UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Cyber Security Risk Assessment Fall 2016

Lecture 13

Quantitative Risk Analysis

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Falling in the Shower

- ***Incident scenario***
  - Fell on the shower and broke the leg
- ***Vulnerabilities***
  - slip on the water or trip on the border
  - Assume slippery surface is responsible for ¼ of incidents, tripping for ¾
- ***Information on "Customer"***
  - 3yrs, 30yrs, 60yrs, 75yrs
  - Average duration of home stay - 7years
- ***What are you going to buy?***
- ***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
- ***Floor 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

Quantitative Risk Analysis - I

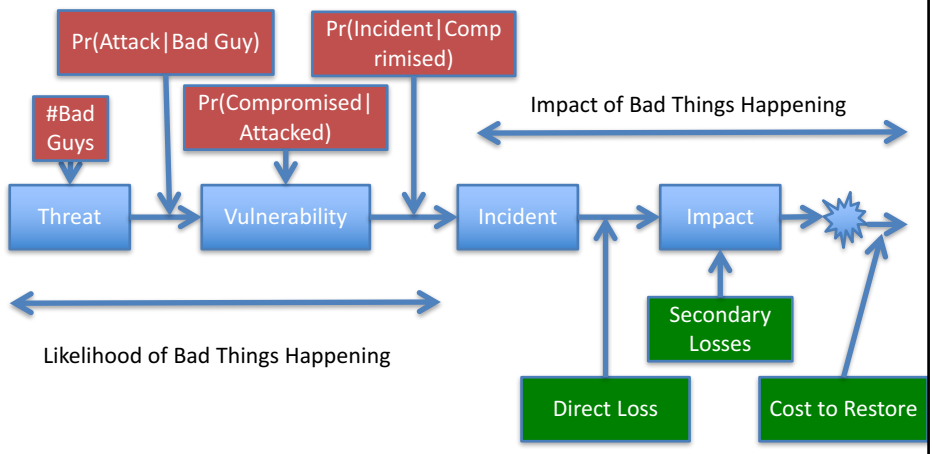
- ***Relations***
  - Risk = Likelihood * Impact
  - Benefit = Original Risk – Risk with Countermeasure
  - Value = Benefit – Cost of Countermeasure
- ***Financial Aspects are easier to calculate***
  1. Business Impact
  2. Cost of Countermeasures
- ***Uncertainty is harder to manage***
  3. Likelihood estimation

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Quantitative Risk Analysis - II

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



UNIVERSITY OF TRENTO - Italy

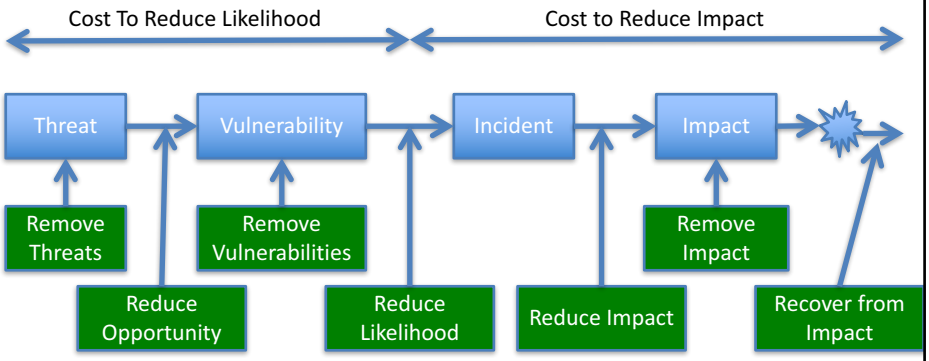
eit Digital MASTER SCHOOL

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



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 = 150K€

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Falling in the Shower – Impact?

- ***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
- ***Floor 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

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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Expected Costs x Event

	Likelihood	Impact	Expected Risk
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 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
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)

- ***Amortized Cost of 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

	#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 = 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 a 75yrs***
  - Walk-in Shower
  - Walk-in Shower + Anti-Slip Mat
- ***For a 60yrs***
  - Anti-slippery floor + Incident Insurance

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Step 1: 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)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Dimensions of a BIA

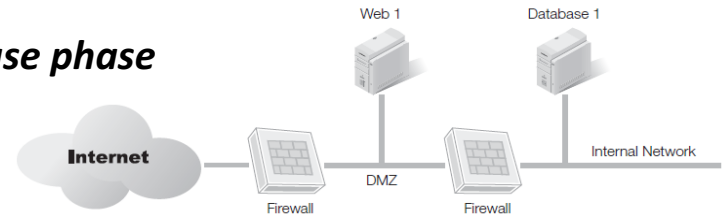
- ***Identify the business impact of IT disruptions***
- ***Mission-critical IT systems and components***
  - Does not analyze all IT functions
  - Stakeholders identify mission-critical systems
  - Compliance issues often drive BIA
- ***Scope defines the boundaries of the plan***
  - Small organizations: 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)***

UNIVERSITY OF TRENTO - Italy

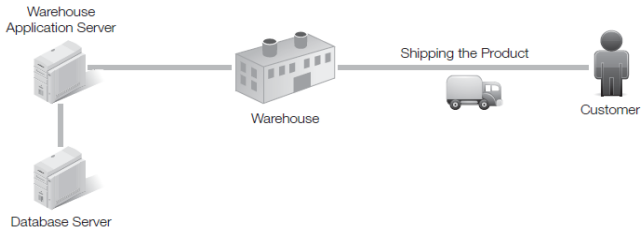
eit Digital MASTER SCHOOL

Defining Scope of a BIA

- ***Purchase phase***



- ***Shipment phase***



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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

- ***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***

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

UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

Step 2 – Computing Costs

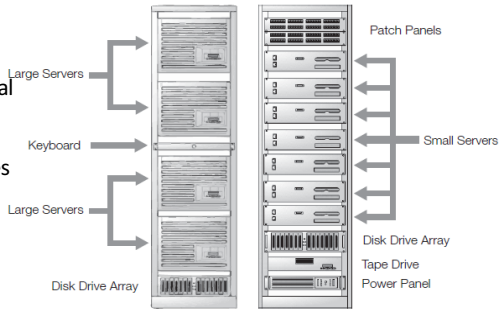
- ***Review different types of countermeasure***
  - In-place countermeasures
    - For example already in place to meet other goals (e.g. compliance)
  - Already Planned countermeasures
  - Approved countermeasures
  - Overlapping countermeasures
- ***Consider also alternative ways of executing the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

UNIVERSITY OF TRENTO - Italy

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 themeselves
    - 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?

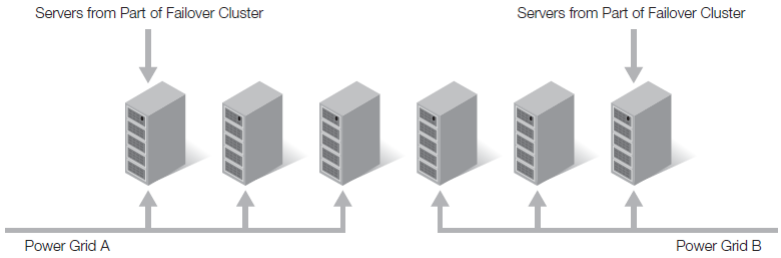


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Calculating Costs

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

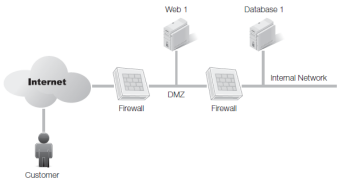


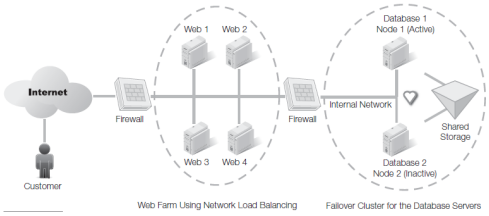
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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!





UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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"?***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Further reading

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