UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Cyber Security Risk Assessment Fall 2016

Lecture 03 – Introducing Risk Assessment

Fabio Massacci

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What is a vulnerability, a threat, and risk?

- ***Threat***
  - circumstance, capability, event, action that could breach securtity 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

Unintentional Threats	Intentional Threats
Environmental: ▪ Fire, wind ▪ Lighting, flooding ▪ Accident ▪ Equipment failures	Individuals or Organizations: ▪ Hackers ▪ Criminals ▪ Disgruntled employees
Human: ▪ Keystroke errors ▪ Procedural errors ▪ Programming bugs	

Intentional Threat Types

- ***Attive Attacks***
  - Aim to modify system'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'assets
  - Detecting them is harder than preventing them
  - e.g traffic analysis

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Threat Agents

- ***Insider Attacks***
  - The treat 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***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Tangible Assets and Threats

	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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Historic Threats to Tangible Assets

- ***Hardware***
  - Desktop computer stolen at Sutter Physicians Services and Sutter Medical Foundation, which contained about 3.3 million patients' mediacal 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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Unwanted Consequences

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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Which incident does affect…

	Unauthorized disclosure	Deception	Disruption	Usurpation
Confidentiality	No	No	Yes	kInd of
Integrity	Yes	No	Yes	Not really
Availability		Kind of		No

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Which incident does affect… (2015)

	Unauthorized disclosure	Deception	Disruption	Usurpation
Confidentiality	yes	No but can lead to a later compromise	No	Yes
Integrity	No	Yes	Yes if data is also corrupted	Yes
Availability	No	No but can lead to a later compromise	Yes	Maybe, depends on context of implementation

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

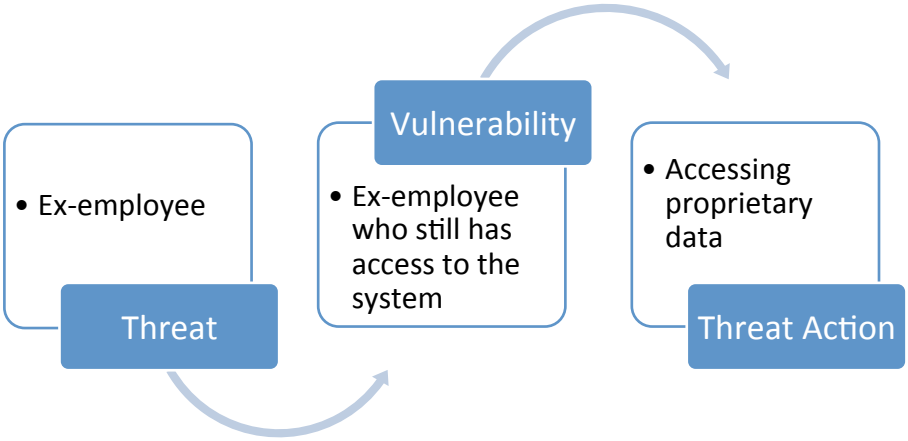
Threat/Vulnerability Pair

- ***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

UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

Threat/Vulnerability Pair and Threat Action



UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

Threat/Vulnerability Pair Examples

- ***Example "Classic"***
  - Asset
    - Sensitive Files
  - Threat Source
    - Unauthorized users (e.g., hackers)
  - Vulnerability
    - Identified flaws in system design
    - New patches not applied
  - Threat Action
    - Unauthorized access to files
- ***Example "Unexpected"***
  - Asset
    - Expensive Hardware
  - Threat Source:
    - Fire or negligent person
  - Vulnerability
    - Sprinklers used to suppress fire damage
    - Protective tarpaulins not in place
  - Threat Action
    - Sprinkler system turned on→hardware wet and to be thrown away

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What is a security control?

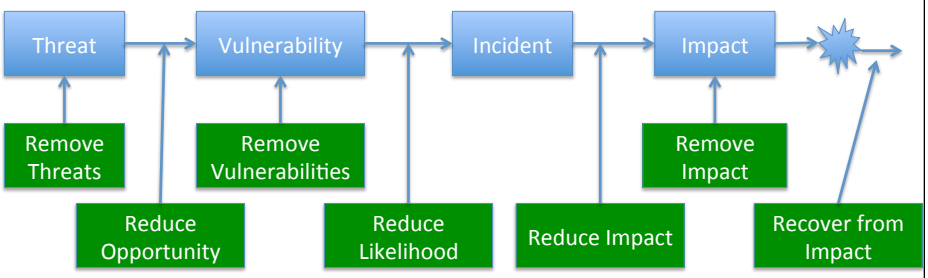
- *an action, device, a procedure or technique that …*
- *reduces a threat, a vulnerability, or an attack by ….*
- *eliminating it,*
- *minimizing the harm it causes, or*
- *discovering and reporting it so that corrective action can be taken*

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



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Which control does protect…

	Preventive	Detective	Reactive
Confidentiality	Yes	Depends on time (if half way through attack may be yes)	Too late – pay ransom
Integrity	Yes	Needed for mantaining integrity	Yes (at least if only the final state truly important)
Availability	Yes (throught redundant services)	Yes	Yes (through redundant services, if only the final state truly important)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Which control does protect… (2015)

	Preventive	Detective	Reactive
Confidentiality	Yes	Yes if detection happens before the exfiltration take place	No, may be stopped in "between"
Integrity	Yes	No, may be stopped in "between"	Yes
Availability	Yes (redundant resources)	No, may be stopped in "between"	Yes

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

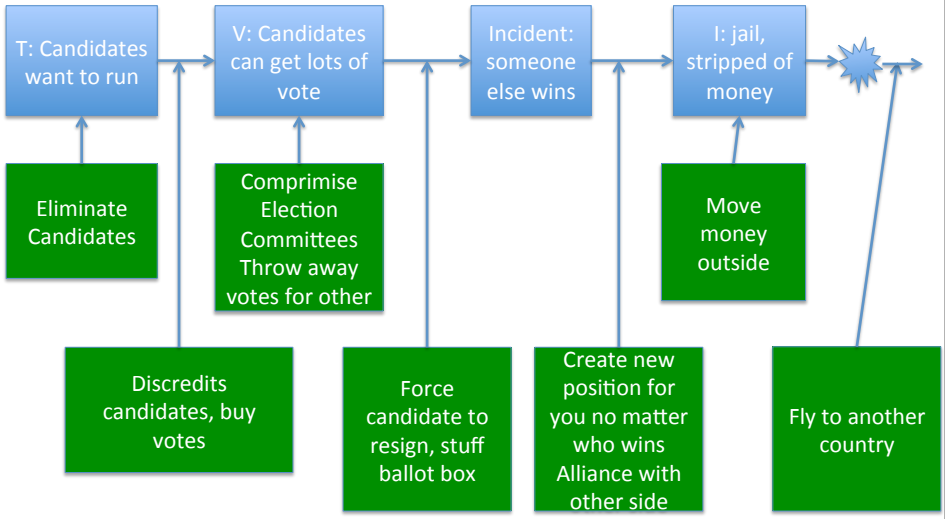
The Russian Election Problem

- ***Suppose you are the currrent Russian president***
  - Threats: Opposition candidates want elected positions
  - Vulnerabilities: Voters can vote for them
  - (Un)wanted Incident: Another candidate wins the post of president
  - Impact: Winning candidate send Putin to jail and strip him of his vast riches and powers
- ***Risk Analysis?***

UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

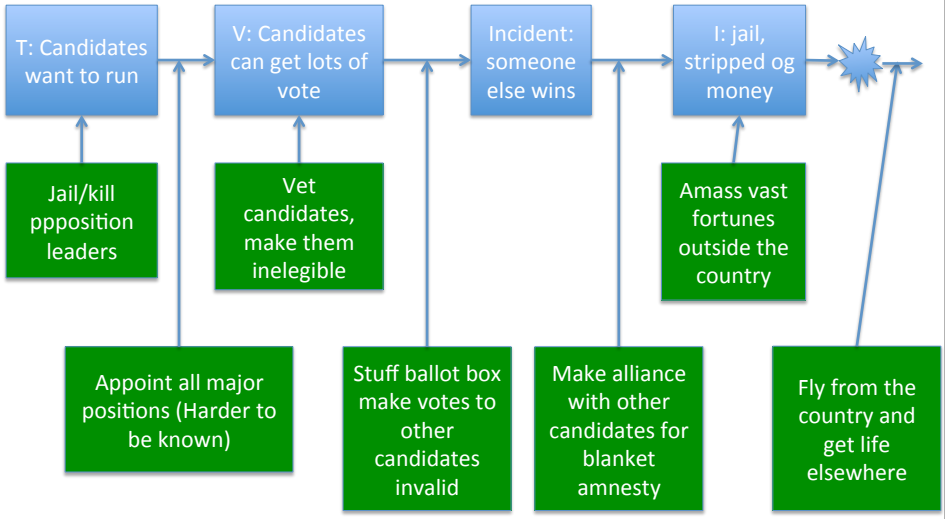
The Russian Election Problem: SRA



UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

The Russian Election Problem: SRA II



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Types of Security Controls

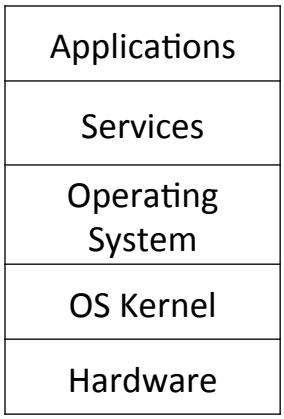
- ***Management Controls***
  - Awareness and Training
  - Security policy and practices
  - Audit and Accountability
  - Risk-assessment
  - Contingency Planning
- ***Technical Controls***
  - Identification and authentication
  - Access and authorization
  - Encryption
  - Digital Signature
  - Privacy-enhancing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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The Mother-Father-Child Problem

- ***Scenario***
  - You are a mother
  - Your asset is your child
  - You can use the father to provide some services
  - You have to balance security and cost
- ***Only one thing is possible for you***
  - Bring the child to school
  - Collect the child from school
- ***What is safer for a child?***
  - Go back home from school alone?
  - Go back with the father?

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Threats

- ***Threats***
  - Going Alone: kidnapping, car accident, being lost, assault by third party (30)
  - Father pick-up: car accident, father is delayed something happen (0)
- ***Threat Agents***
  - Going alone: kidnapper, assault by third parties
  - Father pick-up: father is bad driver, father is kidnapper

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Design your controls

- ***Going Alone***
  - Preventive: body guard, gps (for getting lost), go with other children, training children not to take lift from unknown persons
  - Detective: phone, monitoring (call if at home in time), gos tracker
  - Reactive: phone (for alerting), calling police if gps stray, gun - shoot the wanna-be offender
- ***Father pick up***
  - Preventive: father goes by foot, remember father to pick child up, child to stay at school
  - Detective: check father (call home if in time)
  - Reactive: gun might work (but unlikely to be used)
- ***Risk avoidance:***
  - stay at home

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Design your controls (2015)

- ***Going Alone***
  - Preventive: “school bus”, training (not accept lift from strangers), safe neighboord, pepper spray(?)
  - Detective: GPS tracker, cell phone,
  - Reactive: pepper spray (?)
- ***Father pick up***
  - Preventive: driver course for the father, choose a better father
  - Detective: call the father to check he collect the child in time
  - Reactive: airbag

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Mother, Father, and CHILD II

- ***Going alone…***
  - upon instructions on security measures
    - the child would not accept lift from unknown people (authentication + preventive)
    - He would scream if forced (reactive)
    - If he doesn't show up at planned time mother will react (detective)
  - Trust assumption: on screaming passers-by will react and act
- ***Trustworthy but very costly***
  - Persistent training of "user" (i.e. child)
    - Do not take lift for people you don't know
  - Resistance to social engineering attacks must be trained
    - It doesn't matter it was just a nice old man
  - 100% alert monitoring by mother

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Mother, Father and Child III

- ***The father solution is dirty cheap***
  - Can be quickly authenticated by the child
  - No training of any kind
  - No measure against social engineering
  - No monitoring
- ***The father is trusted by the mother…***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Mother, Father and Child IV

- ***Making "Going alone" trustworty is expensive***
  - Lots of additional security measures
- ***"Father picks up" is trusted and cheap***
  - No security measure
- ***The father is trusted by the mother...***
  - But **almost all** child kidnapping, beating, and killing are done by fathers or close members of the family
  - Only few (8% worldwide) done by "maniacs" unknown to the child
    - U.N. Statistics
- ***A Trusted Component is not something that is secure. It is something against which we plan no defence***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Understanding Risk

- ***Outcome of exercise in 2015 was that almost all students but one considered the going alone the most dangerous thing***
- ***It is very difficult to understand exactly risk***
- ***Understanding quantitative risk is even harder***
  - Prevalence Rate:
    - people with a problem vs total population
  - Incidence Rate
    - New people with problem vs total population at beginning of observation period
  - Relative Risk Ratio (comparing two characteristics):
    - People with a problem AND a characteristic (wrt total of people with characteristics) VS People with a problem AND NOT a characteristic (wrt total of people without characteristics)
  - Odds Ratio (comparing two characteristics):
    - People with a problem AND a characteristic (wrt total of people with characteristics) VS People with a problem (wrt total of people)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Risk in a Nutshell

- ***Prevalence = (Old Bad ⋁ New Bad) / All***
- ***Incidence = New Bad / All***
- ***Relative Risk = compare***
  - (Bad ⋀ P) / (All ⋀ P)
  - (Bad ⋀ not P) / (All ⋀ not P)
- ***Odds Ratio = compare***
  - (Bad ⋀ P) / (Good ⋀ P)
  - (Bad ⋀ not P) / (Good ⋀ not P)
- ***Sometimes we have no data…***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk

- Mother-Father-Child: problems at school
  - Bullies
  - Drug trafficking at school
  - Women repeated abusers
- The rest …
  - Drug trafficking
  - Counterfeiting arrests
  - Homicides
  - Hooligans
  - Human trafficking (immigrants)
  - Mafia related arrests
  - Robberies
  - Terrorism
  - Violent Protesters

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk (2015)

- Mother-Father-Child: problems at school
  - Bullies (2)
  - Drug trafficking at school (2)
  - Women repeated abusers (1)
- The rest …
  - Drug trafficking (2)
  - Counterfeiting arrests (1)
  - Homicides (3)
  - Hooligans (11)
  - Human trafficking (immigrants) (0)
  - Mafia related arrests (0)
  - Robberies (4)
  - Terrorism (0)
  - Violent Protesters (0)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threats Agents I

• ***Mother-Father-Child: problems at school***		
– Bullies (“Choose better school”)	2	
– Drug trafficking at school	1	
– Women repeated abusers (“Choose better father”)	7	
• ***The rest …***		
– Drug trafficking	5	
– Counterfeiting arrests		
– Homicides	2	
– Hooligans	1	
– Human trafficking (immigrants)	2	
– Mafia related arrests	1	
– Robberies	14	
– Terrorism		
– Violent Protesters		
• ***TOTAL CRIMINALS***	***35,000***	***100%***
• ***TOTAL ITALIANS (15-60)***	***35,704,907***	

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threats Agents Ib

• ***Mother-Father-Child: problems at school***		
– Bullies ("Choose better school")	3,061	2.2%
– Drug trafficking at school	92	0.1%
– Women repeated abusers ("Choose better father")	2,176	1.6%
• ***The rest …***		
– Drug trafficking	32,163	23.2%
– Counterfeiting arrests	52,156	37.7%
– Homicides	406	0.3%
– Hooligans	4,793	3.5%
– Human trafficking (immigrants)	728	0.5%
– Mafia related arrests	1,687	1.2%
– Robberies	34,852	25.2%
– Terrorism	50	0.0%
– Violent Protesters	6,220	4.5%
• ***TOTAL CRIMINALS***	***13,8384***	***100%***
• ***TOTAL ITALIANS (15-60)***	***35,704,907***	

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threat Victims I

• ***Mother-Father-Child: problems at school***		
– Death by car accidents ("driving lessons")	8	
– Wounded by car accidents ("ibid.")	10	
– Bullies ("Choose better school")	7	
– Women victimization ("better father")	1	
• ***The rest …***		
– Drug addicts in care		
– Gambling Addicts	1	
– Homicides		
– Robberies	7	
– Thefts (Victims)	8	
• ***TOTAL VICTIMS***	**x**	***100%***
• ***TOTAL ITALIANS (15-60)***	***35,704,907***	

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threat Victims Ib

- ***Mother-Father-Child: problems at school***
  - Death by car accidents ("driving lessons") 1,639 0,1%
  - Wounded by car accidents ("ibid.") 49,132 2,6%
  - Bullies ("Choose better school") 3,061 2.2%
  - Women victimization ("better father") 207,784 11,1%
- ***The rest …***
  - Drug addicts in care 164,993 8,8%
  - Gambling Addicts 6,804 0,4%
  - Homicides 406 0,0%
  - Robberies 34,852 1,9%
  - Thefts (Victims) 1,407,268 75,0%
- ***TOTAL VICTIMS*** **1,875,939** ***100%***
- ***TOTAL ITALIANS (15-60)*** ***35,704,907***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threat Victims II

- ***Mother-Father-Child: problems at school***
  - Death by car accidents ("driving lessons") 1,639 0.6% ~~0,1%~~
  - Wounded by car accidents ("ibid.") 49,132 18.8% ~~2,6%~~
  - Bullies ("Choose better school") 3,061 1.2% ~~2.2%~~
  - Women victimization ("better father") 207,784 79.4% ~~11.1%~~
- ***TOTAL CASES OF CONCERN*** **261,616** 100%
- ***The rest …***
  - Drug addicts in care 164,993 8,8%
  - Gambing Addicts 6,8040,4%
  - Homicides 406 0,0%
  - Robberies 34,852 1,9%
  - Thefts (Victims) 1,407,268 75,0%
- ***TOTAL VICTIMS*** 1,875,939 ***100%***
- ***TOTAL ITALIANS (15-60)*** ***35,704,907***
  - Couples without kids 4,968,683
  - Couples with kids+Mother+kids 10,536,814

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threat Victims III

- ***The "find a better partner" problem in 2014***
  - Beating
  - Domestic abuse
  - Severe injuries
  - Sexual assault
  - Stalking
  - Threatened
- ***Tot Victims*** **x** ***100%***
- ***Tot Italian W (15-60)*** **17,954,696**

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – Threat Victims IIIb

- ***The "find a better father" problem***

– Beating	16,319	7,9%
– Domestic abuse	13,774	6,6%
– Severe injuries	70,284	33,8%
– Sexual assault	4,471	2,2%
– Stalking	12,492	6,0%
– Threatened	90,444	43,5%
Tot VICTIMS	**207,784**	***100%***
Tot Italian W (15-60)	**17,954,696**	

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – MFC - I

- ***The original problem:***
  - Total cases from 1974 to 2014 in Italy
  - Estimated cases of disappearence for Italian minors
  - Proportionally from known Italian cases (1,186)
    - 32% no cause recorded < 2007
    - Foreign minors data is unrealiable as they give fake names
- ***What happened to Italian disappeared minors?***
  - Run away from shelter
  - Run away from home 3
  - Kidnapped by relative 8
  - Victims of crime 4
  - Lost (psychological problems)
- ***TOTAL DISAPPEARED***
- ***TOTAL MINORS in 2014 (4-17)*** **17,954,696**

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Estimating Risk – MFC - Ibis

- ***The original problem:***
  - Total cases from 1974 to 2014 in Italy
  - Estimated cases of disappearence for Italian minors
  - Proportionally from known Italian cases (1.186)
    - 32% no cause recorded < 2007
    - Foreign minors data is unrealiable as they give fake names
- ***What happened to Italian disappeared minors?***

– Run away from shelter	671	38,1%
– Run away from home	578	32,8%
– Kidnapped by relative	490	27,8%
– Victims of crime	21	1,2%
– Lost (psychological problems)	1	0,1%
TOTAL DISAPPEARED	***1,761***	***100%***
TOTAL MINORS in 2014 (4-17)	**17,954,696**	

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Suggested Exercise

- ***Principles of Epidemiology***
  - http://health.mo.gov/training/epi/index.html
- ***Textbook***
  - Managing Risk in Information Systems.
    - Chapter 2 – "Managing Risk: Threats, Vulnerabilities, and Exploits"
  - Next three exercises are on Google Classroom

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Exercise 1 – Estimate Various Risks

- ***Given the data on Threat Agents (Slide I.bis) and Threat Victims (Slides I.bis) for criminal records in Italy***
  - Census 2011
- ***For any of the item below see what would be relevant rates for your scenario (eg a relevant P), what you can compute and what you can't compute, etc.***
  - Prevalence Rate (for a given period, eg the census year)
    - (Old Bad $\vee$ New Bad) / All
  - Incidence Rate (for given period)
    - New Bad / All
  - Relative Risk = compare
    - (Bad $\wedge$ P) / (All $\wedge$ P)
    - (Bad $\wedge$ not P) / (All $\wedge$ not P)
  - Odds Ratio = compare
    - (Bad $\wedge$ P) / (Good $\wedge$ P)
  - (Bad $\wedge$ not P) / (Good $\wedge$ not P)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Exercise 2 – "Better Father"

- ***Given the data on threat victims (Slides II to III.bis)***
  - Census 2011
- ***For any of the item below see what you can compute and what you can't compute, what would be relevant P for you, etc.)***
  - Prevalence Rate (for a given Period eg the census year)
    - (Old Bad ⋁ New Bad) / All
  - Incidence Rate (for a given period)
    - New Bad / All
  - Relative Risk = compare
    - (Bad ⋀ P) / (All ⋀ P)
    - (Bad ⋀ not P) / (All ⋀ not P)
  - Odds Ratio = compare
    - (Bad ⋀ P) / (Good ⋀ P)
    - (Bad ⋀ not P) / (Good ⋀ not P)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Exercise 3 - MFC

- ***Given the data on MFC (Slides I.bis)***
  - Census 2011
- ***For any of the item below see what would be relevant rates for your scenario (eg a relevant P), what you can compute and what you can't compute, etc.***
  - Prevalence Rate
    - (Old Bad ⋁ New Bad) / All
  - Incidence Rate
    - New Bad / All
  - Relative Risk = compare
    - (Bad ⋀ P) / (All ⋀ P)
    - (Bad ⋀ not P) / (All ⋀ not P)
  - Use relative risk when you know the entire population (or a have a good idea about it)
  - Odds Ratio = compare
    - (Bad ⋀ P) / (Good ⋀ P)
    - (Bad ⋀ not P) / (Good ⋀ not P)
  - Use odds ration when you don't know the whole population (i.e. Bad+Good = sample(All))