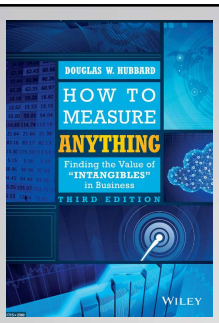
ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

EVOLUZIONE DEL RISK MANAGEMENT
E
RISK QUANTIFICATION

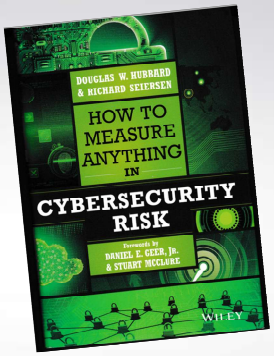
Alberto Piamonte
ISACA Roma

1

1



Più di 150.000 copie vendute, trad. in 8 lingue, testo universitario . . . .



- Si parte da una indagine sui metodi di analisi dei rischi IT che ha coinvolto circa 200 esperti del settore
- Si fa il punto teorico/pratico sullo stato dell'arte
- 1-2 giugno un corso sulle nuove metodologie organizzato da ISACA CHICAGO, con la partecipazione degli autori (*e dal sottoscritto !*)

ISACA Rome Chapter

5 giugno 2020

2

2

Agenda

- Approccio attuale al cybersecurity risk: *non è una soluzione ma rappresenta il problema*
- Cambio di paradigma: *da qualitativo a quantitativo*
- La soluzione: *usare strumenti statistici consolidati*
  - «in teoria»
  - «in pratica»
- Esempi Pratici

ISACA Rome Chapter

3

The Biggest Cybersecurity Risk

Question: What is Your Single Biggest Risk in Cybersecurity?

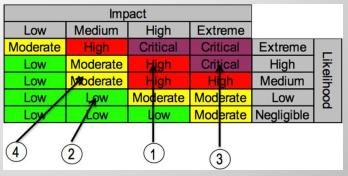
Answer: How You Measure Cybersecurity Risk

ISACA Rome Chapter

4

Current Solution

- Here are some risks plotted on a "typical heat map".
- Suppose **mitigation costs** were:
  - Risk 1: $725K – High
  - Risk 2: $95K – Low
  - Risk 3: $2.5M – Critical
  - Risk 5: $375K – Moderate
- What mitigations should be funded and what is the priority among these?



5

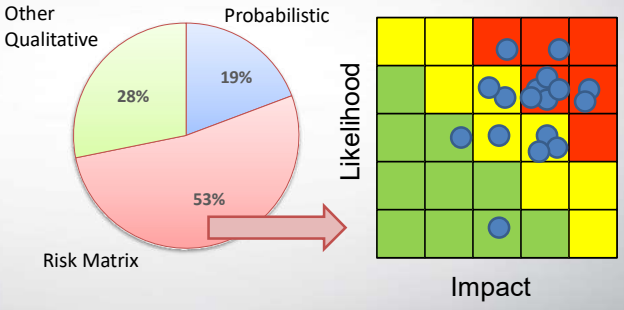
Current Solutions

- Most standards and certification tests promote risk analysis as a type of ordinal scoring method
- The "Risk Rating Methodology" on OWASP.org states:
- "Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the "**likelihood**". At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. *Generally, identifying whether the likelihood is low, medium, or high is sufficient*."

6

The Current Most Popular Method

Share of Methods Used in Cybersecurity Risk Assessment



Source: HDR 2015 Survey of Cybersecurity Risk Methods (173 Responses)

7

Can Analysis or Expertise be a "Placebo button"?

Hubbard, da riconosciuto esperto di tecnica delle decisioni, ipotizza che :

- **In short, we should *assume* increased confidence from analysis is a "placebo button."**

Placebo button is a push-button or other control which has apparent functionality but has no physical effect when pressed.
- Office thermostats
- Walk buttons
- London Underground train door buttons
- …

the **illusion of control** psychological effect

- **Real benefits have to be measured.**

8

What the Research Says

- There is mounting evidence against (and none for) the effectiveness of "risk scores" and "risk matrices."
- Fundamental misconceptions about statistical inference may keep some from adopting quantitative methods.
- Experts using even naïve statistical models outperform human experts who do not.

Note: **Every improvement we are about to has already been adopted in several cybersecurity environments**.

ISACA Rome Chapter

5 giugno 2020

9

9

Ma qualcuno ha continuato la ricerca di soluzioni migliori . . .

Fortunately, other researchers have run experiments[25] showing that experts can be trained to be better at estimating probabilities by applying a battery of estimation tests, giving the experts a lot of quick, repetitive, clear feedback along with training in techniques for improving subjective probabilities. In short, researchers discovered that *assessing uncertainty is a general skill that can be taught with a measurable improvement*. That is, when calibrated cybersecurity experts say they are 85% confident that a major data breach will occur in their industry in the next 12 months, there really is an 85% chance it will occur.

ISACA Rome Chapter

5 giugno 2020

10

10

The human brain is a relatively inefficient device for noticing, selecting, categorizing, recording, retaining, retrieving, and manipulating information for inferential purposes. Why should we be surprised at this?[19]

Tools for improving the Human Component

Our goal is actually to elevate the expert. We want to treat the cybersecurity expert as part of the risk assessment system. Like a race car or athlete, they need to be monitored and fine-tuned for maximum performance. The expert is really a type of measurement instrument that can be "calibrated" to improve its output.

Subjective Probability Component

A critical component of risk analysis is cybersecurity experts' assessment of the likelihoods of events, like cybersecurity breaches, and the potential costs if those events occur. Whether they are using explicit probabilities or nonquantitative verbal scales, they need to judge whether one kind of threat is more likely than another. Since we will probably have to rely on the expert at some level for this task, we need to consider how the experts' skill at this task can be measured and what those measurements show.

ISACA Rome Chapter

11

Imparimo a «scomporre» il problemi

Doing the math explicitly, even if the inputs themselves were subjective estimates, removes a source of error. If we want to estimate the monetary impact of a denial of service attack on a given system, we can estimate the duration, the number of people affected, and the cost per unit of time per person affected. Once we have these estimates, however, we shouldn't then just *estimate* the product of these values—we should *compute* the product. Since, as we have shown earlier, we tend to make several errors of intuition around such calculations, we would be better off just doing the math in plain sight.

ISACA Rome Chapter

12

Una premessa: Le possibili scale di misura

La misurazione, nel senso più ampio, consiste nell'attribuzione di numeri a oggetti o eventi seguendo determinate regole. Il fatto che si possano assegnare dei numeri seguendo regole differenti porta a differenti tipi di scala e differenti tipi di misurazione" (S. S. Stevens, 1946)

I possibili tipi di scale di misura definiti da Stevens sono:

- Scala nominale
- Scala ordinale
- Scala ad intervalli equivalenti
- Scala a rapporti equivalenti

ISACA Rome Chapter

13

Le scale di misura

Università degli Studi di Padova
Facoltà di Psicologia
L4, Psicometria, Modulo B
Le scale di misura

Informazioni	Scala	Caratteristiche	Operazioni
Qualitative	**Nominale**	Categorie (nessun ordine o verso) Definisce una tassonomia.	**Conteggio**
	Ordinale	Categorie (posizione in una graduatoria)	I numeri associati alle classi di equivalenza esprimono unicamente la relazione d'ordine esistente tra le classi, sono dei semplici codici che servono a distinguere e **ordinare, max, min**, ma non ci dicono nulla sulla grandezza delle distanze tra le classi di equivalenza. **Algebriche ?** 🚫
Quantitative	**Intervalli equivalenti**	Differenza tra misure ma non esiste un reale valore 0, **°C, °F** e fanno riferimento ad un'altra scala (°).	**Differenza** tra i numeri associati ai diversi punti della scala
	Rapporti equivalenti	Differenza tra misure ma esiste un reale valore 0, **K**	**Algebriche** 👍

ISACA Rome Chapter

14

Un errore abbastanza comune

Frequenza annua (P)

		€ 10	€ 100	€ 1,000	€ 10,000	€ 100,000	€ 1,000,000
6	100	€ 1,000	€ 10,000	€ 100,000	€ 1,000,000	€ 10,000,000	€ 100,000,000
5	10	€ 100	€ 1,000	€ 10,000	€ 100,000	€ 1,000,000	€ 10,000,000
4	1	€ 10	€ 100	€ 1,000	€ 10,000	€ 100,000	€ 1,000,000
3	0.1	€ 1	€ 10	€ 100	€ 1,000	€ 10,000	€ 100,000
2	0.01	€ 0.10	€ 1.00	€ 10	€ 100	€ 1,000	€ 10,000
1	0.001	€ 0.01	€ 0.10	€ 1	€ 10	€ 100	€ 1,000

6	3.5	4.0	4.5	5.0	5.5	6.0
5	3.0	3.5	4.0	4.5	5.0	5.5
4	2.5	3.0	3.5	4.0	4.5	5.0
3	2.0	2.5	3.0	3.5	4.0	4.5
2	1.5	2.0	2.5	3.0	3.5	4.0
1	1.0	1.5	2.0	2.5	3.0	3.5

$$R = \frac{P + I}{2}$$

		1	2	3	4	5	6
6	100.00	6	12	18	24	30	36
5	10.00	5	10	15	20	25	30
4	1.00	4	8	12	16	20	24
3	0.10	3	6	9	12	15	18
2	0.01	2	4	6	8	10	12
1	0.001	1	2	3	4	5	6
		€ 10	€ 100	€ 1,000	€ 10,000	€ 100,000	€ 1,000,000

Indice Rischio Normalizzato (errato)

6	1.7	2.6	3.4	4.3	5.1	6.0
5	1.6	2.4	3.2	4.0	4.8	5.7
4	1.4	2.2	2.9	3.7	4.4	5.2
3	1.3	1.7	2.1	2.6	3.0	3.5
2	1.1	1.4	1.7	2.0	2.3	2.6
1	1.0	1.1	1.3	1.4	1.5	1.7
	1	2	3	4	5	6

ISACA Rome Chapter

15

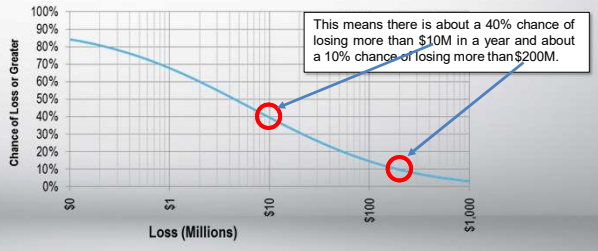
15

What if We Could *Actually Measure Risk* in Cybersecurity?

What if we could measure risk more like an actuary – "The probability of losing more than $10 million due to security incidents in 2021 is 16%"

What if we could prioritize security investments based on a "Return on Mitigation"?

	Expected Loss/Yr	Cost of Control	Control Effectiveness	Return on Control	Action
DB Access	$24.7M	$800K	95%	2,832%	Mitigate
Physical Access	$2.5M	$300K	99%	727%	Mitigate
Data in Transit	$2.3M	$600K	95%	267%	Mitigate
Network Access Control	$2.3M	$400K	30%	74%	Mitigate
File Access	$969K	$600K	90%	45%	Monitor
Web Vulnerabilities	$409K	$800K	95%	-51%	Track
System Configuration	$113K	$500K	100%	-77%	Track



ISACA Rome Chapter

5 giugno 2020

17

17

Why Not Better Methods?

- Cybersecurity is too complex or lacks sufficient data for quantitative analysis…
- Probabilities can't be used explicitly because …

- **Remember, softer methods never *alleviate* a lack of data, complexity, rapidly changing environments or unpredictable human actors…they can only *obscure* it.**

ISACA Rome Chapter

18

Pag. 15 del testo . . .

- **There is no evidence that the types of scoring and risk matrix methods widely used in cybersecurity improve judgment.**
- On the contrary, there is evidence these methods add noise and error to the judgment process. One researcher——Tony CoX—-goes as far as to say they can be "worse than random."
- Any appearance of "working" is probably a type of "analysis placebo." That is, a method may make you feel better even though the activity provides no measurable improvement in estimating risks (or even adds error).
- There is overwhelming evidence in published research that **quantitative, probabilistic methods are effective.**
- Fortunately, most cybersecurity experts seem willing and able to adopt better quantitative solutions. But common misconceptions held by some—including misconceptions about basic statistics—create some obstacles for adopting better methods.

ISACA Rome Chapter

19

Pag. 16

- **It is possible to greatly improve on the existing methods.**
  Many aspects of existing methods have been measured and found wanting. This is not acceptable for the scale of the problems faced in cybersecurity.
- **Cybersecurity can use the same quantitative language of risk analysis used in other problems.**
  As we will see, there are plenty of fields with massive risk, minimal data, and profoundly chaotic actors that are regularly modelled using traditional mathematical methods. We do not need to reinvent terminology or methods from other fields that also have challenging risk analysis problems.
- **Methods exist that have already been measured to be an improvement over expert intuition**.
  This improvement exists even when methods are based, as are the current methods, on only the subjective judgment of cybersecurity experts.
- **These improved methods are entirely feasible.**
  We know this because it has already been done. One or both authors have had direct experience with using every method described in this book in real-world corporate environments. The methods are currently used by cybersecurity analysts with a variety of backgrounds.
- **You can improve further on these models with empirical data.**
  You have more data available than you think from a variety of existing and newly emerging sources. Even when data is scarce, mathematical methods with limited data can still be an improvement on subjective judgment alone. Even the risk analysis methods themselves can be measured and tracked to make continuous improvements.

ISACA Rome Chapter

20

Una concetto fondamentale

Definition of Measurement

Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

The practical differences between this definition and the most popular definitions of measurement are enormous.

Not only does a true measurement not need to be infinitely precise to be considered a measurement, but the lack of reported error—implying the number is exact—can be an indication that empirical methods, such as sampling and experiments, were not used (i.e., it's not really a measurement at all).

Measurements that would pass basic standards of scientific validity would report results with some specified degree of uncertainty, such as, "**There is a 90% chance that an attack on this system would cause it to be down somewhere between 1 and 8 hours**."

…. A measurement is, ultimately, **just information**, and there is a rigorous theoretical construct for information. field called "information theory", was developed in the 1940s by Claude Shannon, an American electrical engineer and mathematician.

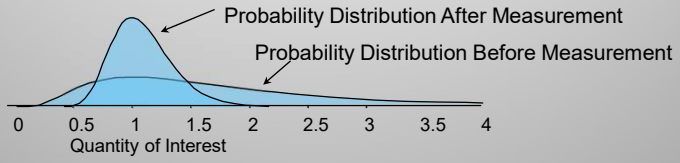
ISACA Rome Chapter

21

The Concept of Measurement

It's not a point value.

- Measurement: a quantitatively expressed reduction in uncertainty based on observation.
- You can quantify your current uncertainty – additional observations reduce it.
- Even marginal reductions in uncertainty can be extremely valuable.



ISACA Rome Chapter

22

La matematica «dell'incertezza»

Doing "Uncertainty Math"

Using ranges to represent your uncertainty instead of unrealistically precise point values clearly has advantages. When you allow yourself to use ranges and probabilities, you don't really have to assume anything you don't know for a fact. But precise values have the advantage of being simple to add, subtract, multiply, and divide in a spreadsheet. If you knew each type of loss exactly it would be easy to compute the total loss. Since we only have ranges for each of these, we have to use probabilistic modeling methods to "do the math."

So how do we add, subtract, multiply, and divide in a spreadsheet when we have no exact values, only ranges? Fortunately, there is a practical, proven solution, and it can be performed on any modern personal computer—the "Monte Carlo" simulation method. A Monte Carlo simulation uses a computer to generate a large number of scenarios based on probabilities for inputs. For each scenario, a specific value would be randomly generated for each of the unknown variables. Then these specific values would go into a formula to compute an output for that single scenario. This process usually goes on for thousands of scenarios.

ISACA Rome Chapter

24

Metodo Monte Carlo

(WikiPedia)

- Il **metodo Monte Carlo** è un'ampia classe di metodi computazionali basati sul campionamento casuale per ottenere risultati numerici. Può essere utile per superare i problemi computazionali legati ai test esatti (ad esempio i metodi basati sulla distribuzione binomiale e calcolo combinatorio, che per grandi campioni generano un numero di permutazioni eccessivo).
- Il metodo è usato per trarre stime attraverso simulazioni. Si basa su un algoritmo che genera una serie di numeri tra loro non correlati, che seguono la distribuzione di probabilità che si suppone abbia il fenomeno da indagare.
- La simulazione Monte Carlo calcola una serie di realizzazioni possibili del fenomeno in esame, con il peso proprio della probabilità di tale evenienza, cercando di esplorare in modo denso tutto lo spazio dei parametri del fenomeno. Una volta calcolato questo campione casuale, la simulazione esegue delle 'misure' delle grandezze di interesse su tale campione. La simulazione Monte Carlo è ben eseguita se il valore medio di queste misure sulle realizzazioni del **sistema converge al valore vero.**
- Le sue origini risalgono alla metà degli anni 40 nell'ambito del Progetto Manhattan. I formalizzatori del metodo sono Enrico Fermi, John von Neumann e Stanisław Marcin Ulam[1], il nome Monte Carlo fu inventato in seguito da Nicholas Constantine Metropolis in riferimento al noto casinò situato a Monte Carlo, nel Principato di Monaco, l'uso di tecniche basate sulla selezione di numeri casuali è citato già in un lavoro di Lord Kelvin del 1901 ed in alcuni studi di William Sealy Gosset[1].
- L'algoritmo Monte Carlo è un metodo numerico che viene utilizzato per trovare le soluzioni di problemi matematici che possono avere molte variabili e che non possono essere risolti facilmente, per esempio il calcolo integrale. L'efficienza di questo metodo aumenta rispetto agli altri metodi quando la dimensione del problema cresce.
- Un primo esempio di utilizzo del metodo Monte Carlo è rappresentato dall'esperimento dell'ago di Buffon e forse il più famoso utilizzo di tale metodo è quello di Enrico Fermi, quando nel 1930 usò un metodo casuale per problemi di trasporto neutronico[1].

ISACA Rome Chapter

5 giugno 2020

25

25

Model Now !

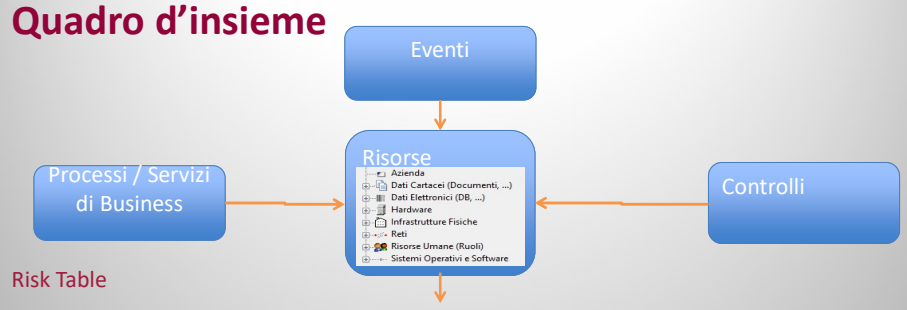
ISACA Rome Chapter

5 giugno 2020

26

26

Quadro d'insieme



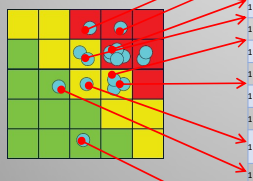
Risk Table

Processi			Impatto	Asset		Minaccia	Probabilità	Impatto		
Proc1	Proc2	Proc3	I Imp	Ast	CL_Thr		PI	RP	II	RI
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	1. Forza maggiore	Effetti di catastrofi ambientali	4.00	1.00	4.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	1. Forza maggiore	Incendi	3.00	2.00	4.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	1. Forza maggiore	Scariche atmosferiche (Fulmini, sovratensioni, ecc.)	3.00	1.00	4.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	4. Problemi tecnici	Guasto nel sistema interno di alimentazione	5.00	3.00	4.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	5. Atti deliberati	Accesso fisico non autorizzato ai locali	2.00	2.00	4.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	1. Forza maggiore	Malfunzionamento dei sistemi IT	4.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	2. Organizzative	Materiale accessorio / supporti non disponibili	2.00	2.00	2.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	2. Organizzative	Risorse mancanti o non adeguate	6.00	3.00	2.00	4.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	3. Errori umani	Dismissione di supporti informatici contenenti dati senza adeguate garanzie	5.00	1.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	3. Errori umani	Utilizzo improprio dei sistemi IT	6.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	5. Atti deliberati	Furto di apparecchiature IT mobili	3.00	3.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	5. Atti deliberati	Manomissione o distruzione di apparati o accessori IT	5.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	5. Atti deliberati	Utilizzo non autorizzato di sistemi IT	4.00	1.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Risorse Umane (Ruoli)	1. Forza maggiore	Epidemie	4.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Risorse Umane (Ruoli)	1. Forza maggiore	Indisponibilità di personale	4.00	1.00	2.00	3.00

27

A Simple "One-For-One Substitution"

- Each "Dot" on a risk matrix can be better represented as a row on a table like this
- Quindi partendo da una struttura logica sostanzialmente eguale ad una utilizzata per la Risk Matrix posso procedere all'elaborazione «statistica» degli eventi identificati
- Come ?



Processi			Impatto	Asset		Minaccia	Probabilità	Impatto		
Proc1	Proc2	Proc3	I Imp	Ast	CL_Thr		PI	RP	II	RI
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	1. Forza maggiore	Effetti di catastrofi ambientali	4.00	1.00	4.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	1. Forza maggiore	Incendi	3.00	2.00	4.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	1. Forza maggiore	Scariche atmosferiche (Fulmini, sovratensioni, ecc.)	3.00	1.00	4.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	4. Problemi tecnici	Guasto nel sistema interno di alimentazione	5.00	3.00	4.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 1 - Gestione rete vendita	4.00	Infrastrutture Fisiche	5. Atti deliberati	Accesso fisico non autorizzato ai locali	2.00	2.00	4.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	1. Forza maggiore	Malfunzionamento dei sistemi IT	4.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	2. Organizzative	Materiale accessorio / supporti non disponibili	2.00	2.00	2.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	2. Organizzative	Risorse mancanti o non adeguate	6.00	3.00	2.00	4.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	3. Errori umani	Dismissione di supporti informatici contenenti dati senza adeguate garanzie	5.00	1.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	3. Errori umani	Utilizzo improprio dei sistemi IT	6.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	5. Atti deliberati	Furto di apparecchiature IT mobili	3.00	3.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	5. Atti deliberati	Manomissione o distruzione di apparati o accessori IT	5.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Hardware	5. Atti deliberati	Utilizzo non autorizzato di sistemi IT	4.00	1.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Risorse Umane (Ruoli)	1. Forza maggiore	Epidemie	4.00	2.00	2.00	5.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Risorse Umane (Ruoli)	1. Forza maggiore	Indisponibilità di personale	4.00	1.00	2.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Risorse Umane (Ruoli)	2. Organizzative	Mancanza o insufficienza di formazione / addestramento	5.00	3.00	2.00	3.00
1 - Principali	1. 1 - Vendite	1. 1. 2 - Gestione Promoter	2.00	Software	2. Organizzative	Sicurezza non integrata nello sviluppo dei sistemi informatici / applicativi	6.00	2.00	2.00	4.00

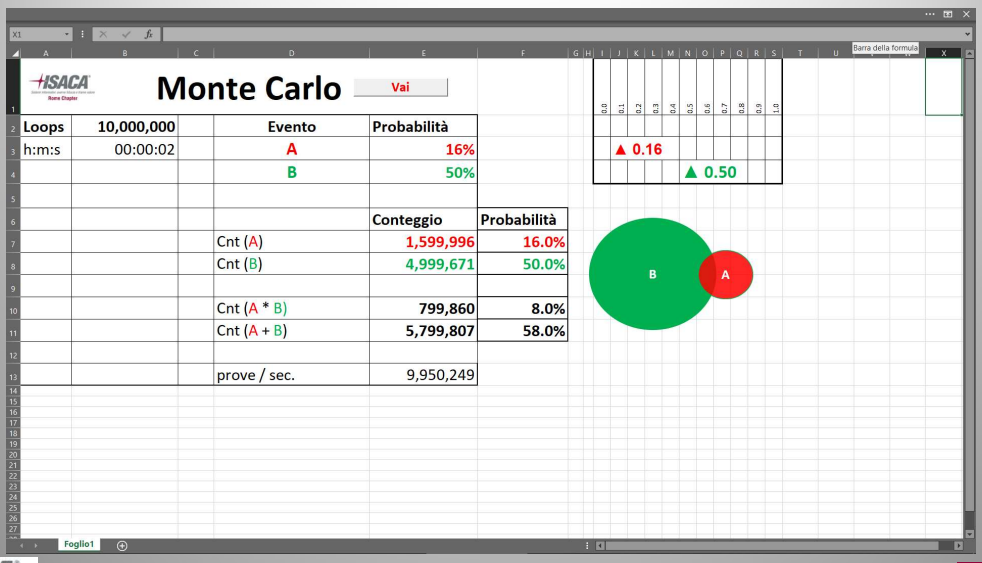
28

Sarebbe bello poter simulare le varie combinazioni per ottenere dati statistici del rischio

Excel : Generazione N. casuali

29

Schermo esempio excel

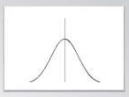


30

Simuliamo un evento specificando:

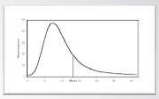
Probabilità acc.
Intensità

Probabilità annua : Distribuzione **normale**



P

Impatto: Distribuzione **log - normale**
Casuale : 90% tra ($L_{inferiore}$ e $L_{superiore}$), solo valori positivi e possibili valori molto alti



L_i - L_s

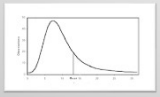
Formula excel :
=SE (CASUALE() < P;
INV.LOGNORM.N(CASUALE();(LN(L_i)+LN(L_s))/2;(LN(L_s)-LN(L_i))/3.29);
0)

Ogni volta che calcoliamo la formula otteniamo un valore casuale, che ha le caratteristiche richieste.
(compreso lo 0 : non accaduto)
L'insieme dei valori ottenuti è, anche lui, una distribuzione e quindi . . . .

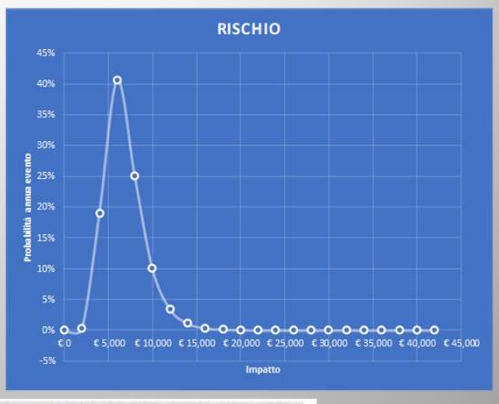
ISACA Rome Chapter

La matematica dell'incertezza

Probabilità



Impatto

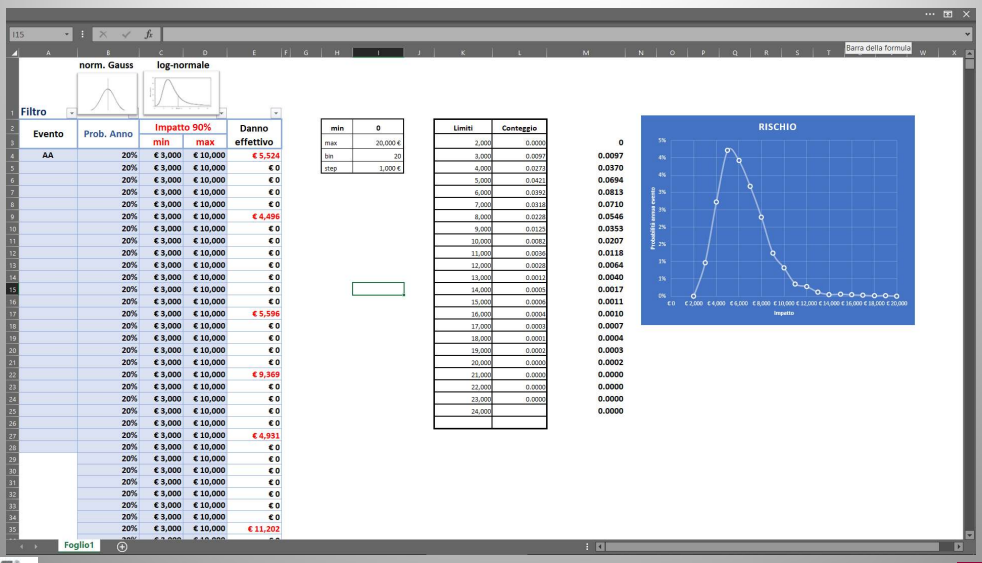


Definition of Measurement

Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

ISACA Rome Chapter

Esempio excel



ISACA Rome Chapter

33

Risk Table (parziale)

1. Ripetere la simulazione n volte (ad es.10.000 volte)
2. Ad ogni «anno» sommare i danni degli eventi avvenuti
3. Registrarne il valore
4. Creare il grafico

norm. Gauss log-normale

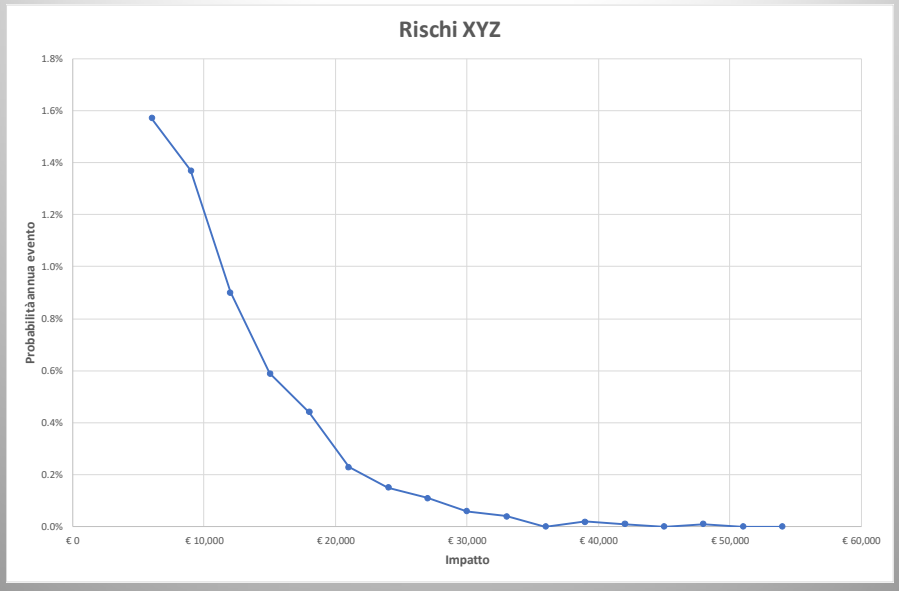
Filtro

Evento	Prob. Anno	Impatto 90% min	Impatto 90% max	Danno effettivo
AA	6%	€ 398	€ 2,512	€ 0
AB	6%	€ 398	€ 2,512	€ 0
AC	10%	€ 398	€ 2,512	€ 0
EG	3%	€ 3,631	€ 22,909	€ 0
RT	7%	€ 3,631	€ 22,909	€ 0
MY	11%	€ 398	€ 2,512	€ 0
MA	6%	€ 832	€ 5,248	€ 2,120
RM	10%	€ 575	€ 3,631	€ 0
DS	12%	€ 398	€ 2,512	€ 1,217
US	4%	€ 398	€ 2,512	€ 0
FM	10%	€ 398	€ 2,512	€ 0
MD	5%	€ 398	€ 2,512	€ 0
UN	5%	€ 398	€ 2,512	€ 1,743
EP	8%	€ 398	€ 251,101	€ 0
IP	1%	€ 832	€ 5,248	€ 0
MF	10%	€ 832	€ 5,248	€ 0
SN	4%	€ 575	€ 3,631	€ 0
SS	5%	€ 398	€ 2,512	€ 0
MD	2%	€ 575	€ 3,631	€ 0
MP	2%	€ 398	€ 2,512	€ 0
UA	13.00%	€ 398	€ 2,512	€ 0
UU	18.00%	€ 3,631	€ 22,909	€ 0
DM	18.00%	€ 3,631	€ 22,909	€ 7,994
NG	16.00%	€ 3,631	€ 22,909	€ 7,416
		Tot. / anno		€ 20,491

anno	Totale danno
1	€ 17,460
2	€ 5,447
3	€ 1,098
4	€ 1,726
5	€ 2,776
6	€ 0
7	€ 898
8	€ 685
9	€ 6,811
10	€ 0
11	€ 1,373
12	€ 19,342
13	€ 15,203
14	€ 726
15	€ 679
16	€ 620
17	€ 1,785
18	€ 2,339
19	€ 2,151
20	€ 53,294
21	€ 0
22	€ 852
23	€ 1,602
24	€ 20,491

ISACA Rome Chapter

34



35

Anche il concetto di rischio accettabile si evolve e diviene :

Curva statistica di accettabilità

36

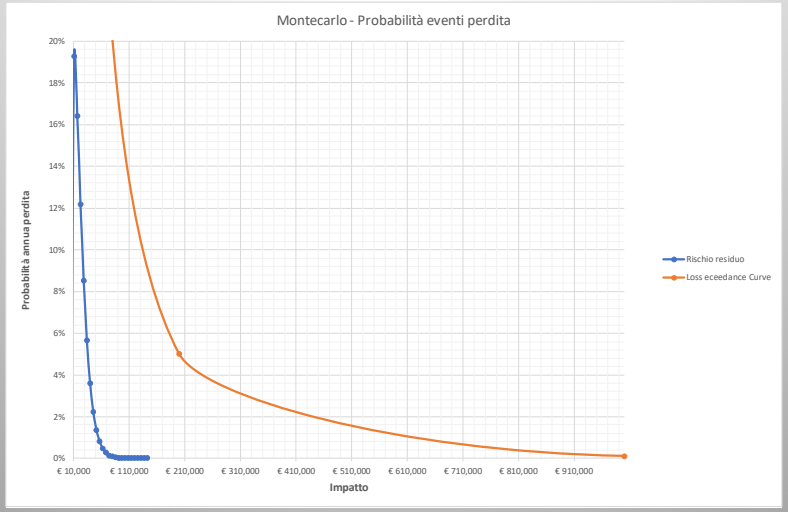
€ 10,000	10.0%
€ 25,000	3.5%
€ 50,000	1.5%
€ 500,000	0.5%

Analista:	Accetterebbe una probabilità del 10% all'anno di perdere più di $ 5 milioni a causa di un rischio di sicurezza informatica?
Dirigente:	preferisco non accettare alcun rischio !
Analista:	anch'io, ma già ora accetta rischi simili in altre aree. Potrebbe sempre spendere di più per ridurre i rischi, ma ovviamente c'è un limite.
Dirigente :	vero. Sarei disposto ad accettare un anno di probabilità del 10% di una perdita di $ 5 milioni.
Analista:	che ne dice di una probabilità del 20% di perdere più di $ 5 milioni in un anno?
Dirigente :	Non spingiamoci troppo avanti. Restiamo con il 10%.
Analista:	fantastico, 10% quindi. Ora, quante possibilità sarebbe disposto ad accettare per una perdita molto più grande, come $ 50 milioni o più? Potrebbe andare un 1%?
Dirigente:	penso che sia troppo. Potrei accettare una probabilità dell'1% all'anno di accettare con una perdita di $ 25 milioni

ISACA Rome Chapter

37

Loss exceedence curve

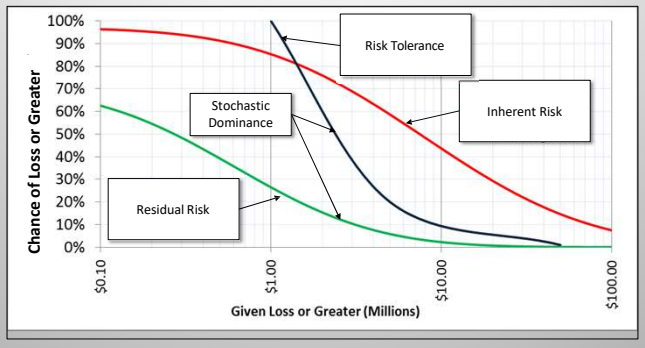


ISACA Rome Chapter

38

Loss Exceedance Curves: Before and After

- How do we show the risk exposure after applying available mitigations?



ISACA Rome Chapter

39

In teoria il metodo sembra funzionare, e la qualità dei dati adesso dipende dalla qualità delle stime.

Vediamo come migliorarla

ISACA Rome Chapter

40

Per migliorare le stime :

- **scomporne le componenti**

Per essere efficace una scomposizione deve essere:

- **chiara**
- **osservabile**
- **utile**

- Scale di misura
- Processi di Business
  - Impatti
  - Risorse utilizzate
- Risorse
  - Eventi
  - Conseguenze RID
  - Probabilità eventi
  - Controlli applicabili
    - Livello di implementazione
- Controllo
  - Standard (ISO, NIST, CSF, ecc.)
  - Efficacia
    - RID
    - Riduzione Probabilità
    - Riduzione impatti
  - Costo

ISACA Rome Chapter

41

~~Definiamo~~ Concordiamo le scale di misura

Frequenza annua

indice	Frequenza annua
1	0.01
2	0.08
3	0.5
4	3
5	20.
6	120.00

Impatto

indice	Impatto
1	€ 1,000
2	€ 6,310
3	€ 39,811
4	€ 251,189
5	€ 1,584,893
6	€ 10,000,000

Rischio

indice	ALE
1	€ 12
2	€ 478
3	€ 19,019
4	€ 757,149
5	€ 30,142,637
6	€ 1,200,000,000

Rapporti equivalenti

Ordinale

Posso eseguire operazioni algebriche sui rischi: somme, differenze, %, ecc. e, se necessario, esprimerle in termini di indice di rischio

ISACA Rome Chapter

42

~~Valutazione~~ Scomposizione e valutazione di Impatto sui processi

Dimensione	Perdita di :			
	Riservatezza	Integrità	Disponibilità	…
Perdita di Produttività	1-6	1-6	1-6	
Risposta all'evento	1-6	1-6	1-6	
Perdita di Competitività	1-6	1-6	1-6	
Multe e penali	1-6	1-6	1-6	
Reputazionale	1-6	1-6	1-6	
…	…	…	…	
Max	1-6	1-6	1-6	

ISACA Rome Chapter

5 giugno 2020

43

43

Risorse utilizzate (direttamente / indirettamente)

Risorse
Azienda
Dati Cartacei (Documenti, …)
Dati Elettronici (DB, …)
Hardware
Infrastrutture Fisiche
Reti
Umane (Ruoli)
Sistemi IT
Software
Servizi esterni
…

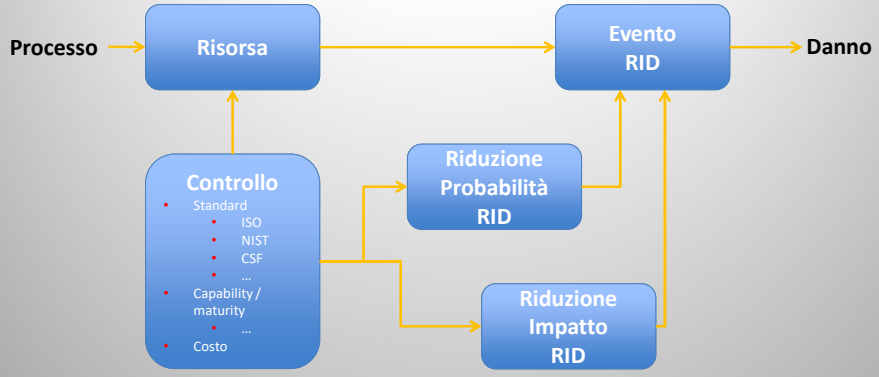
ISACA Rome Chapter

5 giugno 2020

44

44

Minacce e controlli



ISACA Rome Chapter

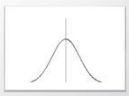
5 giugno 2020

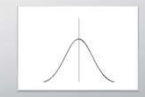
45

45

Controlli

- Controllo
  - Applicabilità
    - Risorsa
    - Minaccia
  - Standard (ISO, NIST, CSF, ecc.)
  - Strumento
  - Efficacia
    - RID
    - Riduzione Probabilità
    - Riduzione impatti
  - Costo





ISACA Rome Chapter

5 giugno 2020

46

46

Possibilità di analisi e confronto «documentato»

- «Filtrando» la Risk Table posso analizzare **statisticamente** per :
  - Processi / servizi
  - Asset
  - Minacce
  - ROSI
  - ….
- Valutare statisticamente soluzioni alternative
  - Nuove soluzioni tecnologiche
  - Nuovi servizi
  - ….

ISACA Rome Chapter

47

Analisi statistica ?

Figure 39—Example Risk Scenarios *(cont.)*

Ref.	Risk Scenario Category	Risk Type: IT Benefit/Value Enablement	Risk Type: IT Programme and Project Delivery	Risk Type: IT Operations and Service Delivery	Example Scenarios: Negative Example Scenarios	Example Scenarios: Positive Example Scenarios
0201	Programme/projects life cycle management (programme/ projects initiation, economics, delivery, quality and termination)	P	P	S	Failing (due to cost, delays, scope creep, changed business priorities) projects are not terminated.	Failing or irrelevant projects are stopped on a timely basis.
0202		S	P	S	There is an IT project budget overrun.	The IT project is completed within agreed-on budgets.
0203		S	P		There is occasional late IT project delivery by an internal development department.	Project delivery is on time.
0204		P	P	S	Routinely, there are important delays in IT project delivery.	The project critical path is managed accordingly and delivery is on time.
0205		P	P	S	There are excessive delays in outsourced IT development project.	Communication with third parties ensures the timely delivery within agreed-on scope and quality.
0206		P	P		Programmes/projects fail due to not obtaining the active involvement throughout the programme/project life cycle of all stakeholders (including sponsor).	Change management is conducted appropriately throughout the life cycle of the programme/project to inform stakeholders on progress and train future users.
0301	IT investment decision making	P		S	Business managers or representatives are not involved in important IT investment decision making (e.g., new applications, prioritisation, new technology opportunities).	There is co-ordinated decision making over IT investments between business and IT.
0302		P		S	The wrong software, in terms of cost, performance, features, compatibility, etc., is selected for implementation.	Upfront analysis is performed and a business case is made up to ensure the adequate selection of software.
0303		P		P	The wrong infrastructure, in terms of cost, performance, features, compatibility, etc., is selected for implementation.	Upfront analysis is performed and a business case is made up to ensure the adequate selection of infrastructure.
0304		P	P		Redundant software is purchased.	
0401	IT expertise and skills	P	P	P	There is a lack of or mismatched IT-related skills within IT, e.g., due to new technologies.	Attracting the appropriate staff increases the service delivery of the IT department.
0402		P	P	P	There is a lack of business understanding by IT staff affecting the service delivery/ projects quality.	Correct staff and skill mix supports project delivery and value delivery.
0403		P	P	P	There are insufficient skills to cover the business requirements.	Correct skill mix and training ensures that there is a thorough understanding of the business by staff and allows full coverage of business requirements.
0404		S	P	P	There is an inability to recruit IT staff.	The correct amount of IT staff, with appropriate skills and competencies is attracted to support the business objectives.
0405		S	P	P	There is a lack of due diligence in the recruitment process.	Candidates are screened to ensure that appropriate skills, competencies and attitude are present.
0406		S	P	P	There is a lack of training leading to IT staff leaving.	IT staff members are able to determine their own training plan based on their aspirations and domains of interest, in collaboration with their superiors.
0407		S	P	P	There is insufficient return on investment regarding training due to early leaving of trained IT staff (e.g., MSA).	Career development is made formal and individual paths are determined to ensure IT staff is motivated to stay for a considerable amount of time.

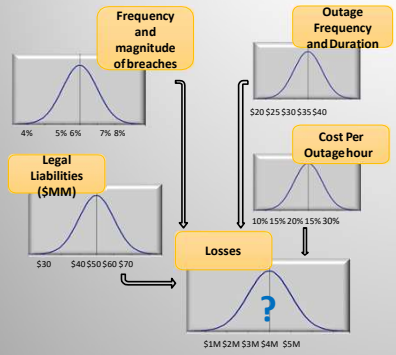
ISACA Rome Chapter

48

Possiamo imparare dagli altri

49

Monte Carlo: How to Model Uncertainty in Decisions



- Simple decomposition greatly reduces estimation error for estimating the most uncertain variables (MacGregor, Armstrong, 1994)
- As Kahneman, Tversky and others have shown, we have a hard time doing probability math in our heads
- In the oil industry there is a correlation between the use of quantitative risk analysis methods and financial performance – and the improvement started after using the quantitative methods. (F. Macmillan, 2000)
- Data at NASA from over 100 space missions showed that Monte Carlo simulations beat other methods for estimating cost, schedule and risks (I published this in *The Failure of Risk Management* and *OR/MS Today*).

50

Un «Sottoprodotto»

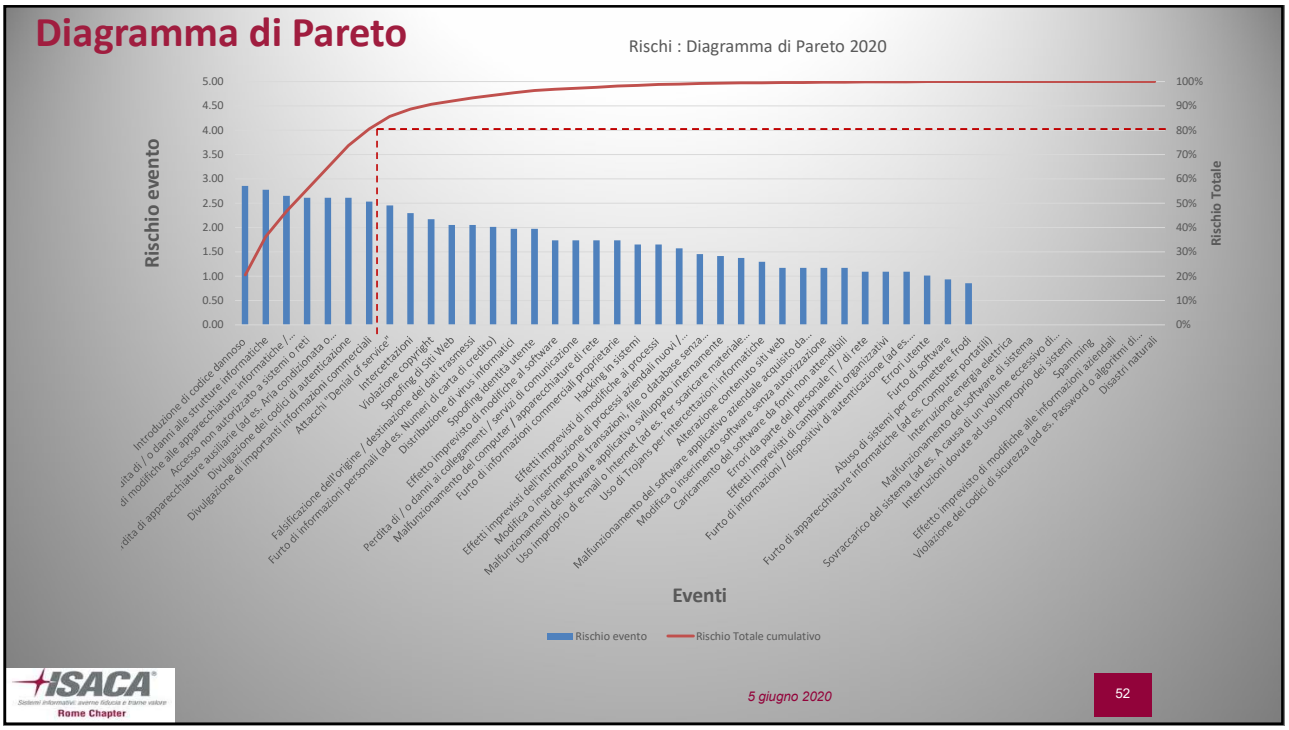
- Il metodo visto mette a disposizione i valori dei rischi in una «Scala a rapporti equivalenti» espressa in ALE €/anno (Annual Loss Expectation).
- Sono quindi possibili
  - Somma di rischi
  - Percentuali
  - Ecc.
- Si possono quindi produrre alcuni utili reports altrimenti impossibili
- Se si utilizza excel, pivot tables: campi calcolati, la soluzione è banale

Rischio	Ind. R. Norm	n	ALE	Tot
AA	4	10	10.000€	100.000€
AB	5	1	2.000.000€	2.000.000€
			Totale	2.100.000€
			IR equiv.	**5.16**

ISACA Rome Chapter

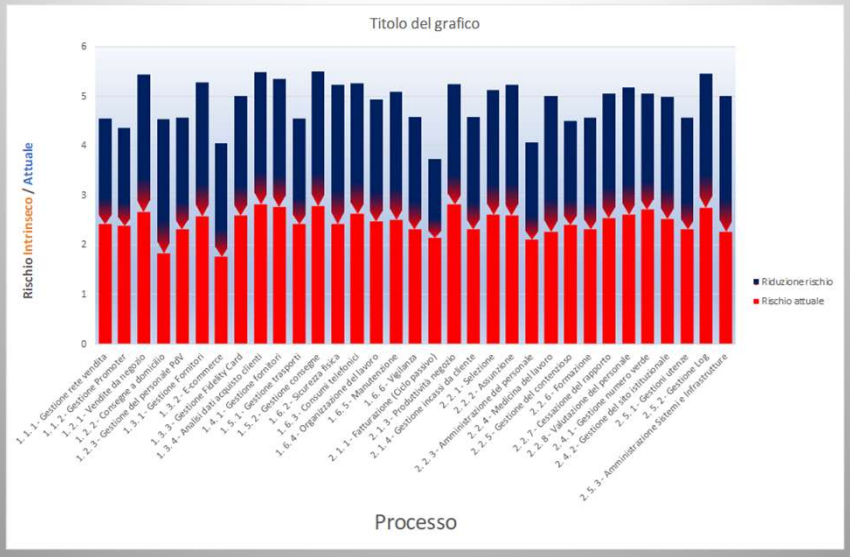
51

Diagramma di Pareto



ISACA Rome Chapter

52



ISACA Rome Chapter

53

Small Samples Tell You More Than You Think

When someone in cybersecurity or any other field says something like, "**We don't have enough data to measure this**," they probably do not understand that they are making a very specific mathematical claim—for which they provided no actual math to support. Did they actually compute the uncertainty reduction from a given amount of data? Did they actually compute the economic value of that uncertainty reduction? Probably not.

Our intuition is one problem when it comes to making probabilistic inferences about data. But perhaps a bigger problem is What We think We learned (but learned incorrectly) about statistics. **Statistics actually helps us make some informative inferences from surprisingly small samples**

Rule of Five

There is a chance that the median of a population is between the smallest and largest values in any random sample of five from that population.

ISACA Rome Chapter

54

Stimando s'impara

Le ricerche ci dicono che:

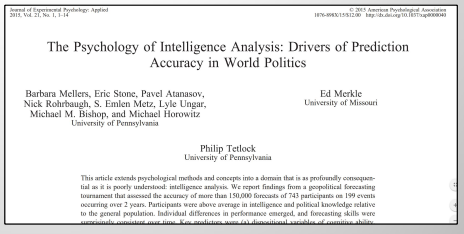
- Non tutti siamo in grado di stimare correttamente le probabilità di accadimento di un evento o l'entità del danno potenziale
- Tutti possono imparare a farlo, anche in modo più che soddisfacente

ISACA Rome Chapter

55

Improving Expert Forecasts

- Tetlock also looked at what improved *forecasting.*
- He tracked 743 individuals who made at least 30 forecasts each over a 2-year period.
- He determined factors that made the biggest difference in the performance of forecasting.



The Psychology of Intelligence Analysis: Drivers of Prediction Accuracy in World Politics

Barbara Mellers, Eric Stone, Pavel Atanasov, Nick Rohrbaugh, S. Emlen Metz, Lyle Ungar, Michael M. Bishop, and Michael Horowitz
University of Pennsylvania

Ed Merkle
University of Missouri

Philip Tetlock
University of Pennsylvania

This article extends psychological methods and concepts into a domain that is as profoundly consequential as it is poorly understood: intelligence analysis. We report findings from a geopolitical forecasting tournament that assessed the accuracy of more than 150,000 forecasts of 743 participants on 199 events occurring over 2 years. Participants were above average in intelligence and political knowledge relative to the general population. Individual differences in performance emerged, and forecasting skills were

Probabilistic Training

- Subjects were trained in basic inference methods, using reference classes, and avoiding common errors and biases.

Teams and Belief Updating

- Teams deliberated more and individuals were willing to update beliefs based on new information.

Selecting the Best

- Brains matter. Both topic expertise and overall IQ were the best predictors of performance.

ISACA Rome Chapter

56

Due tipi di stima di probabilità

- Discreta (binaria) nell'arco di tempo
  - Lancio moneta
  - Data Breach
  - Blocco sistema
  - …
- Continua (Intervallo di confidenza: CI 90%)
  - Conseguenze Data Breach (€ $_{max-min}$)
  - Durata interruzione di servizio (t $_{max-min}$)
  - …

Due atteggiamenti

- **Ottimista**
- **Pessimista**

Il fenomeno è stato studiato (Psicologia delle Decisioni) a partire dagli anni '80: premio Nobel Scienze Economiche 2002.

Per ogni individuo l'atteggiamento relativo alle stime è abbastanza costante (prevale l'ottimismo)

Le ricerche hanno dimostrato che si può imparare a correggere la nostra attitudine «congenita», migliorando, in modo misurabile, la nostra capacità di stima

Esercizi di calibrazione (Corso ½ giornata)

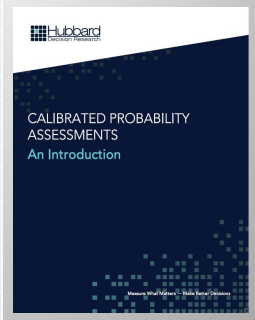
57

Calibration questions

#	Question	Lower Bound (95% chance value is higher)	Upper Bound (95% chance value is lower)
1	What percentage of bronze is typically made of copper?		
2	How many countries have at least one McDonald's?		
3	How many employees did ebay have in the first quarter of 2006?		
4	What was the population of Miami (within the city limits, not the entire metropolitan area) in 1990?		
5	How many casualties did the French suffer in the Battle of Waterloo?		
6	What is the range in miles of a Minuteman Missile?		
7	What is the percentage of IT jobs in the US were unfilled in 1977?		
8	The Supremes' (with Diana Ross) song "Stop! In the Name of Love" was how long? (minutes, seconds)		
9	How many undergraduates attended Cambridge in 1990?		
10	If you could jump 50 feet straight up into the air, how many seconds would you be airborne before you landed?		
11	How many gallons are in a bushel (they are both measures of volume)?		
12	How many sovereign rulers has England had in the last thousand years?		
13	If the air temperature was 5 degrees below zero (Fahrenheit) and the wind speed was 15 mph, what would the temperature adjusted for wind-chill be?		
14	Average cost of testing in software development is what percentage of total project costs?		
15	On average, if a software development project was projected to take 17 months, it actually takes how many months?		
16	How many meters tall is the Sears Tower?		
17	How many gold medals did Jesse Owens win at the 1936 Berlin Olympics?		
18	In 2005, the average combined MPG for all US cars and light trucks on the road was how much?		
19	The average house in the United States uses how many gallons of water per day?		
20	What was the average price in the United States of a house sold in 2001?		

	Statement	Answer (T/F)	Confidence that you are correct (Circle one)
1	The melting point of tin is higher than the melting point of aluminum.		50% 60% 70% 80% 90% 100%
2	In English, the word "quality" is more frequently used that the word "speed".		50% 60% 70% 80% 90% 100%
3	Any male pig is referred to as a hog.		50% 60% 70% 80% 90% 100%
4	California's giant sequoia trees are named for an early 19th century leader of the Cherokee Indians.		50% 60% 70% 80% 90% 100%
5	The Model T was the first car produced by Henry Ford.		50% 60% 70% 80% 90% 100%
6	When rolling 2 dice, a roll of 7 is more likely than a 3.		50% 60% 70% 80% 90% 100%
7	No one has ever been reported to have been hit by any object that fell from space.		50% 60% 70% 80% 90% 100%
8	Sir Christopher Wren was a British anthropologist.		50% 60% 70% 80% 90% 100%
9	Pakistan does not border Russia.		50% 60% 70% 80% 90% 100%
10	The Navy won the first Army-Navy football game.		50% 60% 70% 80% 90% 100%
11	The paperback version of the book "The Da Vinci Code", as of July 2007, still ranks in the top 500 bestselling books on Amazon.		50% 60% 70% 80% 90% 100%
12	Italian has more words than any other language.		50% 60% 70% 80% 90% 100%
13	The month of August is named after a Greek god.		50% 60% 70% 80% 90% 100%
14	The deepest ocean trench is deeper than the Grand Canyon.		50% 60% 70% 80% 90% 100%
15	Abraham Lincoln was the first president born in a log cabin.		50% 60% 70% 80% 90% 100%
16	As of July of 2007, more people search Google for "Harry Potter" than "Hillary Clinton" (according to GoogleTrends).		50% 60% 70% 80% 90% 100%
17	The population of Alabama is higher than the population of Arizona.		50% 60% 70% 80% 90% 100%
18	No category 5 hurricane hit the US in 2004.		50% 60% 70% 80% 90% 100%
19	The UK is among the top 10 largest economies in the world (by GDP).		50% 60% 70% 80% 90% 100%
20	The movie Forest Gump has grossed more to date than E.T. The Extra Terrestrial.		50% 60% 70% 80% 90% 100%

Come interpretare i risultati



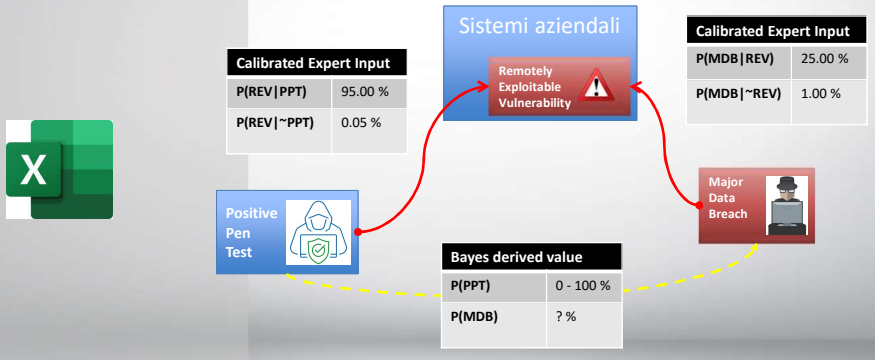
58

Reducing Uncertainty with Bayesian Methods

59

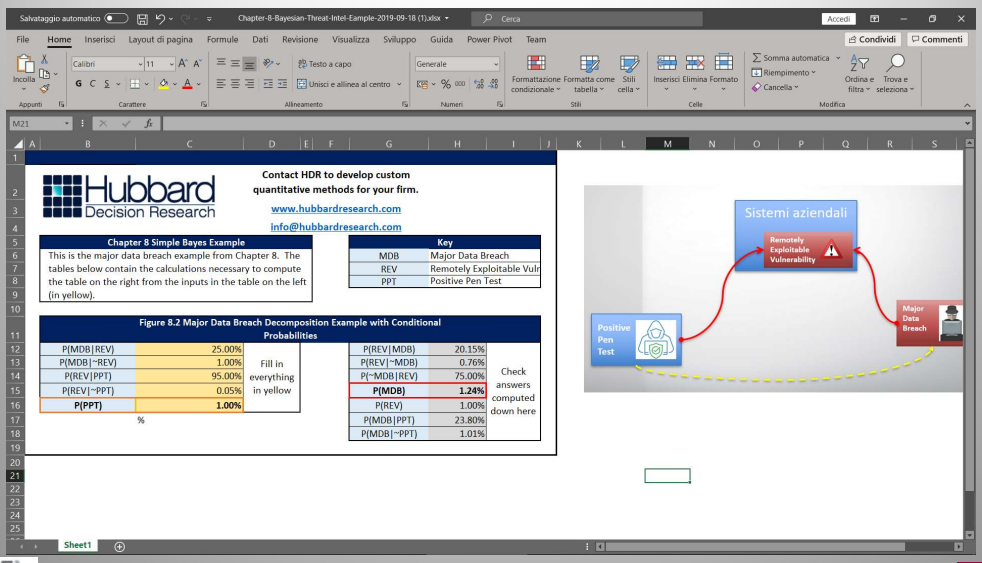
Analisi di un caso specifico

- Esistono metodi matematici per ridurre l'incertezza collegando cause, di cui sappiamo stimare la probabilità, all'effetto di cui vogliamo valutare la probabilità
- Ad esempio:



60

Esempio excel

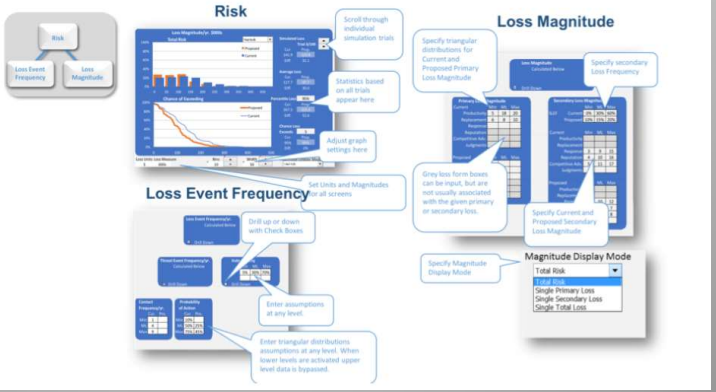


61

Metodologie di Cybersecurity che utilizzano Monte Carlo:

Open FAIR

With a view to creating a tool that helps accelerate the adoption of the Open FAIR standard, the tool provides both experienced and novice risk practitioners with a practical and pragmatic tool to help analyze perceived risk in a consistent and simple to use way, whatever industry they work in. It is now available for our members and others to download and evaluate.



62

Call to Action for Cybersecurity

- Organizations should stop using risk scores and risk matrixes and standards organizations should stop promoting them
- Adopt simple probabilistic methods now: They demonstrate a measurable improvement over unaided intuition and they have already been used. So there is no reason not to adopt them.
- Build on simple methods when you are ready – always based on what shows a measurable improvement.

63

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Questions ?

Grazie per l'attenzione

alberto.piamonte@alice.it

65