Modelling cyber-threats in the Airport domain: a case study from the SECONOMICS project

Workshop ECRIME
Rome, 19 January 2015

Alessandra Tedeschi, Deep Blue S.r.L, Rome, Italy

Project overview

- SECONOMICS is a 36 months project funded in the FP7 Security Theme.

- SECONOMICS goal is:
  - To synthesize **sociological**, **economic** and **security science** into a usable, concrete, actionable **knowledge for policy makers** and **social planners** responsible for citizen's security.

Project approach

- **Sociology**
  - Assess public perception and acceptability to risk and security rules
- **Risk Analysis**
  - Analyze the role of mathematical models in predicting behavior of attackers and defenders and providing guidance on efficient security investment
- **Economics & Public Policy**
  - Study models that can capture the agency, public good and externality issues involved in managing security.

- The project is:
  - **Driven by industry case studies** and will specifically identify security threats in transport and critical infrastructure.

Case studies

Airport Security

Anadolu Airport & Deep Blue

SECONOMICS

Case studies

Critical infrastructure

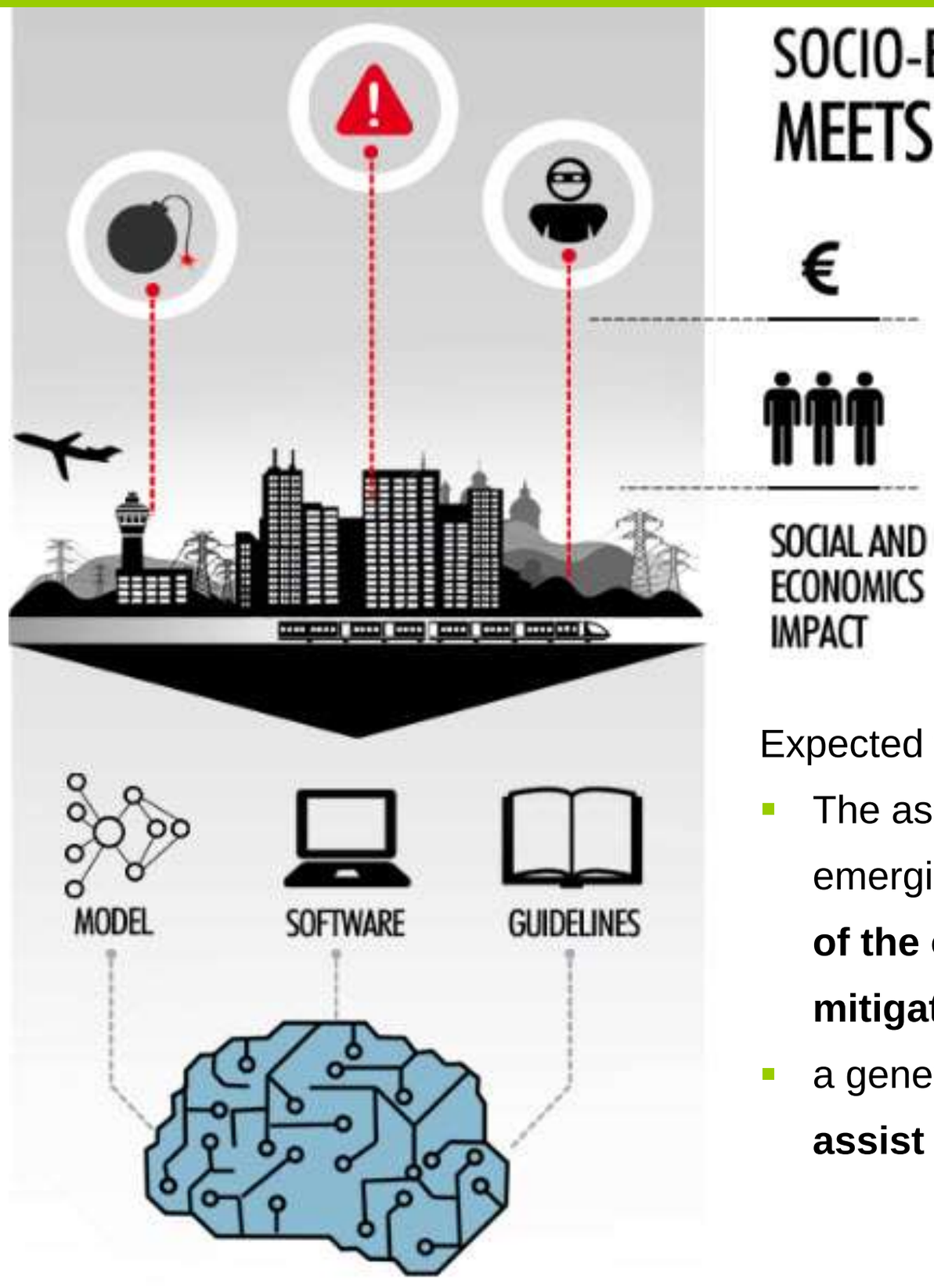
National grid

Case studies

Local Transport

TMB Barcellona Metro

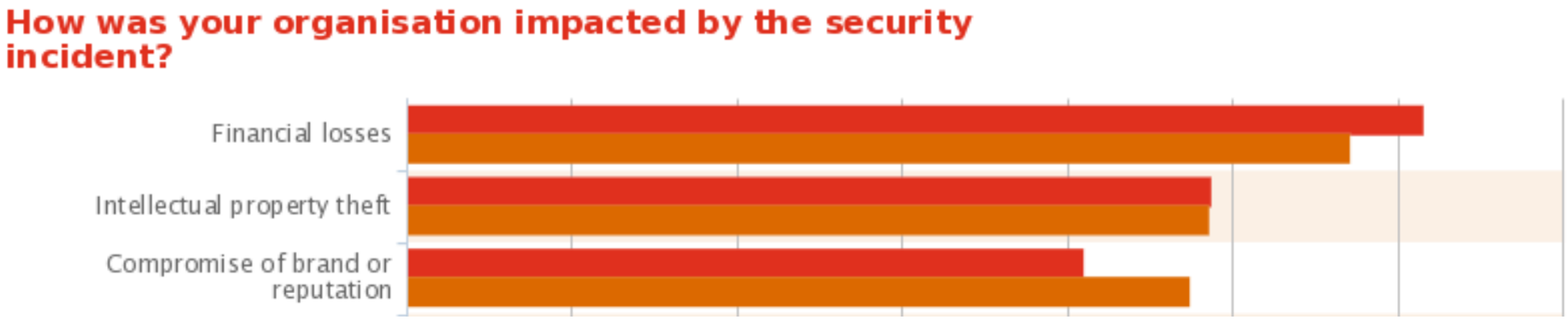
Summarizing SECONOMICS



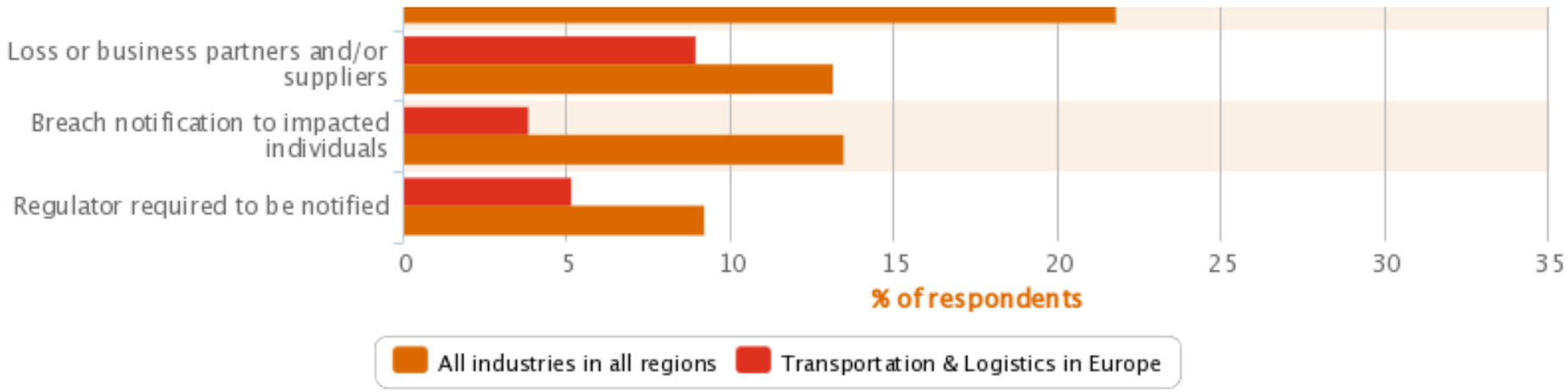
Expected final results:

- The assessment of the future and emerging threats with **rigorous models of the optimal mechanisms for mitigation** within the policy domain.
- a generalized **policy "toolkit" that will assist decision makers.**

Cyber Threats in Transportation & Logistics



Critical transportation infrastructures are increasingly suffering numerous cyberattacks committed by individuals or groups of hackers, who are moved by different motivations and are attempting to alter, damage and/or take control over IT systems or networks.



Source: PwS “The Global State of Information Security 2013”

SECONOMICS

Airport Cyber-Security

Airports are complex organizations that encompass advanced IT infrastructures for

- the **real-time exchange of sensitive data**,
- technologies for **scanning and monitoring** the passenger flow,
- **trained and skilled operators**,
- many different **organisation interacting**,
- **complex procedures and rules**,

being vulnerable to a multitude of attacks and IT-based emerging threats.

Reported Airport Security Cyber Attacks - Few Cases

Indira Gandhi International (IGI) Airport attack to the passenger processing system (2011)

Direct impact: approx. 50 flights delayed and their passengers had to be manually checked in.

http://www.zdnet.com/blog/india/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june/710

Airports Authority of India (AAI) cyber security at risk (2012)

Serious vulnerabilities in the cargo management system at Chennai, Coimbatore, Kolkata, Amritsar, Lucknow and Guwahati airports reported by the National Technical Research Organisation (NTRO).

http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html

Uncovered malware hidden in the private network (VPNs) of a major non-U.S. international airport (2012)

The Citadel Trojan malware was discovered during a routine security sweep of the 30 million PCs protected by Trusteer's software.

http://www.businessweek.com/articles/2012-08-15/cyber-wars-reach-a-new-frontier-the-airport

Cyber attack against the Istanbul Ataturk International Airport (2013)

The passport control system at the departure terminal was hit causing many problems at the Istanbul Ataturk International Airport.

http://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html

Seconomics for Airport Cyber-Security

- Two different approaches were proposed:
  - The Adversarial Risk Analysis (ARA) model has been adopted to provide airport management organisations with an **optimum portfolio of preventive security measures** for the scenario under analysis
  - Game Theory Economic Models applied to the analysis of proper **regulatory models for fair cyber-security cost allocation in the airport domain**

Development of an Airport Security Scenario for ARA models

On the basis of real attacks analysis and field research, **potential future scenarios** have been developed that ought to:

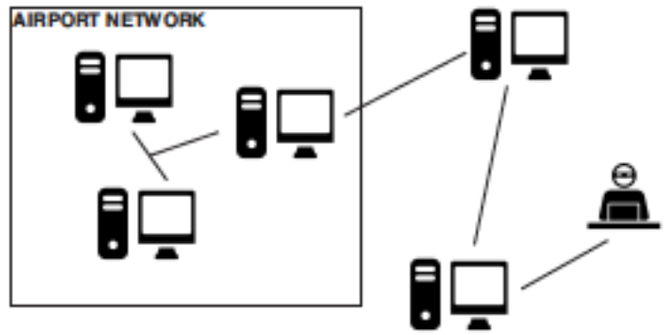
- be **representative** of the airport environment, with representative risks
- include **threats** poised to become more impactful, or more widespread, or to migrate in the airport infrastructure, contributing to the overall risk of the airport's assets, operations or users.

The case, and the estimations, addresses a
Southeastern European small-size international airport,
with an average budget of 2–3 millions euros per year, with around 5% of the total budget spent on security and less than ten connections per day.

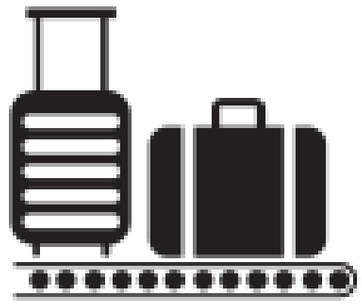
SECONOMICS

Cyberthreat

➢ One of the most fierce **green hacktivist group** in Europe aims at **gaining visibility in media outlets through a cyber attack**



➢ Taking advantage of the lack of staff training in IT security, the hacktivists implement and execute a **spear phishing attack** targeting airport IT systems administrators. The infected attached documents or links then give a **backdoor in the systems to the attacker**, with the target access privileges.



➢ **A malfunction in the baggage handling and management systems is caused**. This provokes a switch back to manual procedures for baggage checking and routing and thus flights delay.

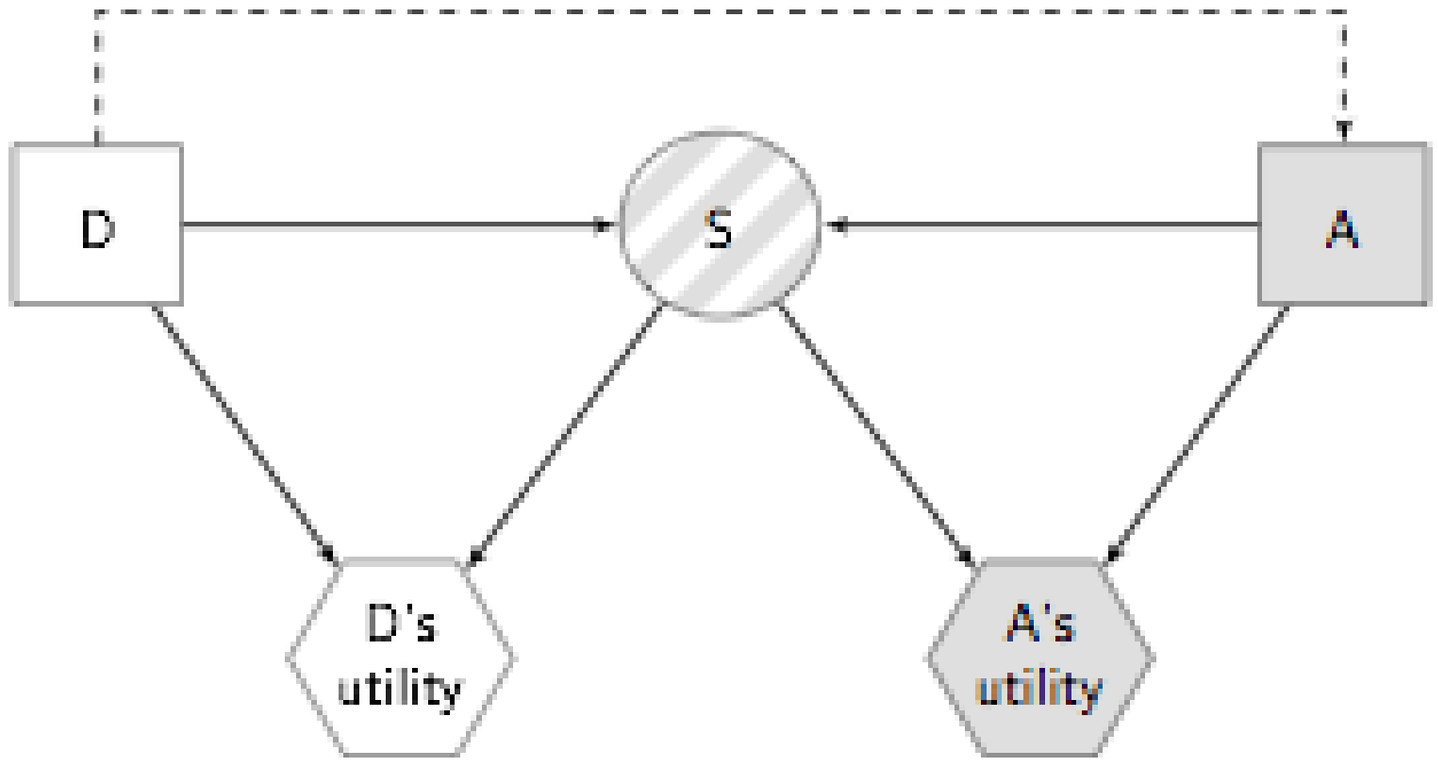
The Adversarial Risk Analysis - ARA Model Applied

The Adversarial Risk Analysis model has been adopted to provide airport authorities with the **optimum portfolio of preventive measures** in the scenario.

> The **ATTACKER** faces uncertain situations and needs to make a choice from a set of available actions each having **different probability** of yielding an outcome.
She decides which action he will make based on his **belief in the utility.**

> The **DEFENDER** formulates strategies based on **compliance with policy and regulation** and with what she know about hackers to deter them from attacking her IT infrastructures.

The ARA Model Applied: The Influence Diagram



The uncertainty associated with the **success of an attack S is probabilistically dependent on the actions of both the Attacker and the Defender (S | d, a)**

The arc from the Defender's decision node to the Attacker's reflects that the **Defender's choice is observed by the Attacker.**

Utility functions over the consequences for the Defender and the Attacker are computed by **maximising positive impacts** and **minimising negative ones** for each actor.

Defender Dynamics

Strategy of airport authorities to protect their IT infrastructures against the actions of hackers according to procedures:

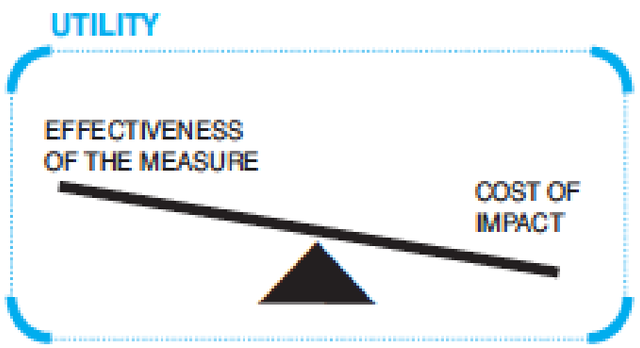
D1. Define a **security program** covering and implementing the elements of the five security areas: governance and people, policy, processes, procedures, controls.

D2. Implement **continuous monitoring, periodic analysis, audit and up-date**.

D3. Implement **attack response** on event discovery.

The dynamics for the **DEFENDER** are:

1. She invests a **portfolio of security measures** x = (x1, x2, x3, x4), incurring in a cost CD.
2. She faces the **operational costs in relation with an eventual cyberattack** (assure continuity, deploy remediation, perform forensics).
3. She gets her **utility**, which depends on the hypothetical costs caused by a successful attack and the investment costs.



Costs of Security Measures

Defender step	Control Area	Security Measure	Estimated Cost	Effectiveness
D1	CA1. Governance and People	Security governance	€40k	60%
		User awareness and training	€20k + €20k	
		Enforcement of measures on infractions	€5k	
		Background checks on employees and 3rd parties	€5k	
	CA2. Policy and Processes	Information security policy	€25k	50%
		Data management policy		
		Computer and data use policy		
		Security processes and procedures	€10k	
	CA3. Technical controls	Network segmentation and firewalls	€40k	75%
		Antivirus	€15k	
		IDS/IPS	€30k	
		VPN endpoints	€10k	
D2	CA4. Operations	Continuous monitoring of alerts related to system/application access, integrity monitoring, and network traffic	€18k (1FTE IT operator/1yr)	80%
		Periodic security risk analysis and vulnerability assessment	€6k (1FTE Security manager/3m)	
		Periodic user recertification	€2k (1FTE Security manager/1m)	
		Periodic update of critical software and configurations	€3k (1FTE IT operator/2m)	
D3	CA5. Attack response	Deploy emergency measures	€10k-€100k	90%
		Perform forensics	€80k	
		Deploy remediation measures	€20k-€80k	
		Update security areas	€10k-€40k	

SECONOMICS

Attacker Dynamics

Attacker dynamics:

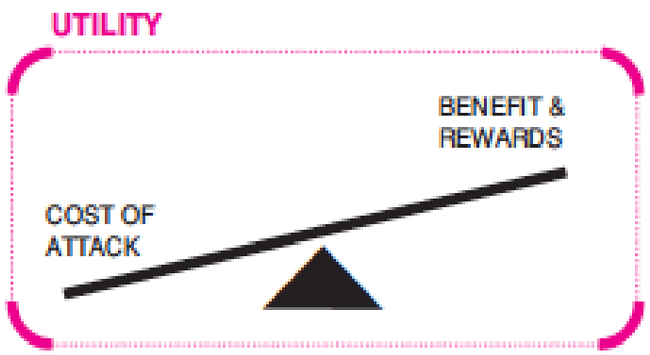
A1. **Recon**

A2. **Weaponize**

A3. **Attack** execution

The **ATTACKER**, as an intelligent opponent:

1. sees the **security investments** x, i.e. we consider a Sequential Defend-Attack model.
2. decides what **type of attack** they will undertake.
3. faces the **operational costs** CA in monitoring defender security measures and preparing the attack.
4. gets **the corresponding utility**, which depends on both the benefits She may get from a successful attack and the costs entailed to implement her decision.



SECONOMICS

Intelligence Costs for the Attacker

Attacker step	Attack action	Attack element	Estimated costs
A1	Gather intelligence	Internet search	€1.5k (1FTE Junior Computer Scientist/1m)
		Phone calls	-
		Hacking clients/partners/ contractors	€0 – 10k
	Identify exploitable vulnerabilities	Software vulnerabilities	€1.5–7.5k (1FTE Junior Computer Scientist/1–5m)
		People /social engineering	€4.5k (1 FTE/3m)
A2	Select vulnerability	Cost effectiveness assessment	—
	Prepare exploit	Buy/develop exploit code	€200– 60k (average €2.5k) / €1.5k (1FTE Junior Computer Scientist/1m)
	Prepare delivery method	Spear phishing set up	€375 (1FTE Junior Computer Scientist/1w)
	Finalize crafting attack	All attack parts engineered together	€375 (1FTE Junior Computer Scientist/1w)
A3	Deliver	Crafted email	—
	Exploit	Trigger the exploit	—
	Command and control	Collect further intelligence	€375–1.5k (1FTE Junior Computer Scientist/1w–1m)
		Cover tracks	—
		Reach target system	—
	Activation	Manipulate systems and/or data	€375–4.5k (1FTE Junior Computer Scientist/1w–3m)
		Affect levels of service of the target	—
		Cause harm to the target or its clients	—

Preliminary Results

The ARA model provides the **optimum portfolio of preventive measures** for an average budget of 125,000 euros to invest in two different cases:

(1) experienced cyber-attackers needing shorter preparation times and with higher rates of success;

> the defender will tend to invest on the **most effective and most expensive measures** and this fact prevents them from investing on other cheaper but less effective areas.

(2) novice hacker group having incomplete technical knowledge or insight into the airport's organization.

> airport authorities would tend to invest on **more measures**, aiming at covering asmany control areas as possible, although not necessarily investing on the most effective ones.

Extensions & Future Works

The model is open to extensions, such as e.g.

- airportsof different **size** and with different **peculiarities**
- **larger and more complex technical infrastructures**,
- **new threats** (more than one intelligent attacker),
- additional **recovery measures** deployed by different agents (sequential Defend-Attack-Defend model with more than one defender).
- **networks effect** on more than one airport

Q&A

alessandra.tedeschi@dblue.it