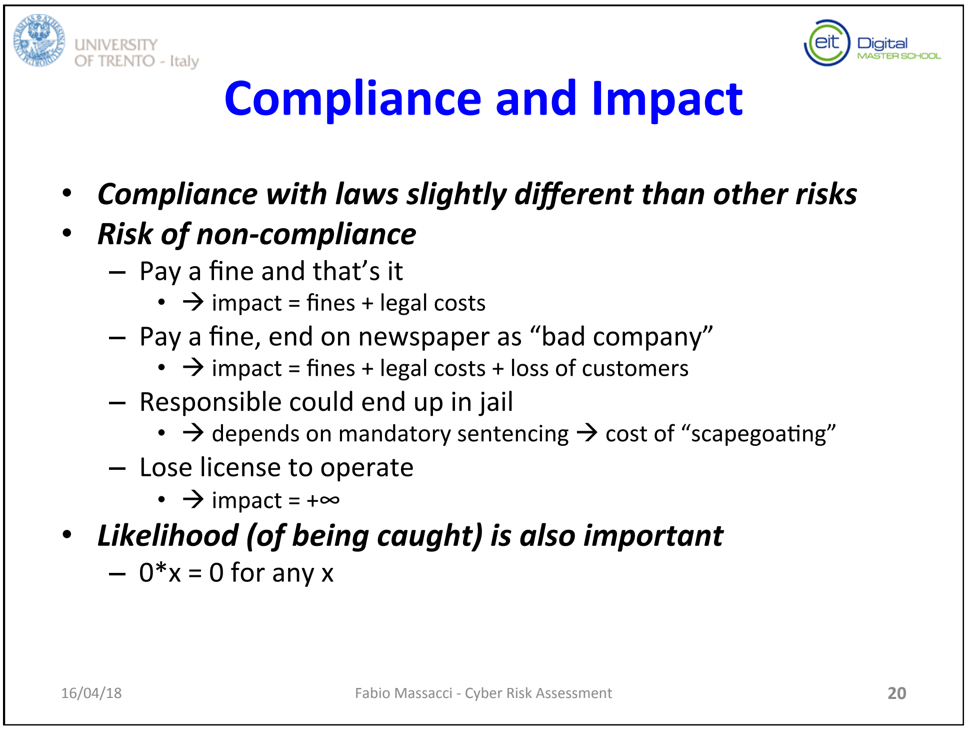
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Falling in the Shower - Impact

- ***Assumption***
  - Cost of 1 day at home if working = 10€/hr x 8hrs/day
  - Lifespan at 80yrs
- ***Broken Leg at 3yrs = 25K€***
  - Surgery → 20K€
  - Baby sitting at home 40days → 5K€
- ***Broken Leg at 30years = 30K€***
  - Surgery → 15K€
  - At home 40 days + 30 days reduced functionality → 10K
  - Physiotherapy x 10 days → 5K€
- ***Broken Leg at 60years = 85K€***
  - Surgery → 40K€
  - At home 40 days + 6months reduced functionality → 25K€
  - Physiotherapy x 3 months = 20K€
- ***Broken Leg at 75years = 190K€***
  - Surgery → 40K€
  - Support at home 50K€ x 3 years = 150K€

16/04/18 Fabio Massacci - Cyber Risk Assessment 19



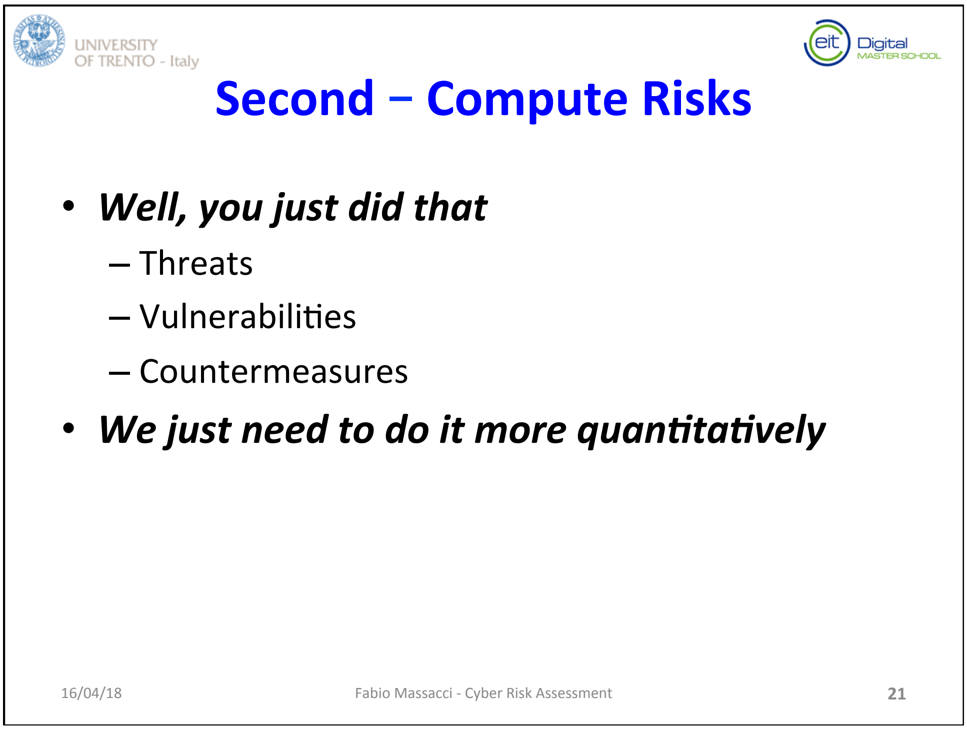
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Compliance and Impact

- ***Compliance with laws slightly different than other risks***
- ***Risk of non-compliance***
  - Pay a fine and that's it
    - → impact = fines + legal costs
  - Pay a fine, end on newspaper as "bad company"
    - → impact = fines + legal costs + loss of customers
  - Responsible could end up in jail
    - → depends on mandatory sentencing → cost of "scapegoating"
  - Lose license to operate
    - → impact = +∞
- ***Likelihood (of being caught) is also important***
  - 0*x = 0 for any x

16/04/18 Fabio Massacci - Cyber Risk Assessment 20

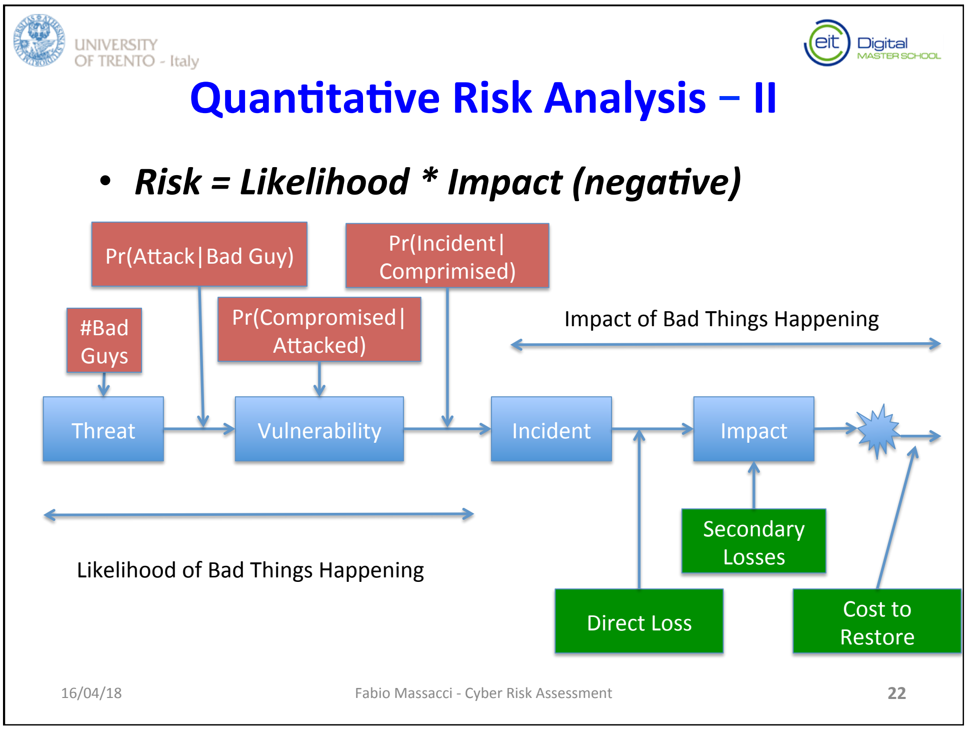


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Second – Compute Risks

- ***Well, you just did that***
  - Threats
  - Vulnerabilities
  - Countermeasures
- ***We just need to do it more quantitatively***

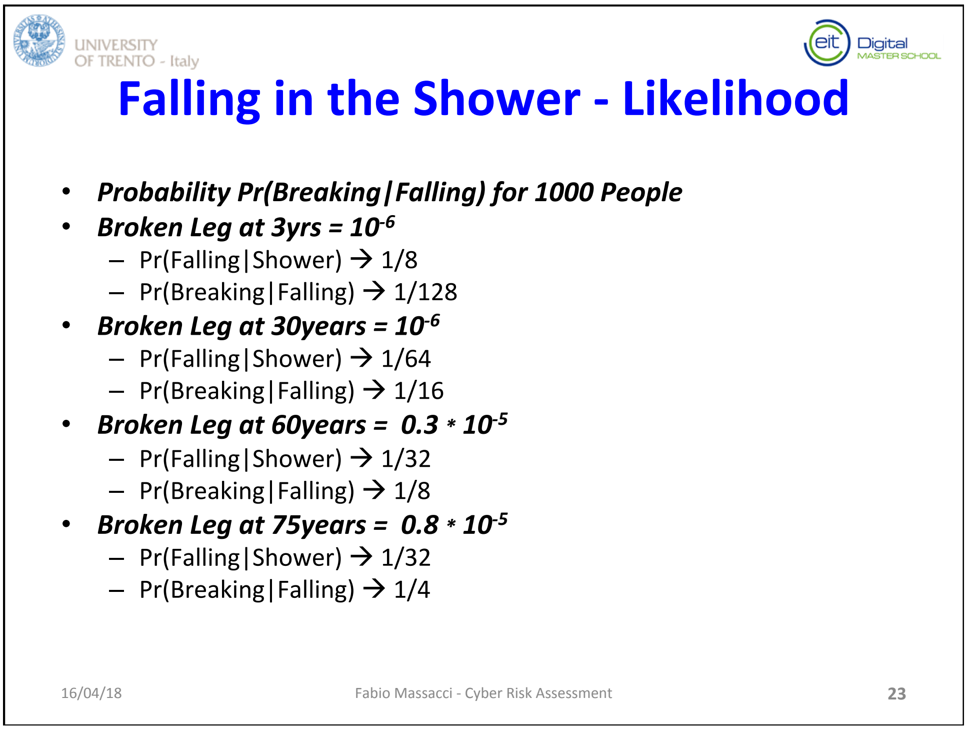


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

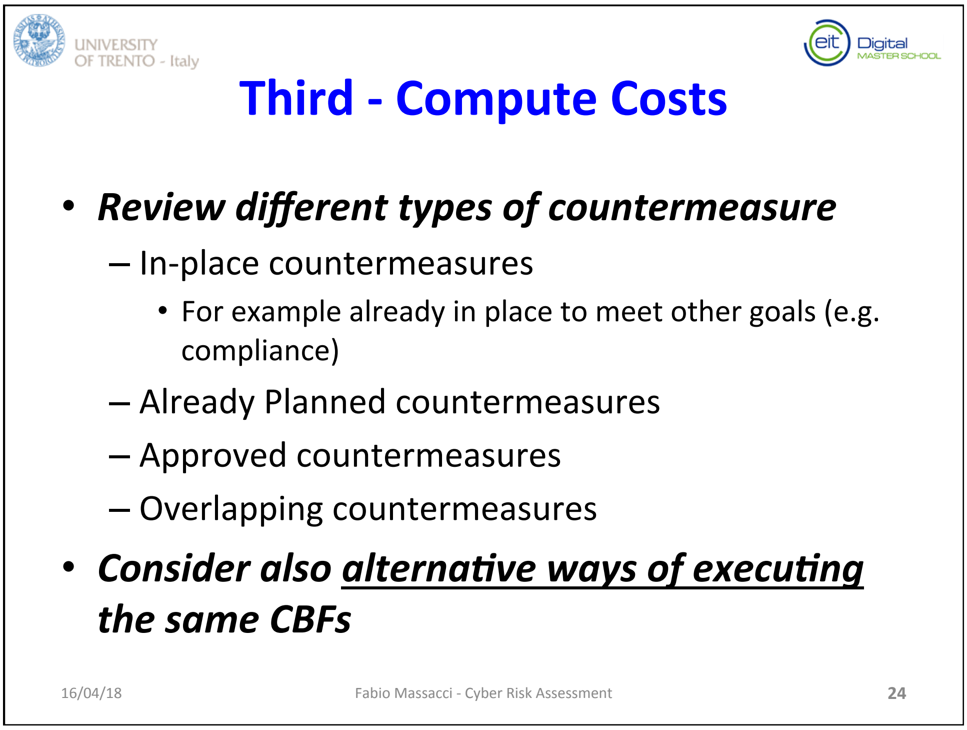
Quantitative Risk Analysis – II

- ***Risk = Likelihood * Impact (negative)***



Falling in the Shower - Likelihood

- ***Probability Pr(Breaking|Falling) for 1000 People***
- ***Broken Leg at 3yrs = 10^{-6}***
  - Pr(Falling|Shower) → 1/8
  - Pr(Breaking|Falling) → 1/128
- ***Broken Leg at 30years = 10^{-6}***
  - Pr(Falling|Shower) → 1/64
  - Pr(Breaking|Falling) → 1/16
- ***Broken Leg at 60years = 0.3 * 10^{-5}***
  - Pr(Falling|Shower) → 1/32
  - Pr(Breaking|Falling) → 1/8
- ***Broken Leg at 75years = 0.8 * 10^{-5}***
  - Pr(Falling|Shower) → 1/32
  - Pr(Breaking|Falling) → 1/4



Third - Compute Costs

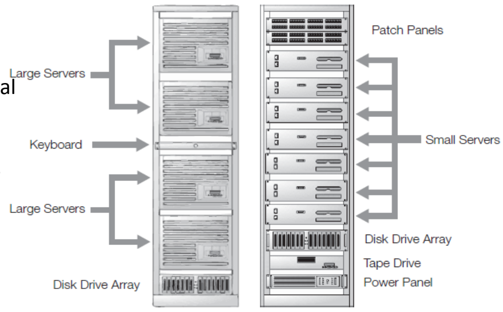
- ***Review different types of countermeasure***
  - In-place countermeasures
    - For example already in place to meet other goals (e.g. compliance)
  - Already Planned countermeasures
  - Approved countermeasures
  - Overlapping countermeasures
- ***Consider also alternative ways of executing the same CBFs***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Calculating Costs

- ***Initial purchase***
  - Small servers vs big server
- ***Facility***
  - Do we need to change the physical location
- ***Installation & Operation***
  - Things never work by themselves
    - Air Carrier → very powerful but requires 1K people to operate
    - Nuclear submarine → can do a lot less but 25 people can operate it
  - This may be a recurring costs!
- ***Training***
  - Can anybody use it?

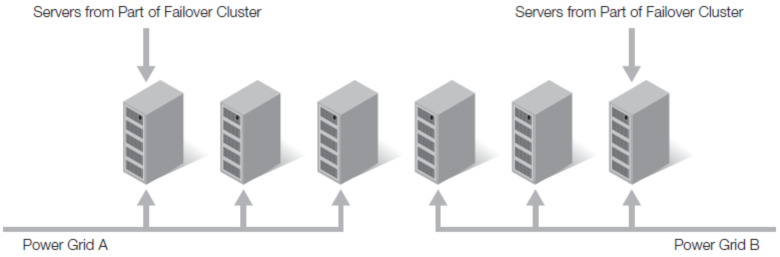


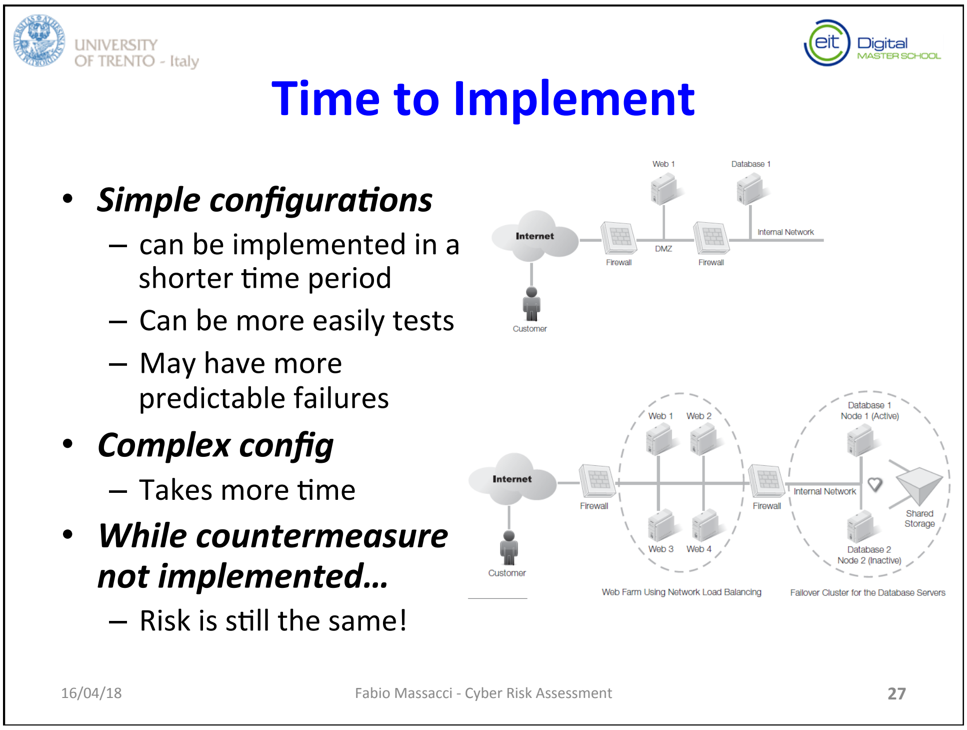
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Calculating Costs

- ***Look for hidden costs***
- ***Is extra power required to eliminate a single point of failure?***

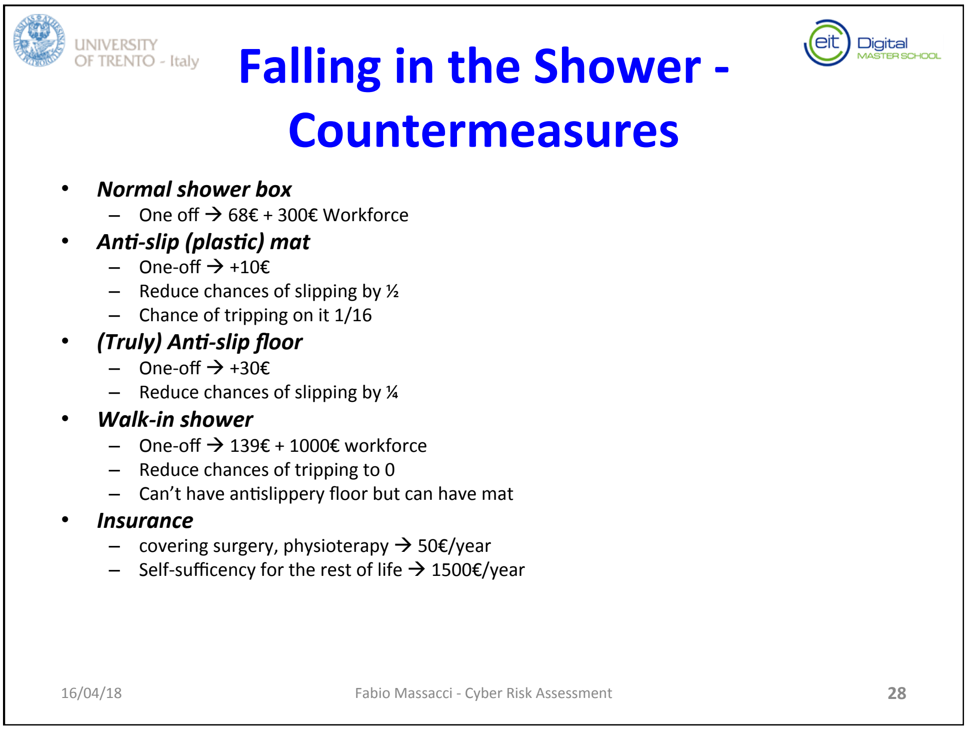

Servers from Part of Failover Cluster
Servers from Part of Failover Cluster
Power Grid A
Power Grid B



Time to Implement

- ***Simple configurations***
  - can be implemented in a shorter time period
  - Can be more easily tests
  - May have more predictable failures
- ***Complex config***
  - Takes more time
- ***While countermeasure not implemented…***
  - Risk is still the same!

Web 1
Database 1
Internet
Firewall
DMZ
Firewall
Internal Network
Customer
Web 1
Web 2
Database 1
Node 1 (Active)
Internet
Firewall
Firewall
Internal Network
Shared Storage
Web 3
Web 4
Database 2
Node 2 (Inactive)
Customer
Web Farm Using Network Load Balancing
Failover Cluster for the Database Servers



Falling in the Shower - Countermeasures

- ***Normal shower box***
  - One off → 68€ + 300€ Workforce
- ***Anti-slip (plastic) mat***
  - One-off → +10€
  - Reduce chances of slipping by ½
  - Chance of tripping on it 1/16
- ***(Truly) Anti-slip floor***
  - One-off → +30€
  - Reduce chances of slipping by ¼
- ***Walk-in shower***
  - One-off → 139€ + 1000€ workforce
  - Reduce chances of tripping to 0
  - Can't have antislippery floor but can have mat
- ***Insurance***
  - covering surgery, physioterapy → 50€/year
  - Self-sufficency for the rest of life → 1500€/year

Prioritizing Risk Elements

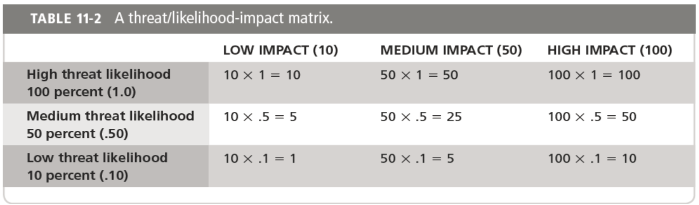


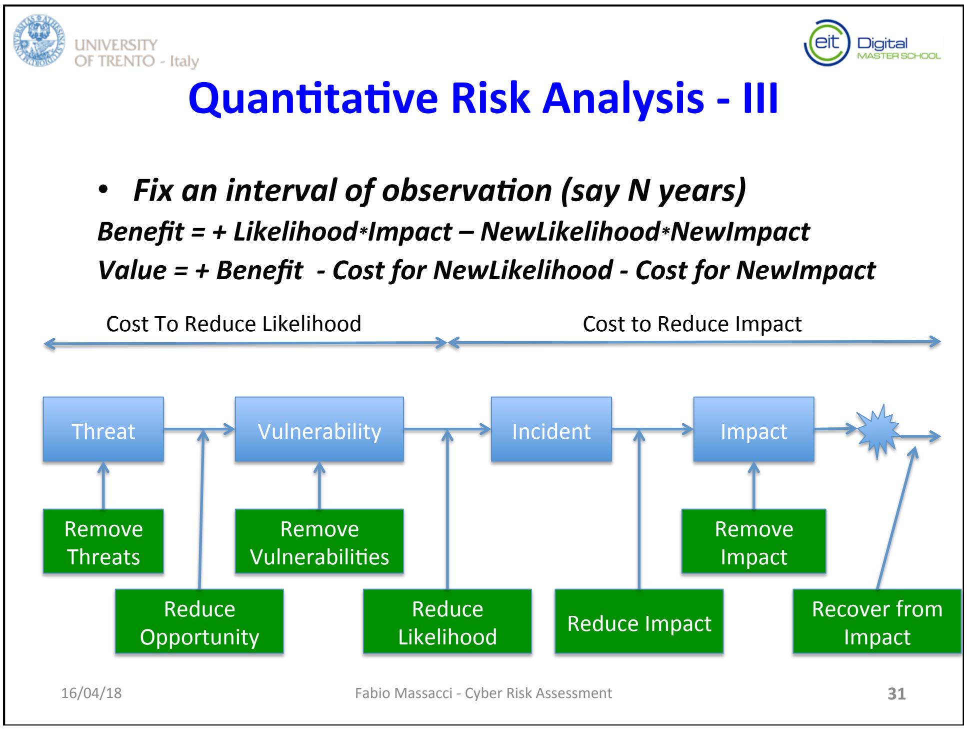
TABLE 11-2 A threat/likelihood-impact matrix.

	LOW IMPACT (10)	MEDIUM IMPACT (50)	HIGH IMPACT (100)
High threat likelihood 100 percent (1.0)	10 × 1 = 10	50 × 1 = 50	100 × 1 = 100
Medium threat likelihood 50 percent (.50)	10 × .5 = 5	50 × .5 = 25	100 × .5 = 50
Low threat likelihood 10 percent (.10)	10 × .1 = 1	50 × .1 = 5	100 × .1 = 10

- ***Remember that ordinals don't scale!***
  - We quantize things but this can be misleading
- ***Example shower incident (1yr salary = 50K)***
  - IF Impact >1yr salary → High Risk=3
  - ELSE IF Impact >1 month → Medium risk = 2
  - ELSE Low risk = 1
  - Do the same for likelihood
  - High Risk = High Likelihood * High Impact = 3*3 = 9
- ***Did something changed over our prioritization with "cardinals"?***

Cost Benefit Analysis Report Elements

- Recommended countermeasure
- Risk to be mitigated
- Annual projected benefits
- Initial costs
- Annual or recurring costs
- A comparison of costs and benefits
- Recommendation



Quantitative Risk Analysis - III

- *Fix an interval of observation (say N years)*

Benefit = + Likelihood*Impact – NewLikelihood*NewImpact

Value = + Benefit - Cost for NewLikelihood - Cost for NewImpact

Cost To Reduce Likelihood

Cost to Reduce Impact

Threat

Vulnerability

Incident

Impact

Remove Threats

Remove Vulnerabilities

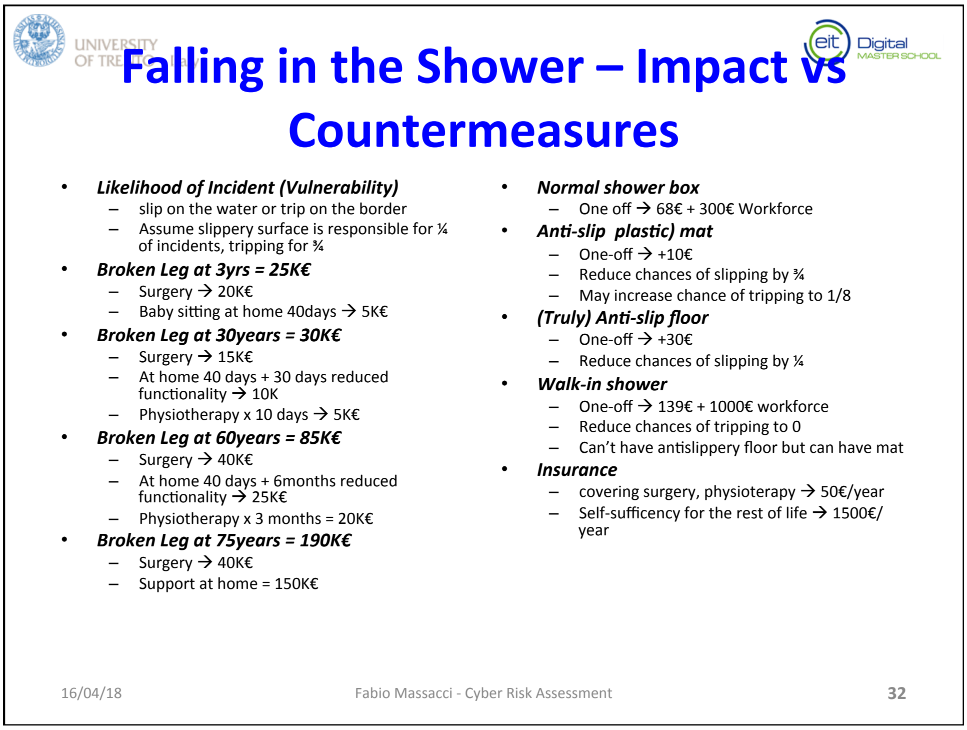
Remove Impact

Reduce Opportunity

Reduce Likelihood

Reduce Impact

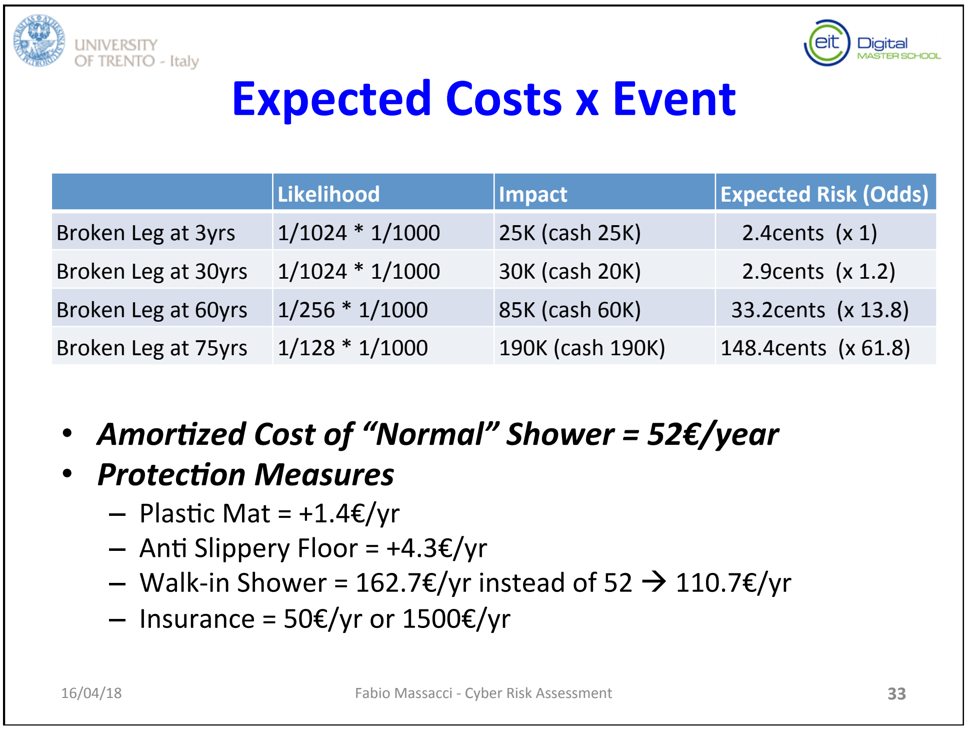
Recover from Impact



Falling in the Shower – Impact vs Countermeasures

- ***Likelihood of Incident (Vulnerability)***
  - slip on the water or trip on the border
  - Assume slippery surface is responsible for ¼ of incidents, tripping for ¾
- ***Broken Leg at 3yrs = 25K€***
  - Surgery → 20K€
  - Baby sitting at home 40days → 5K€
- ***Broken Leg at 30years = 30K€***
  - Surgery → 15K€
  - At home 40 days + 30 days reduced functionality → 10K
  - Physiotherapy x 10 days → 5K€
- ***Broken Leg at 60years = 85K€***
  - Surgery → 40K€
  - At home 40 days + 6months reduced functionality → 25K€
  - Physiotherapy x 3 months = 20K€
- ***Broken Leg at 75years = 190K€***
  - Surgery → 40K€
  - Support at home = 150K€

- ***Normal shower box***
  - One off → 68€ + 300€ Workforce
- ***Anti-slip plastic) mat***
  - One-off → +10€
  - Reduce chances of slipping by ¾
  - May increase chance of tripping to 1/8
- ***(Truly) Anti-slip floor***
  - One-off → +30€
  - Reduce chances of slipping by ¼
- ***Walk-in shower***
  - One-off → 139€ + 1000€ workforce
  - Reduce chances of tripping to 0
  - Can't have antislippery floor but can have mat
- ***Insurance***
  - covering surgery, physioterapy → 50€/year
  - Self-sufficency for the rest of life → 1500€/year



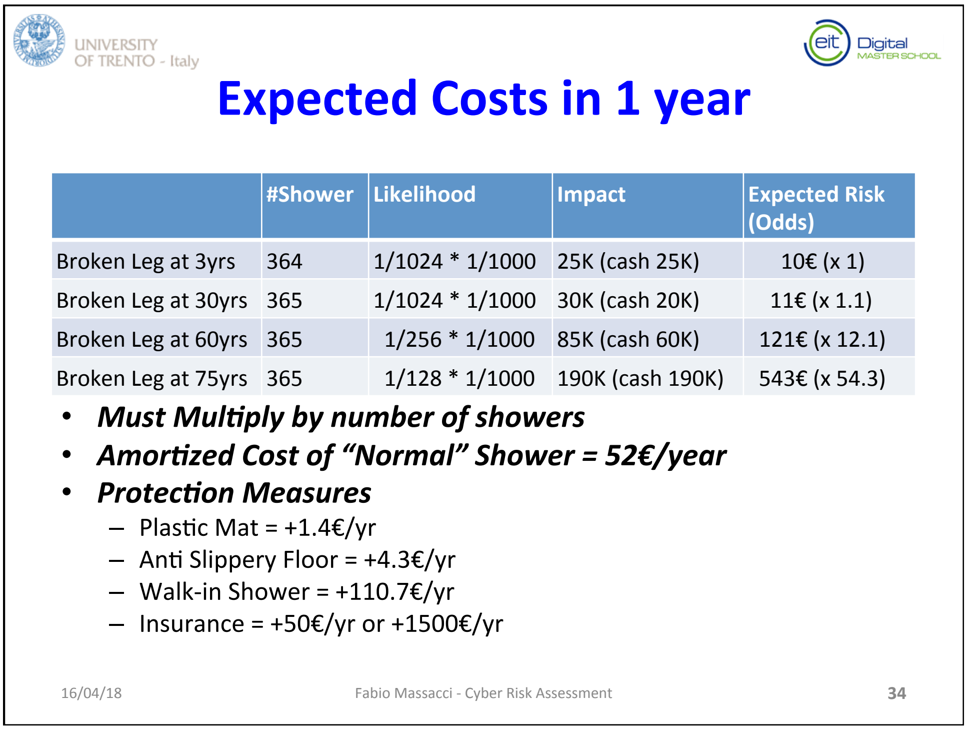
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Expected Costs x Event

	Likelihood	Impact	Expected Risk (Odds)
Broken Leg at 3yrs	1/1024 * 1/1000	25K (cash 25K)	2.4cents (x 1)
Broken Leg at 30yrs	1/1024 * 1/1000	30K (cash 20K)	2.9cents (x 1.2)
Broken Leg at 60yrs	1/256 * 1/1000	85K (cash 60K)	33.2cents (x 13.8)
Broken Leg at 75yrs	1/128 * 1/1000	190K (cash 190K)	148.4cents (x 61.8)

- ***Amortized Cost of "Normal" Shower = 52€/year***
- ***Protection Measures***
  - Plastic Mat = +1.4€/yr
  - Anti Slippery Floor = +4.3€/yr
  - Walk-in Shower = 162.7€/yr instead of 52 → 110.7€/yr
  - Insurance = 50€/yr or 1500€/yr



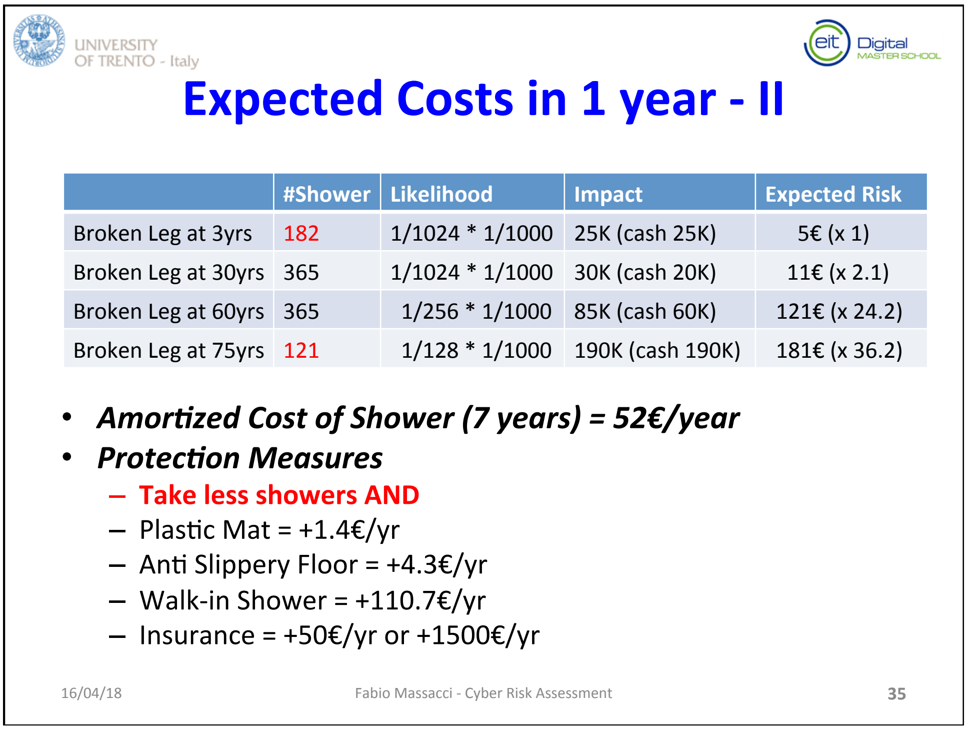
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Expected Costs in 1 year

	#Shower	Likelihood	Impact	Expected Risk (Odds)
Broken Leg at 3yrs	364	1/1024 * 1/1000	25K (cash 25K)	10€ (x 1)
Broken Leg at 30yrs	365	1/1024 * 1/1000	30K (cash 20K)	11€ (x 1.1)
Broken Leg at 60yrs	365	1/256 * 1/1000	85K (cash 60K)	121€ (x 12.1)
Broken Leg at 75yrs	365	1/128 * 1/1000	190K (cash 190K)	543€ (x 54.3)

- ***Must Multiply by number of showers***
- ***Amortized Cost of "Normal" Shower = 52€/year***
- ***Protection Measures***
  - Plastic Mat = +1.4€/yr
  - Anti Slippery Floor = +4.3€/yr
  - Walk-in Shower = +110.7€/yr
  - Insurance = +50€/yr or +1500€/yr



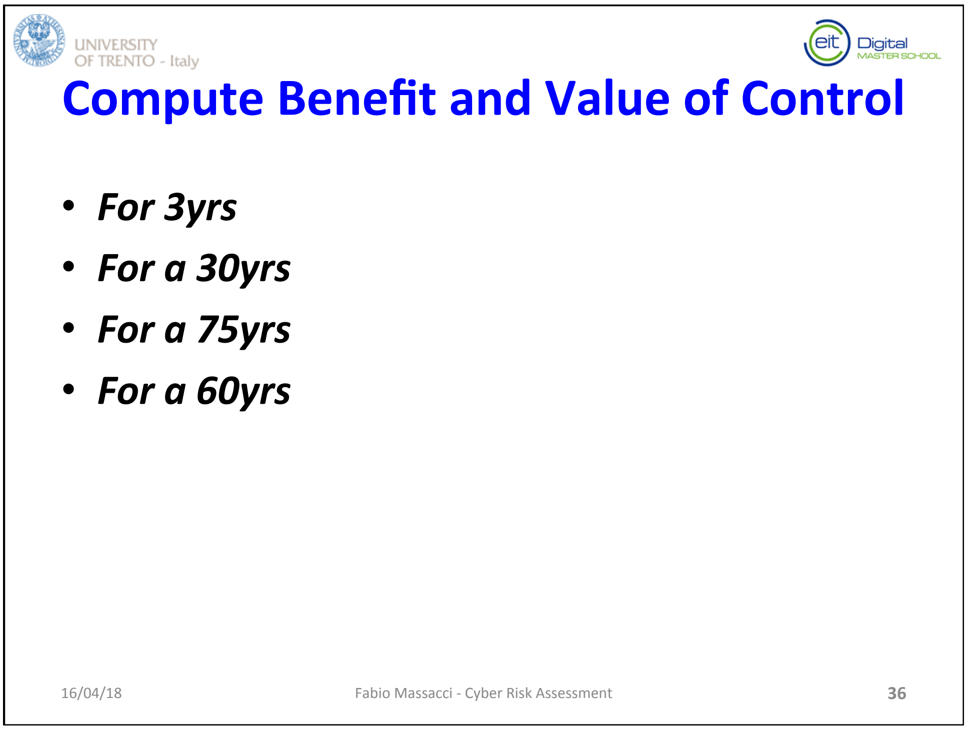
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Expected Costs in 1 year - II

	#Shower	Likelihood	Impact	Expected Risk
Broken Leg at 3yrs	182	1/1024 * 1/1000	25K (cash 25K)	5€ (x 1)
Broken Leg at 30yrs	365	1/1024 * 1/1000	30K (cash 20K)	11€ (x 2.1)
Broken Leg at 60yrs	365	1/256 * 1/1000	85K (cash 60K)	121€ (x 24.2)
Broken Leg at 75yrs	121	1/128 * 1/1000	190K (cash 190K)	181€ (x 36.2)

- ***Amortized Cost of Shower (7 years) = 52€/year***
- ***Protection Measures***
  - **Take less showers AND**
  - Plastic Mat = +1.4€/yr
  - Anti Slippery Floor = +4.3€/yr
  - Walk-in Shower = +110.7€/yr
  - Insurance = +50€/yr or +1500€/yr

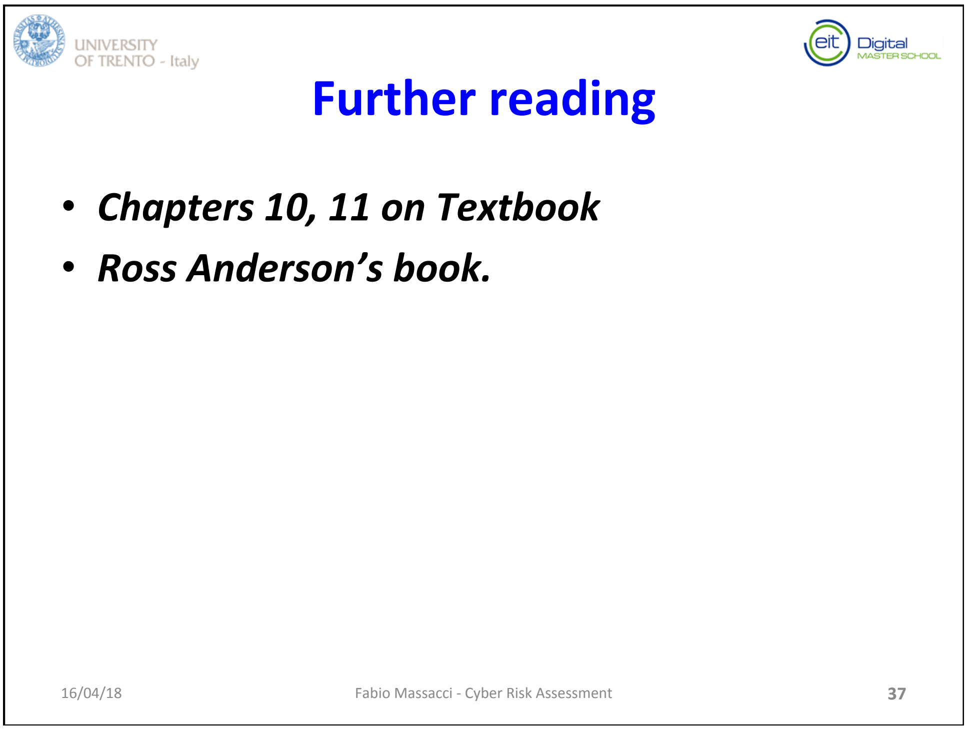


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Compute Benefit and Value of Control

- ***For 3yrs***
- ***For a 30yrs***
- ***For a 75yrs***
- ***For a 60yrs***



Further reading

- *Chapters 10, 11 on Textbook*
- *Ross Anderson's book.*