11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Dynamic Risk Analyses and Dependency-Aware Root Cause Model for Critical Infrastructures

Steve Muller[abc], Carlo Harpes[a], Yves Le Traon[b],
Jean-Marie Bonnin[c], Sylvain Gombault[c], and Paul Hoffmann[d]

[a] *itrust consulting s.à r.l.*
[b] *University of Luxembourg*
[c] *Télécom Bretagne*
[d] *Luxmetering G.I.E.*

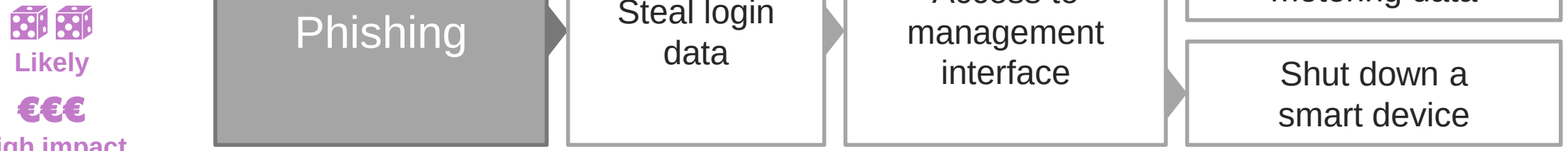
This is how we started …

Risk 1

Likely

€€€

High impact

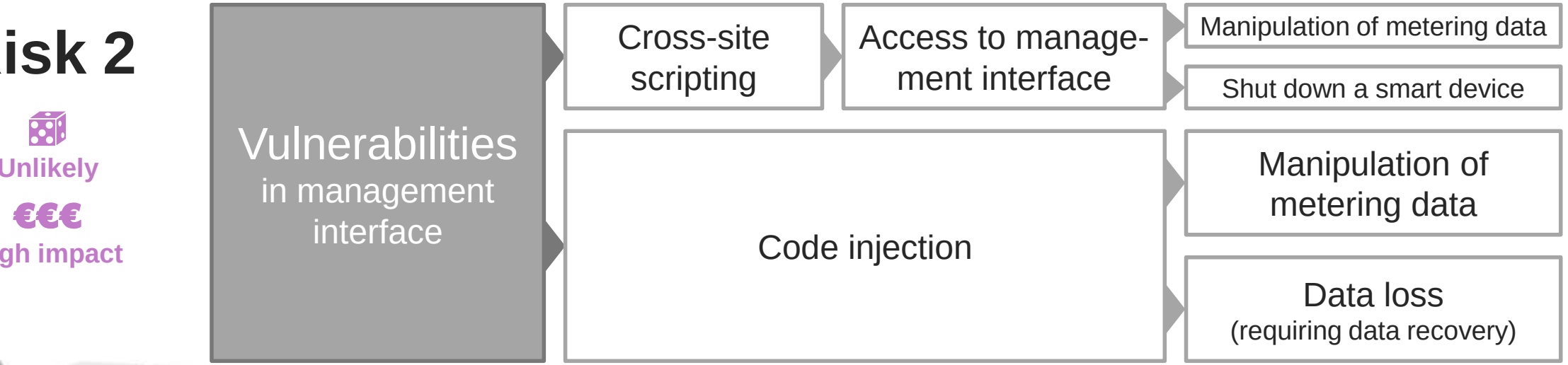


Risk 2

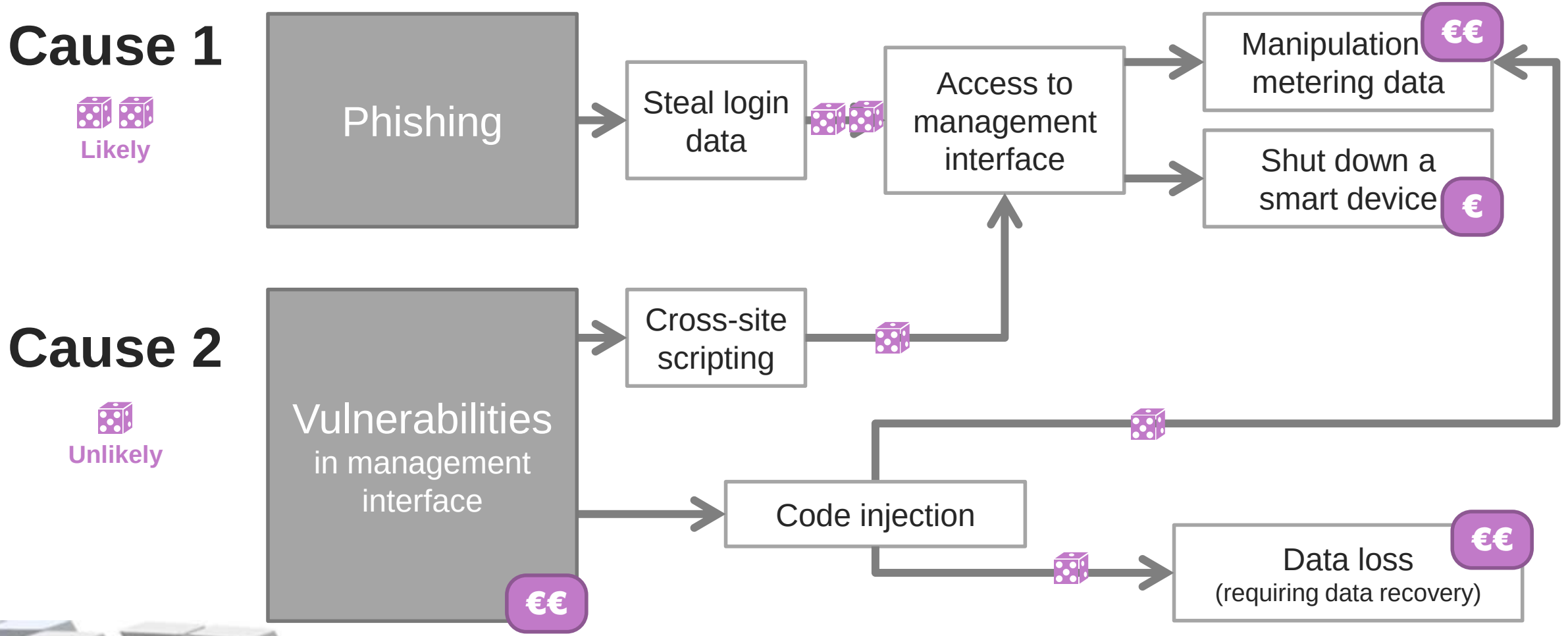
Unlikely

€€€

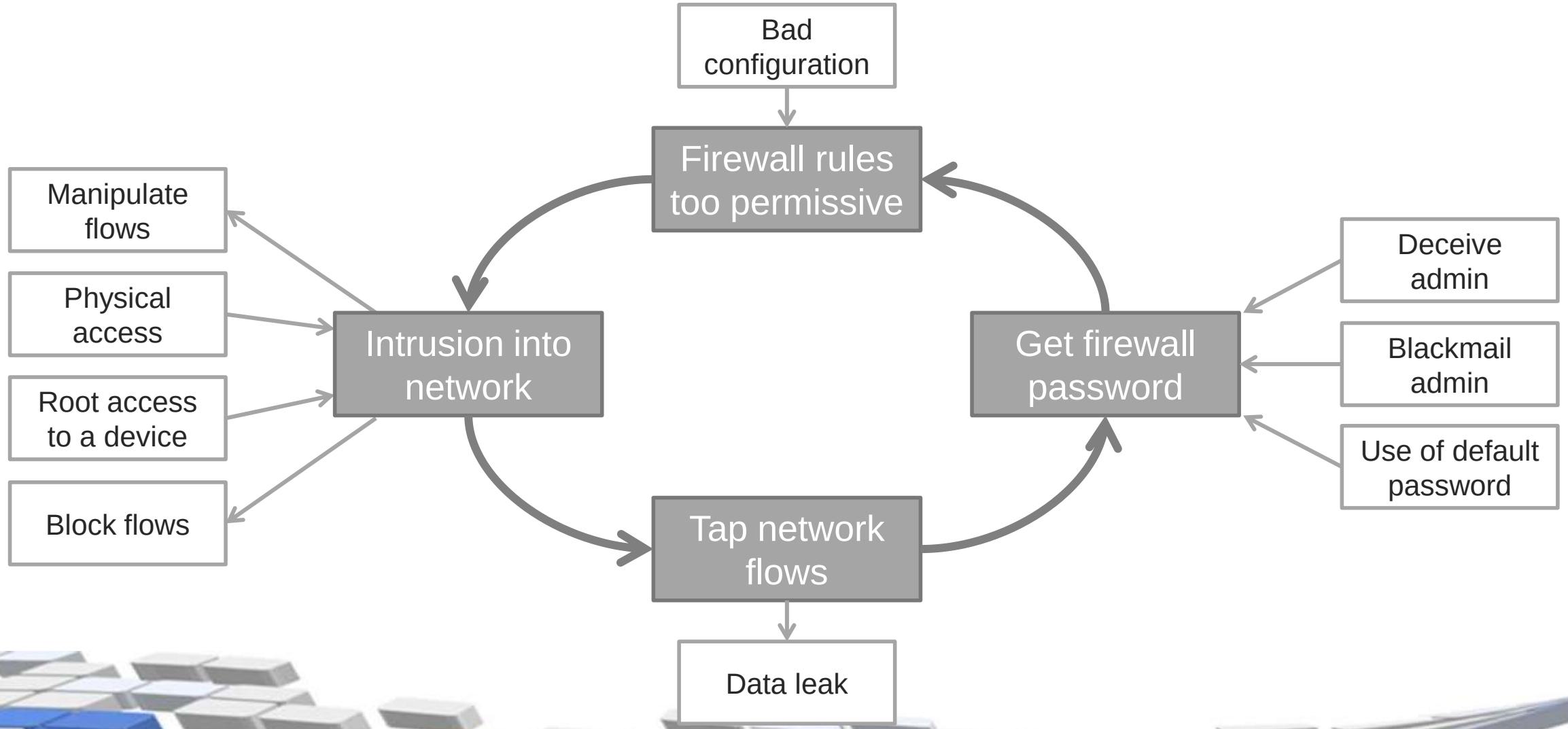
High impact



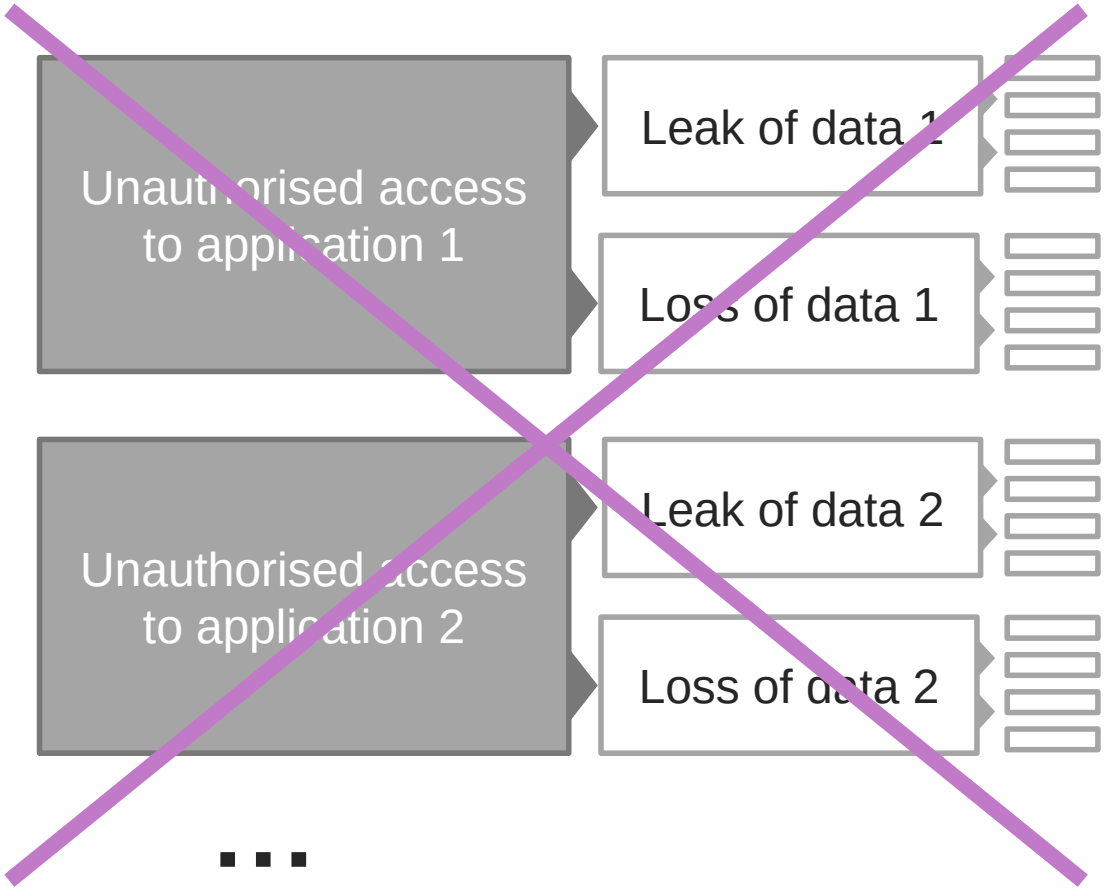
… and what we ended up with

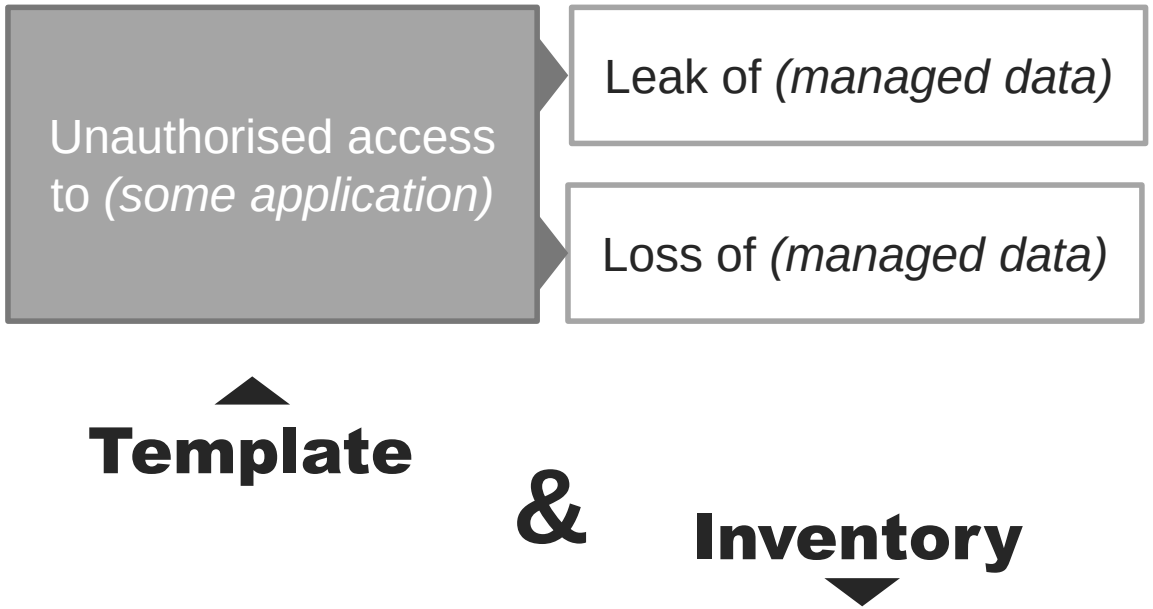


Sometimes there are cycles



There is still a lot of repetition





data 1 *is managed by* application 1

data 2 *is managed by* application 2

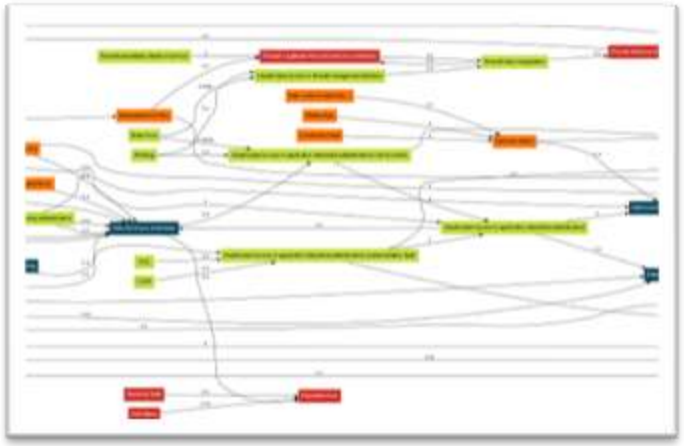
The luxmetering GIE use-case (1/2)

CRITIS 2016

Inventory	×	Templated dependency graph	=	Full dependency graph

12 devices (with multiplicity)
9 networks
37 applications
43 flows
14 data sets
26 certificates
9 sets of credentials
18 services

53 nodes (security events)
104 edges (causal relations)



502 nodes (security events)
1516 edges (causal relations)

Inventory:	18 h (2 md)

Graph:	30 h (4 md)
Estimate:	9 h (1 md)

Generate:	4 s
Fine-tune:	7 h (1 md)

The luxmetering GIE use-case (2/2)

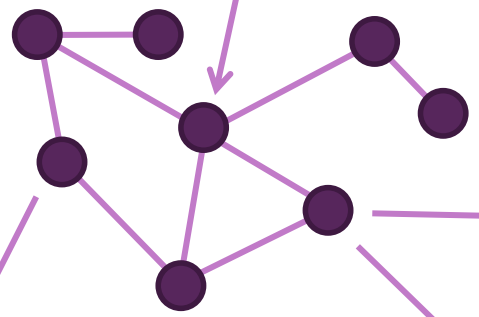
CRITIS 2016

25 root causes, incl.:

- Social engineering
- Password guessing
- DDoS
- Physical access to central system
- Physical intrusion into smart meter
- Environmental incident
- Attrition/Age

Social engineering

- occurs once every 16 years (in expectation)
- no direct impact



Electricity theft €

41% chance → once/39y

Reputation loss €€

99% chance → once/16.2y

Grid failure €€€€

51% chance → once/31.4y

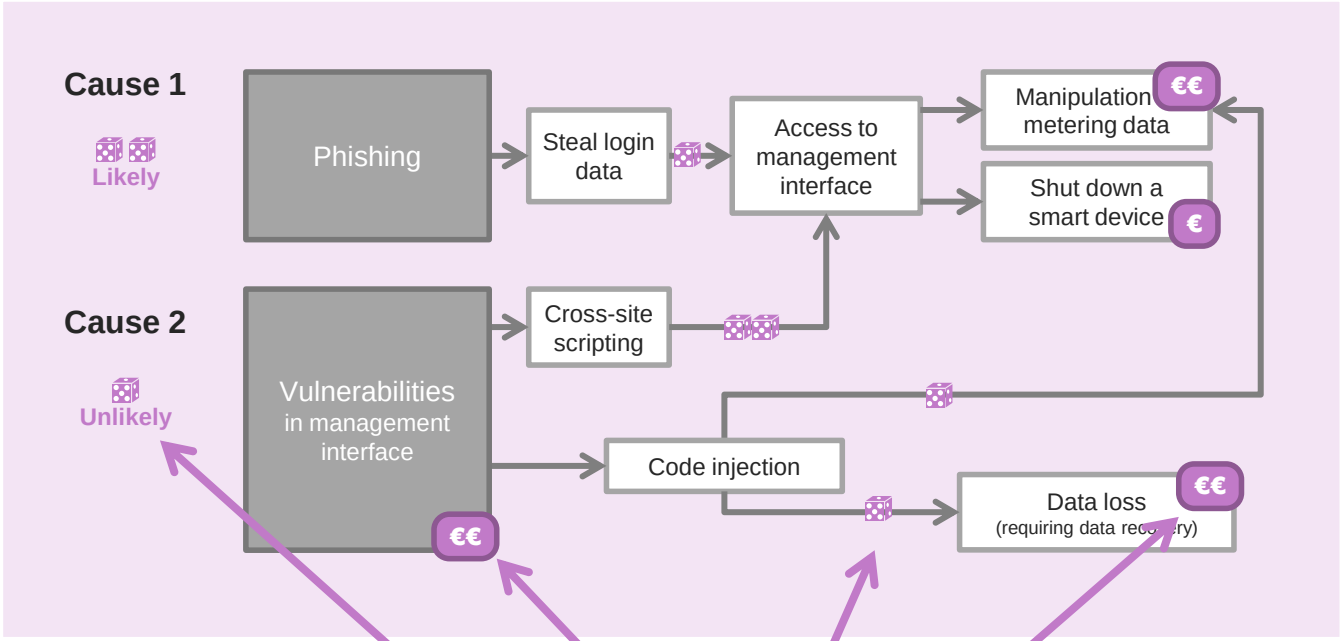
CRITIS 2016

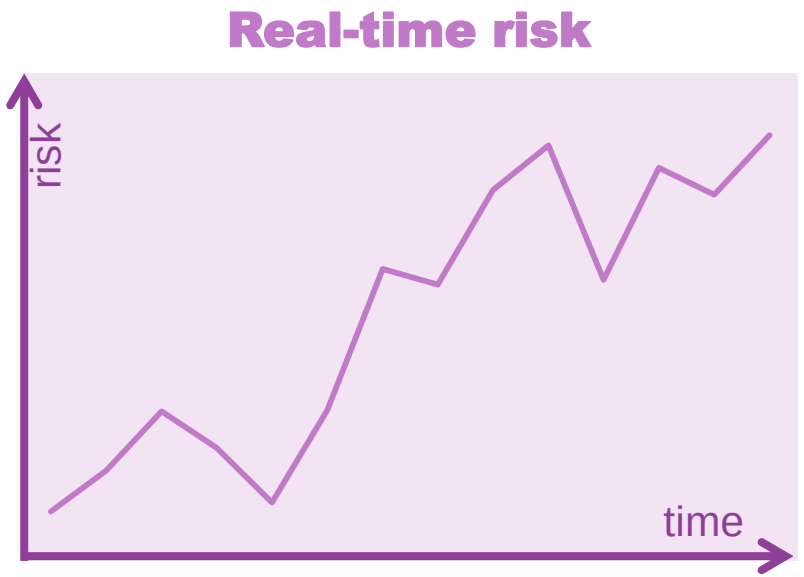
Risk matrix (anonymised)

	I[·]	L[·] × I[·]	CSRF	Improper/missing input validation	Brute force	Broken or missing authentication	Buffer overflow	Social engineering	Distributed Denial of service attack	Manipulate/block flows from field devices (DC; SM)	Physical access to facility	Access to admin network	Data concentrator physical intrusion	Smart meter physical intrusion	(bug/time/unknown cause)	Data center incident (fire..)	Construction fault	Attrition/Age	Data concentrator defunct/destroyed
L[·]	-	-	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
L[·] × I[·]	-	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
Reputation loss	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
Electricity theft	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
Grid failure	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Scenario]	###	###	###	###	###	###	###	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Scenario]	###	###	###	###	###	###	###	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Scenario]	###	###	###	###	###	###	###	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###
[Scenario]	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###	###

Probability that a **root cause** (column) engenders a **security event** (row)

Outlook: dynamic risk analyses





Measure these dynamically

Thank you!

This work was supported by

Fonds National de la Recherche Luxembourg

(project reference 10239425)