

V-Research

#cybersecurity
#private
#r&d #science #engineering
#italy

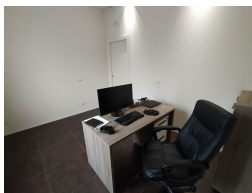


Marco Rocchetto

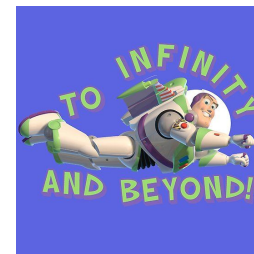
Michele Ambrosi



- Founded in **2020**, **Verona** – IT
- A **private R&D lab** that bridges **foundational challenges** and **engineering needs**
- Our **mission** is to develop a:
 - **scientific theory of cybersecurity** and
 - a tool-chain for the secure engineering of **cyber-physical systems**



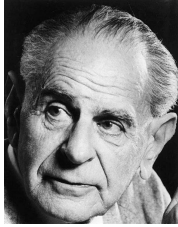
edulife
apprendere per crescere insieme



2020
2ppl

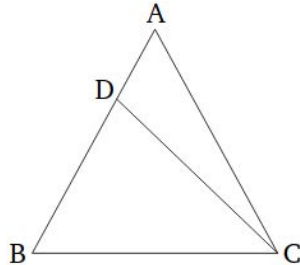
Consultancy - R&D - EDU

2022
10 ppl



A theory which is not refutable by any conceivable event is non-scientific. Irrefutability is not a virtue of a theory (as people often think) but a vice.

K. Popper, Conjectures and Refutations



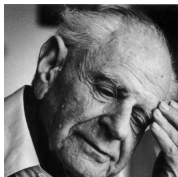
Time & Understanding →



Step 1: understand triangles
Math, Deductions, Predictions

Step 2: build pyramids
Engineering, Induction, Falsification

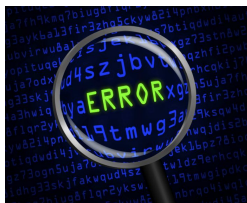
Unfalsifiability of security claims



Cormac Herley^{a,1}

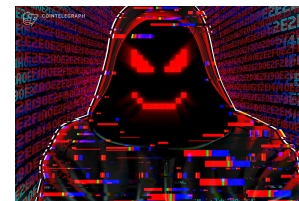
^aMicrosoft Research, Redmond, WA 98052

There is an inherent asymmetry in computer security: Things can be declared insecure by observation, but not the reverse. There is no observation that allows us to declare an arbitrary system or technique secure. We show that this implies that claims of necessary



Errors
Best Practices

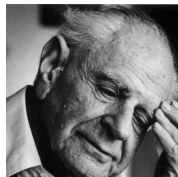
Time! & Understanding?



System under
attack

Step 2: Induce triangles
Math, Inductions, Post-dictions

Step 1: build pyramids
Engineering, Induction, Falsification
Expertise



Un

Corm

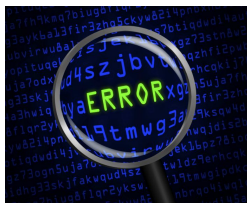
Micro

Ther

be d

no c

tech



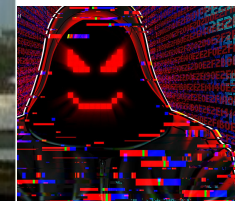
Errors
Best Practices

Step 2: Induce trian
Math, Inductions, Post-d

TRUST ME



IEEE
CYBER
SECURITY



ystem under
attack

: build pyramids
Induction, Falsification
Expertise

V-Research

Cybersecurity Risk Assessment

Marco Rocchetto

Michele Ambrosi



- **Cybercrime up 600%** Due to COVID-19 Pandemic
- **71.1 million** people fall **victim** to cyber crimes yearly
- **Individuals lose \$318 billion** to cybercrime.
- **Individuals of phishing scams lost \$225** on average.
- Global annual **cost** of cybercrime: around **\$6 trillion per year**
- **Ransomware is 57x more** destructive in 2021 than it was in 2015
- **23 days** (average) to recover from **ransomware**
- **10% increase** in average total **cost of a breach** from 2020-2021
- **27.4% increase** of security breaches (enterprise)
- Enterprises needed **50 days to resolve** an insider's attack
- **66% SMB at least 1 incident** in 2018-2020
- **SME data breach** cost \$120,000-**\$1.24 million**



There are no secure systems (1)

- What is the definition of a secure system?

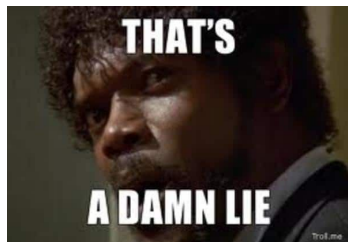
We don't know it (yet)

- So how can we make a system secure?

We can't

- But I know a guy that told me that his software is hacker-proof...

Well...



...or even worst!



Even if we start from a **secure set of requirements** (whatever it is), from a theoretical perspective the only thing we know right now is that to test the **security** of a software we should **explore the entire space of the system's states**.



Rice's Theorem



In computability theory and computational complexity theory, an **undecidable problem** is a decision problem for which it is proved to be impossible to construct an algorithm that always leads to a correct yes-or-no answer.

UNDECIDABLE




Let p be a property of a formal language that is nontrivial, meaning

1. there exists a recursively enumerable language having the property p ,
2. there exists a recursively enumerable language not having the property p ,

Then it is undecidable to determine for a given Turing machine M , whether the language recognized by it has the property p .

What are the properties that make a system secure?




An unauthorized person is able to read and take advantage of information stored in the computer:

- sometimes extends to “traffic analysis”, the intruder only observes the patterns of information use from which he can infer some information content
- includes the unauthorized use of a proprietary program.

CONFIDENTIALITY



- Social Engineering
- Packet Sniffing
- Wiretapping
- Keyloggers




An unauthorized person is able to make changes in stored information – a form of sabotage. It should be noted that in the case of this kind of violation, the intruder does not necessarily see the information he has changed.

INTEGRITY



- Spoofing
- Man-In-The-Middle
- Session hijacking



An intruder can prevent an authorized user from referring to, or from modifying information, even though the intruder may not be able to refer to, neither modify the information themselves.

AVAILABILITY



- DOS/DDOS
- Electrical power attacks
- 802.11 de-auth

Some considerations:

- Confidentiality of what and for who?
- Integrity of what?

} **Access Control**

- Availability is fine (of the entire system of course), but how can be guaranteed?

The only truly secure system is one that is
powered off, cast in a block of concrete and
sealed in a lead-lined room with armed guards
— and **even then I have my doubts.**

Eugene H. Spafford
Purdue University

There are no secure systems (2)

OK, so what can we do?

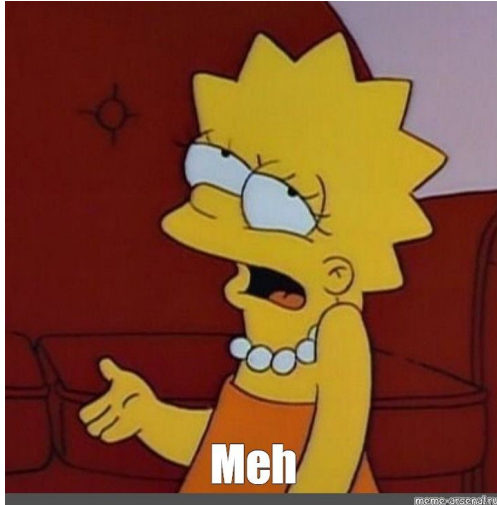
Do we just sit down and wait for the end to come?

Do we shut down the company?

No! The only answer is...



Worldwide



Italy



The real world - How is it?

Worldv



Me



Italy



The real world - How is it?

Worldv



If politics is like this...

Italy



What about small companies?

The real world - How is it?

Worldv



If politics is like this...



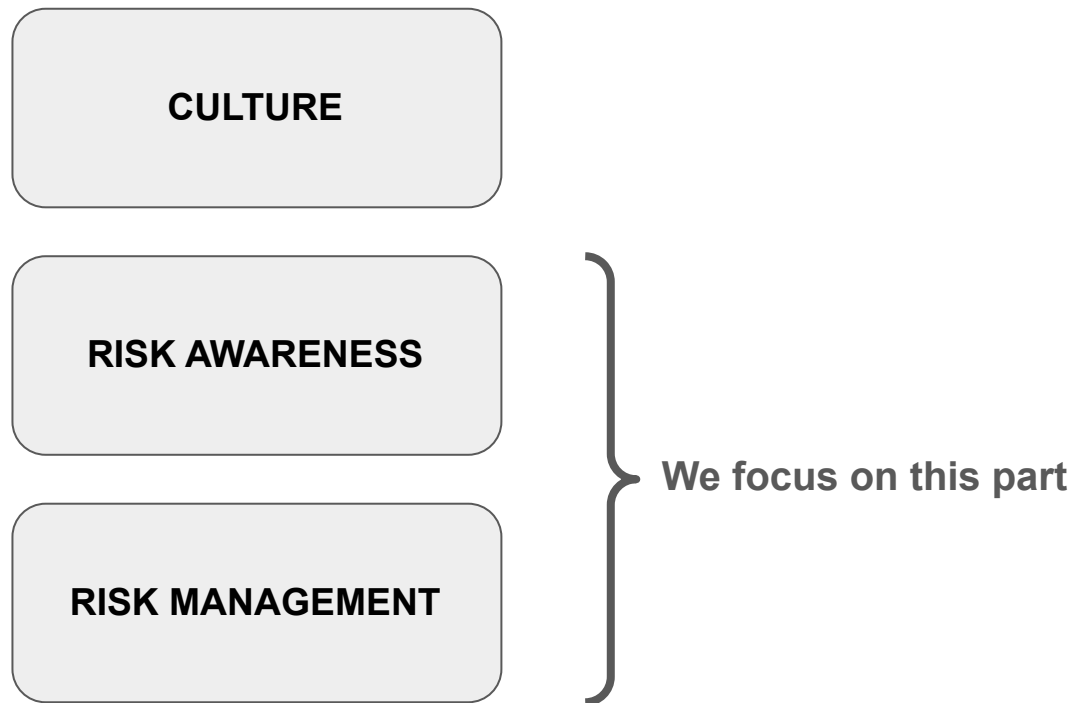
Not so good!



Italy

panies?

Cybersecurity starts with 3 fundamental pillars:



Organizations must be aware of what are the risks of their business:

- Risk awareness must start from C-suite
- Organizations cannot be protected from something that they don't know
- Risk awareness is not (only) about technical risks



Risk cannot be avoided but it need to be managed in the right way:

- Understand the likelihood
- Understand the impact
- Prioritize



Managing risk is expensive but not doing it can be more expensive!



The risk management process consists of the following steps:

UNDERSTAND THE CONTEXT



- Interview C-suite members
- Understand business model
- List business processes
- Understand complexity (number of buildings, number of people, outsourced activities, etc.)

DEFINE THE PERIMETER



- Define critical business processes
- Define any out-of-scope business process

IDENTIFY THE ASSETS



- For each business process list involved **immaterial** assets (e.g. reputation, intellectual property, etc.)
- For each business process list involved **material** assets (e.g. hardware devices, software, etc.)

IDENTIFY THE THREATS

ESTIMATE LIKELIHOOD AND IMPACT

DRAFT A REMEDIATION PLAN

The risk management process consists of the following steps:

UNDERSTAND THE CONTEXT

DEFINE THE PERIMETER

IDENTIFY THE ASSETS

IDENTIFY THE THREATS

ESTIMATE LIKELIHOOD AND IMPACT

DRAFT A REMEDIATION PLAN



- For each material asset identify the threats
- For each threat define a scenario



- For each threat estimate the likelihood (probability to happen)
- For each threat estimate the impact on the entire organization
- Draft risk matrix



- Fix a risk threshold
- Provide a remediation for each threat above the fixed threshold
- Draft a remediation implementation plan prioritizing activities with respect to risk

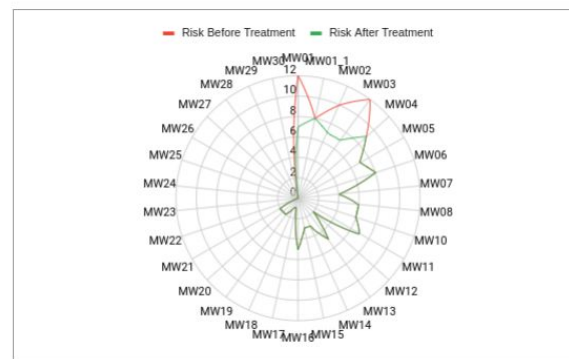
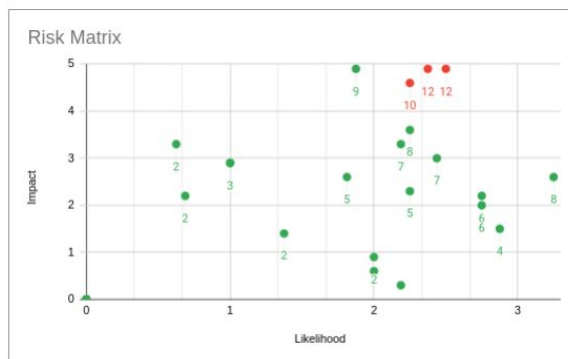
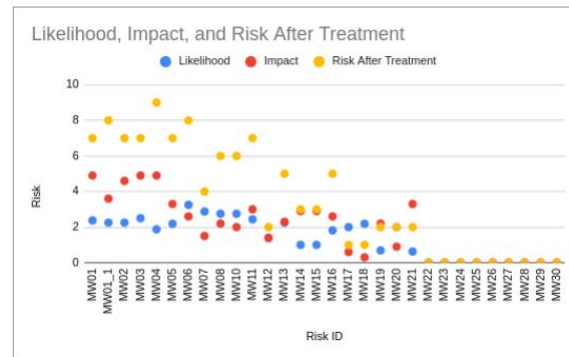
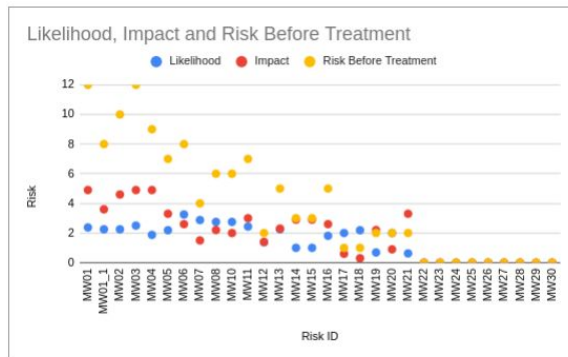
Here is a partial real example of how we conduct a risk assessment for an asset:

EXAMPLE DOCUMENT

The real world - Hand on (3)

Risk ID	Likelihood	Impact	Risk Before Treatment	Risk After Treatment
MW01	2.375	4.9	12	7
MW01_1	2.25	3.6	8	8
MW02	2.25	4.6	10	7
MW03	2.5	4.9	12	7
MW04	1.875	4.9	9	9
MW05	2.1875	3.3	7	7
MW06	3.25	2.6	8	8
MW07	2.875	1.5	4	4
MW08	2.75	2.2	6	6
MW10	2.75	2	6	6
MW11	2.4375	3	7	7
MW12	1.375	1.4	2	2
MW13	2.25	2.3	5	5
MW14	1	2.9	3	3
MW15	1	2.9	3	3
MW16	1.8125	2.6	5	5
MW17	2	0.6	1	1
MW18	2.1875	0.3	1	1
MW19	0.6875	2.2	2	2
MW20	2	0.9	2	2
MW21	0.625	3.3	2	2
MW22	0	0	0	0
MW23	0	0	0	0
MW24	0	0	0	0
MW25	0	0	0	0
MW26	0	0	0	0
MW27	0	0	0	0
MW28	0	0	0	0
MW29	0	0	0	0
MW30	0	0	0	0

THRESHOLD 10



And...



Marco Rocchetto
marco@v-research.it



Michele Ambrosi
michele.ambrosi@v-research.it