CSIRA: A method for analysing the risk of cybersecurity incidents

Aitor Couce Vieira[13], Siv Hilde Houmb[2], David Rios Insua[3]

[1]Universidad Rey Juan Carlos, Spain
[2]Secure-NOK AS, Norway
[3]Instituto de Ciencias Matemáticas, Centro Superior de Investigaciones Científicas, Spain

Contents

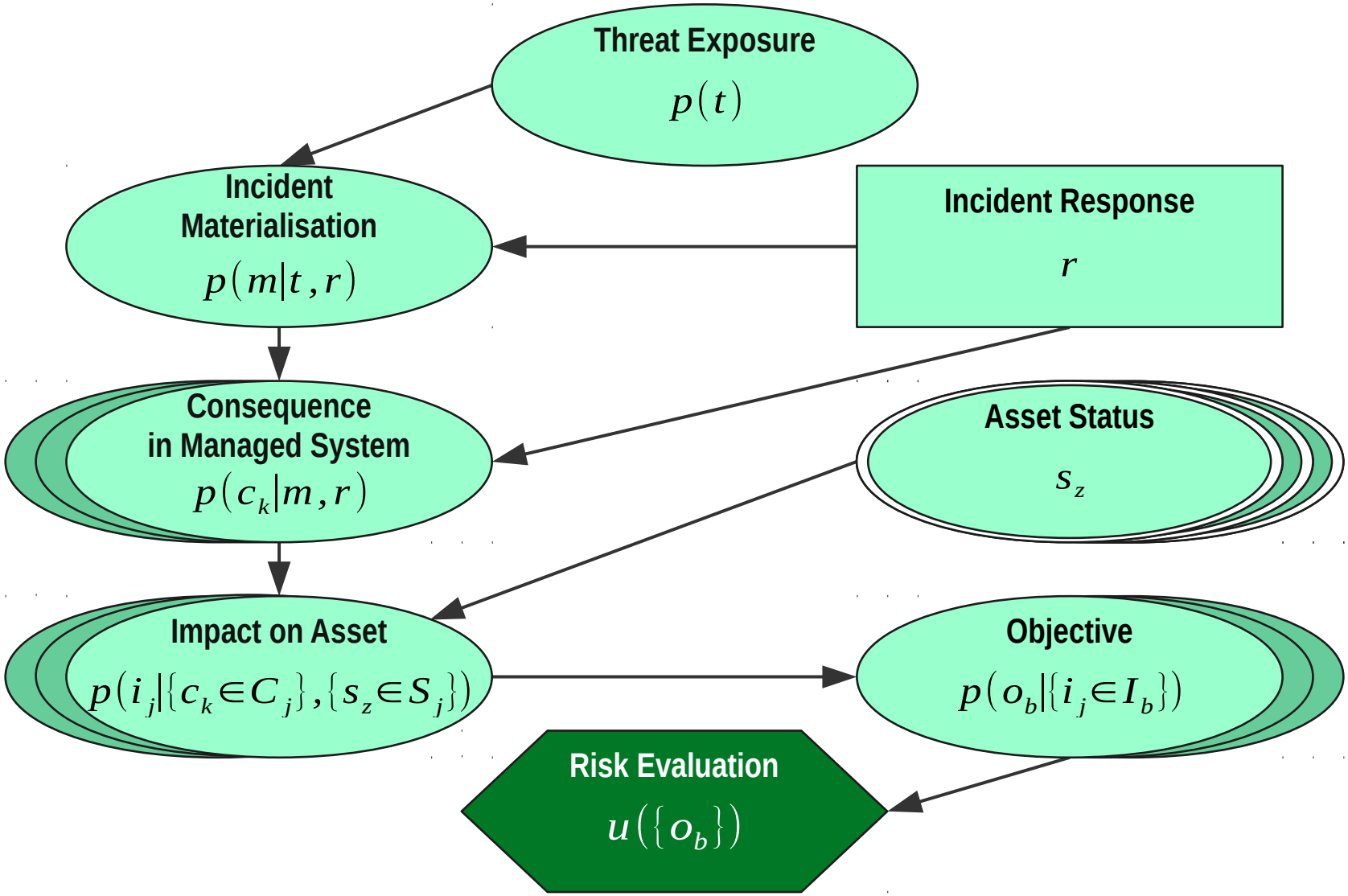
GIRA

General model for incident risk analysis

CSIRA

Simplified application of GIRA for cybersecurity

GIRA: General model for incident risk analysis



GIRA: General model for incident risk analysis

Risk calculation

$$p\Big(\{o_b\},\{i_j\},\{c_k\},m,t\Big) = p(o_1,\ldots,o_B,\ldots,c_1,\ldots,c_K,m,t) =$$

$$= \Big[\prod_{b=1}^{B} p(o_b|\{i_j \in I_b\})\Big]\Big[\prod_{i=1}^{J} p(i_j|\{c_k \in C_j\},\{s_z \in S_j\})\Big]\Big[\prod_{c=1}^{K} p(c_k|m,r)\Big]p(m|t,r)p(t)$$

Risk evaluation

Maximising expected utility: $r^* : \max \psi(r)$

$$\psi(r) = \int \cdots \int \quad u\Big(\{o_b\}\Big)p\Big(\{o_b\},\{i_j\},\{c_k\},m,t\Big) \quad dt\ dm\ dc_K \ldots do_1$$

… or other alternative method: e.g., prospect theory.

CSIRA: Simplification of GIRA for cybersecurity

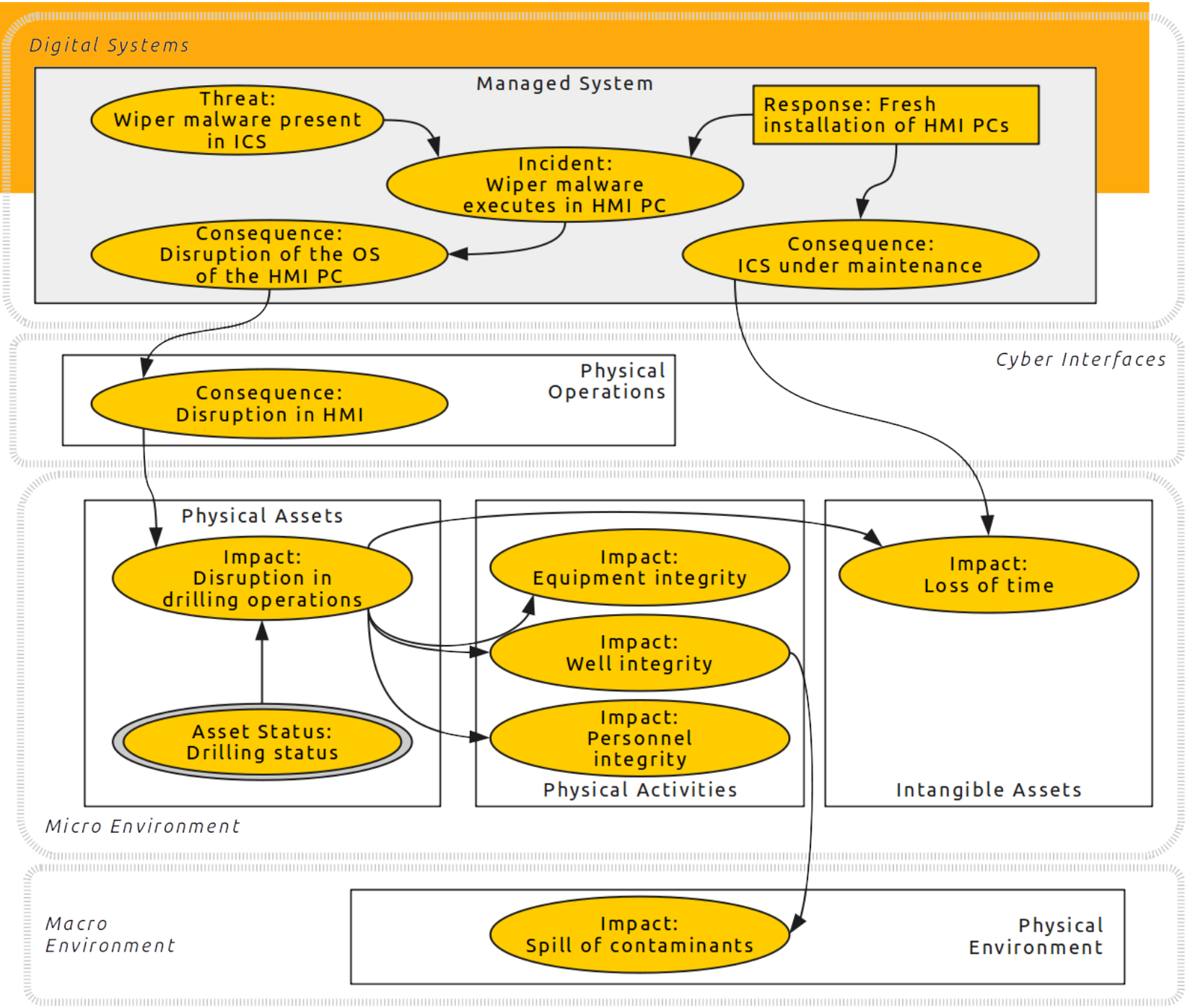
Framework for simple risk analysis

And non-expert use

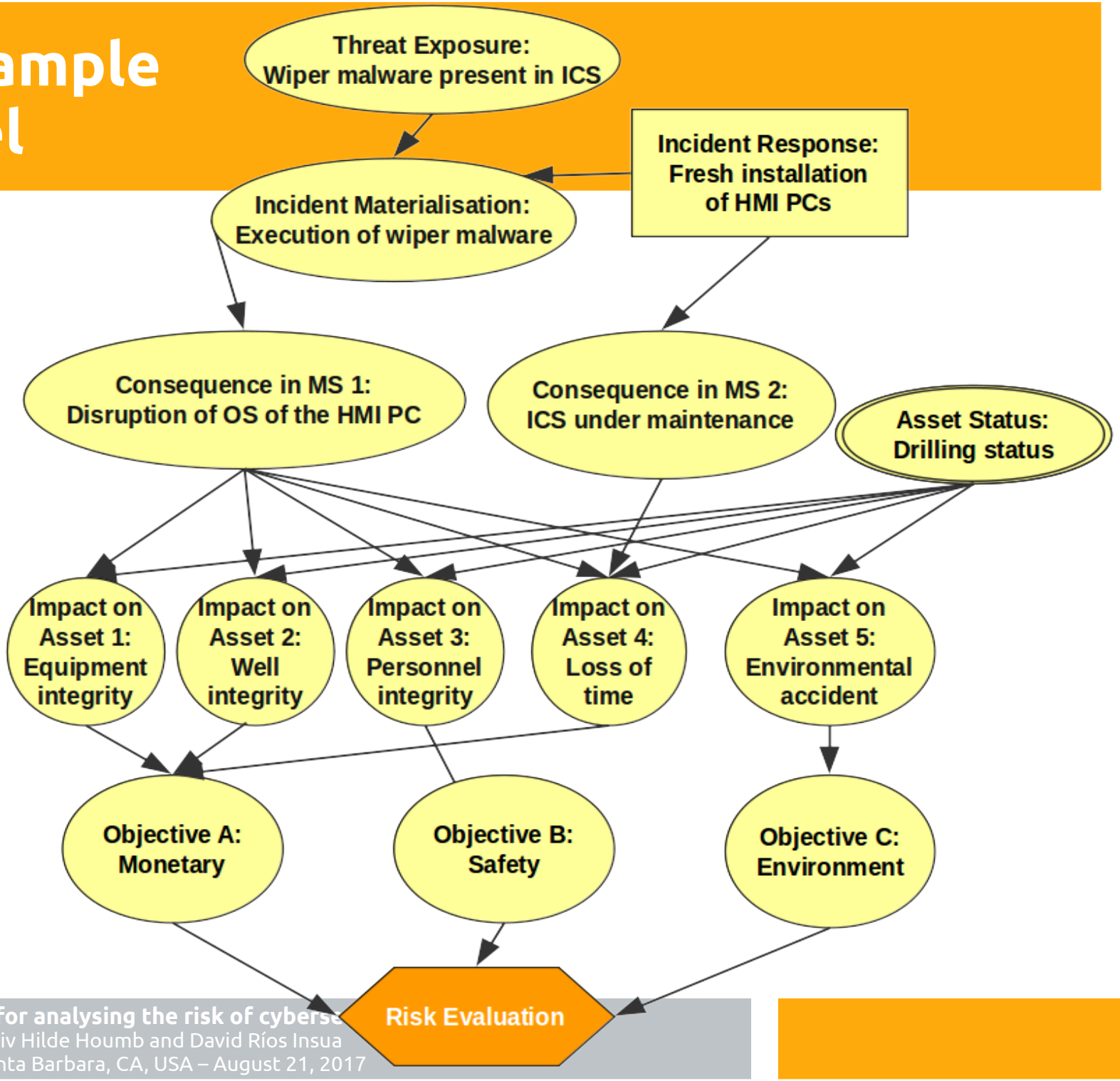
Likelihood: certain, possible, rare and impossible

Risk evaluation: ordering risk scenarios derived from the incident

Example incident

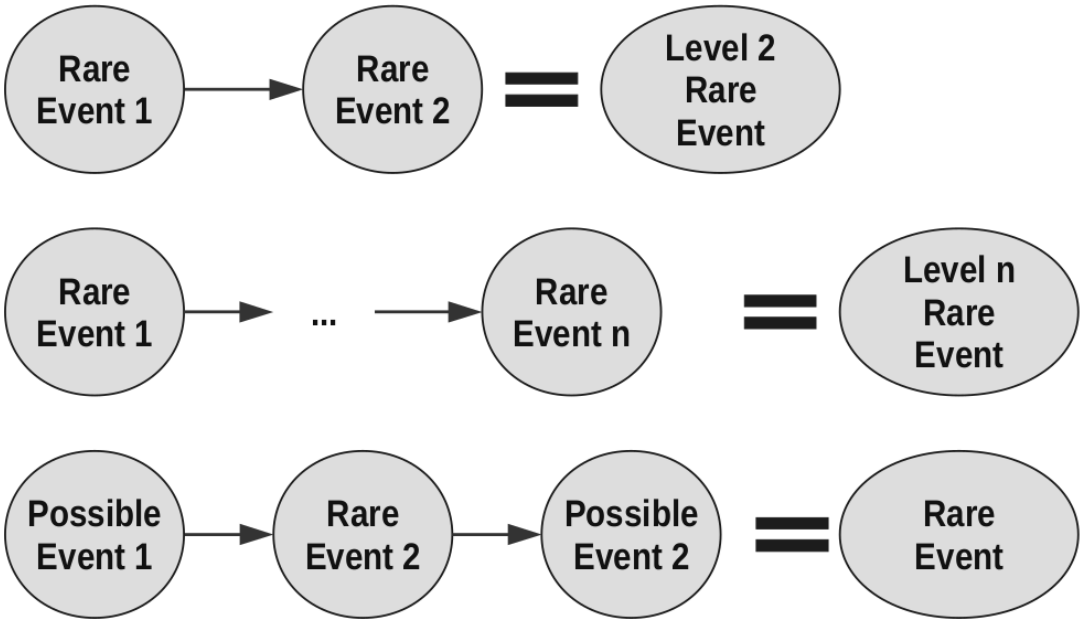


CSIRA: Example case model



CSIRA: Risk calculation example (I)

Likelihood	Probability
Certain	P(s) = 1
Possible	P(s) = (α,1)
Rare	P(s) = (0,α)
Impossible	P(s) = 0



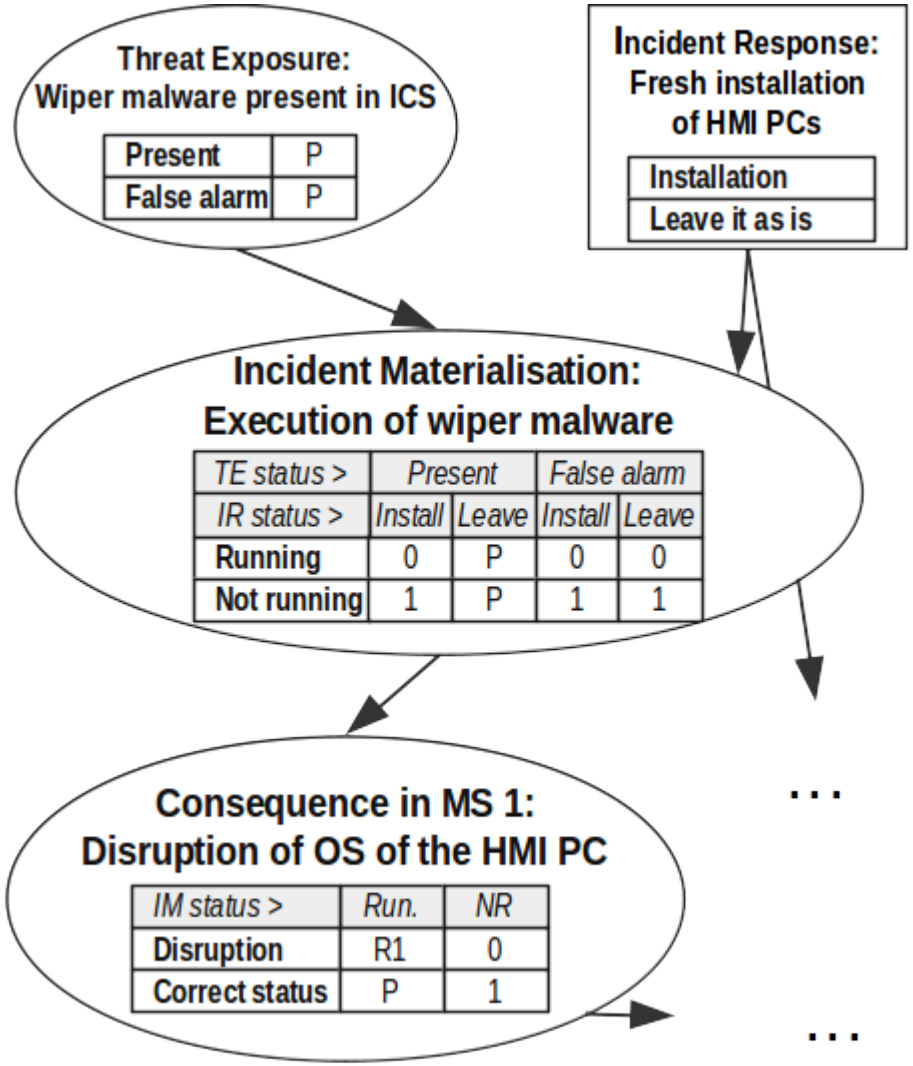
CSIRA: Risk calculation example (II)

Possible in $(1 \times 10^{-2}, 9.99 \times 10^{-1})$
Rare Level 1 in $(1 \times 10^{-12}, 9.99 \times 10^{-11})$
Rare Level 2 in $(1 \times 10^{-22}, 9.99 \times 10^{-21})$
...

Event	User input	Numerical marginal probability	Numerical overall probability	Output to user
Event 1	Possible	5×10^{-2}	5×10^{-2}	Possible
Event 2	Rare	6×10^{-12}	3×10^{-13}	Rare
Event 3	Rare Level 4	3×10^{-42}	9×10^{-55}	Rare Level 5

Alternatively, for simplification:
Rarer than rare for Level 2 and higher

CSIRA: Risk calculation example (III)



CSIRA: Risk evaluation example

Elicitation of preferences for the response scenarios only.

E.g., for a Bayesian Network with 2 states in the response node and 3 objective nodes with three states:

- Complete utility elicitation (with certainty) requires comparing 27 scenarios ...
- … and at least 2/3 times more with uncertainty
- **CSIRA**: Just eliciting the preferences for the responses. In the example, comparing 2 scenarios.

CSIRA: Risk evaluation example

… e.g., in the example case,
compare between two responses:

Response: Leave it			
Monetary objective status	**Monetary objective likelihood**	**Safety objective status**	**Safety objective likelihood**
€ 0	Possible	Does not create safety risk	Possible
€ 100.000 - € 1.000.000	Rare	Creates safety risk	Rare Level 2
€ 1.000.000 >	Rarer Level 5		

Response: Re-installation			
Monetary impact	**Monetary objective likelihood**	**Safety impact**	**Safety objective likelihood**
€ 0	Impossible	Does not create safety risk	Certain
€ 100.000 - € 1.000.000	Certain	Creates safety risk	Impossible
€ 1.000.000 >	Impossible		

On-going / future work

R framework for GIRA-based risk studies

Small program for CSIRA/simple-GIRA

Mature/evolve them in real applications

Support

AXA-ICMAT Chair | H2020 CYBECO Project | RFFVEST CIRFOG Project | MINECO | COST Action

CSIRA: A method for analysing the risk of cybersecurity incidents

Aitor Couce Vieira[13], Siv Hilde Houmb[2], David Rios Insua[3]

[1]Universidad Rey Juan Carlos, Spain
[2]Secure-NOK AS, Norway
[3]Instituto de Ciencias Matemáticas, Centro Superior de Investigaciones Científicas, Spain