



The Role of Economics in Cybersecurity

Muriel Figueredo Franco¹, Bruno Rodrigues¹, Aljosa Pasic², Burkhard Stiller¹

¹ Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH, Switzerland
{franco, rodrigues, stiller}@ifi.uzh.ch

² Atos Research and Innovation ARI, Madrid, Spain
aljosa.pasic@atos.net

Agenda

- Introduction and Basics
- Related Fields
- New Approaches
 - SEConomy Framework
 - Protection Recommendation
- Discussion and Conclusions

Introduction and Basics

Introduction


- As businesses and governments go digital, they are exposed to **increasing number of threats**
 - ⇒ Governance, risk assessment, security assessment, and operations management are critical for digital era
- Cybersecurity is no longer “just” a technology perspective
 - ⇒ **Societal and economic** impacts equally important



Technology Intelligence

**WannaCry cyber attack cost the NHS
£92m as 19,000 appointments
cancelled** [Telegraph, 2018]

Cybersecurity Facts




Frequency of **DDoS attacks**
increased more than 2.5 times
between 2014 and 2017 [Kaspersky 2018]

DDoS attacks averaged between
\$ 20,000 - \$ 40,000 per hour
[Kaspersky 2018]

*Cyber threats are
increasing*

Financial losses



34% of businesses hit with
Ransomware took a week or more to
regain access to their data [Symantec 2018]

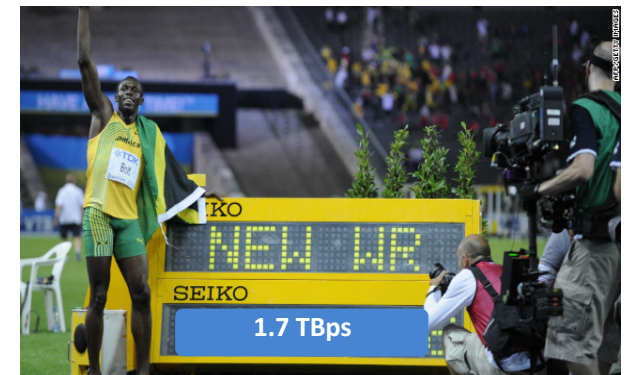


The global Ransomware damage
costs are **totaling around \$ 11.5
billion** [Cybersecurity Ventures 2019]

Real-world Cases

- Rheinmetall AG (Germany) was infected by a **Ransomware** at the end of September 2019
 - Weekly losses of approx. \$ 3-4 million
 - Recovery time expected to be approx. 4 weeks
- **Mishandling of private keys** lead to losing \$ 155 millions in Bitcoins
 - QuadrigaCX case (Canada)
- The biggest **DDoS attack** to date occurred on March 5, 2018
 - 1.7 TB/s attack on GitHub

DDoS: Distributed Denial-of-Service



Predictions

Damage related to cybercrime will hit **\$ 6 trillion** annually by 2021

[Cybersecurity Ventures 2019]

Destruction of data, stolen money, theft of personal and financial data, business disruption, reputation harm

The total number of DDoS attacks globally will reach 17 million by 2020 [Hosting Tribunal 2019]

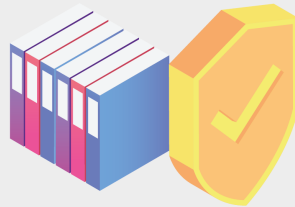
Ransomware attacks will quadruple by 2020 [Forbes Insights 2019]

Healthcare will be the main target

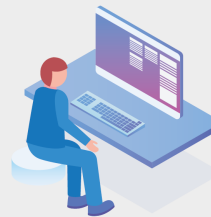




CYBER SECURITY



**Education,
Prevention**



**Monitoring,
Maintenance**



**Remediation,
Insurance**

Cybersecurity Economics' Basics

- Many problems plaguing cybersecurity are **economic in nature**
 - Systems fail because the organizations often fail to assess the risks of failure
 - Regulatory interventions may be necessary to strengthen cybersecurity measures, hardening, or awareness (the least)
 - *E.g.*, based on ENISA, ISO, and NIST
- **Different costs** have to be considered during the planning on cybersecurity support measures

$$\underbrace{Risks}_{\substack{\text{financial loss} \\ \text{reputation loss}}} \rightarrow CAPEX + OPEX$$

Related Fields

Overview of Cybersecurity Selected Work

Threat	Solutions	Insights
DDoS	[15], [40]	Blockchain-based solutions are arising to detect and mitigate DDoS attacks
Malware	[9], [29], [22], [20]	Trend technologies (e.g., neural networks and self-organizing networks) are being used to classify malwares and to plan the security to reduce ransomware impacts
Botnet	[15], [43], [5], [48], [8]	Machine learning is a trending topic of detecting botnets. As botnets have behavior patterns, artificial intelligence techniques could be useful.
Social Engineering	[27], [36], [46], [16]	Solutions are using machine learning to recognize patterns to identify imminent social engineering and protect against sophisticated attacks
Sabotage	[25], [45]	Machine learning has also been used as a tool to detect and understand the impact of cyberattacks against institutions
Others	[1], [18]	Several cloud-based solutions have been proposed to mitigate different cyberattacks (e.g., malwares, side-channel, and DDoS)

Cybersecurity Economics Modeling

- Cybersecurity Economics Modeling

- Fundamental model for investments related to various information security goals

[Loeb 2002]

- Overview on metrics and models toward a probabilistic mapping of security economics

[Böhme 2010]

- ROSI (Return On Security Investments)

- Risks Assessment Frameworks

- ISO 27005 (Risk Management Standard)

- NIST's Special Publication 800-37 and 800-53

Organizational

- ENISA, STRIDE, LINDDUN, DREAD

- AFCEA: cybersecurity economics in a practical framework

- Idea of creating cost categories for the different threats

Mapping of
Cyber Risks

SECCORD and IPACSO

- Establishing, preserving, and increasing CIA

- Specificities of cybersecurity
 - Economic models
 - Incentives
 - Mix of proactive vs. reactive security
 - New versus existing security controls
 - Trade-offs
 - Effective engineering
 - Cost of non-compliance
 - Externalities (e.g., network effects)
 - Information asymmetry
 - Ambiguity bias (preference for proven tech)
 - Risk perceptions
 - Learning effects
- CIA: Confidentiality, Integrity, Availability



SecCord

effectsplus



VALUESEC and SECONOMICS

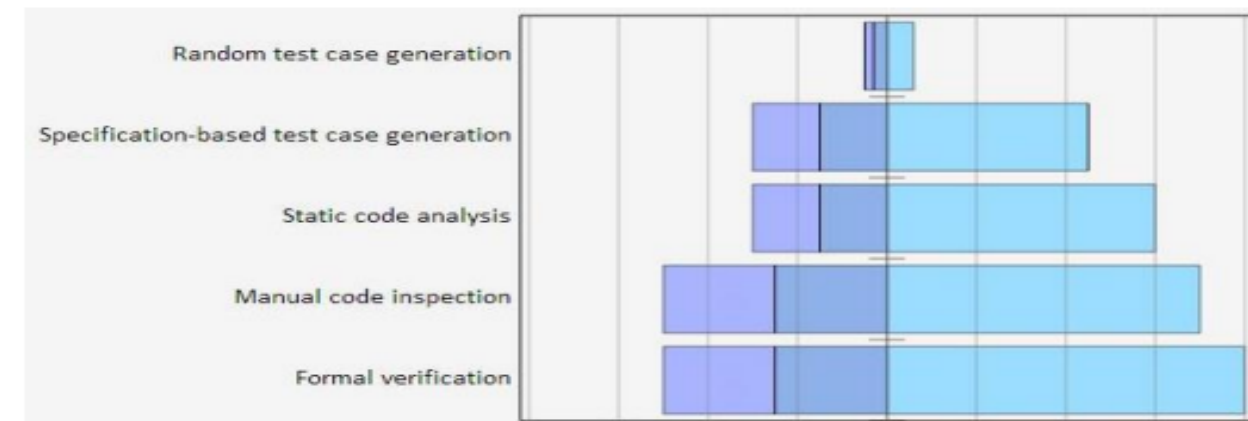
- From physical security to cybersecurity
 - **Measure uncertainty** (*things will happen we have not thought about or expected*)
 - **Model complexity** (multi-stakeholder, multidimensional scenarios, threats, vulnerabilities, damages, *conflicting interests, externalities*)
 - **Multitude of methods and tools; lack of data** (*no “always best” or “one size fits all” method and tool*)
 - **Value function =**
risk reduction + cost benefit + qualitative criteria



Lessons Learnt

- Effectiveness of manual intervention
(Valuesec: big RRA, small CBA and QCA)
- Assessment over large period changes
(CIRAS: no break-even point in cybersecurity)
- Effectiveness of risk assessment
(SECONOMICS: visual vs. textual tools)
- Usefulness of scoring systems as a risk factor
(SECONOMICS: importance of data source)
- Investment in early stages of software development vs. later stages
(NESSOS: application to tools in different scenarios)

ValueSec Context	Scenario chosen	Use case(s) = Security Measures	Possible Decision Motivation
1. Public mass event	F1 Terrorist threat, Valencia	Grandstand protection and access control	Political image and local businesses
2. Mass transportation	Compromising of high speed trains in a depot	CCTV coverage, sensors and improved Command & Control	Cost-effective prevention of business damages
3. Aviation	Terrorist threat to a major European airport hub	Advanced LAG detection devices	Reduction of low-probability-high impact risk
4. Communal security	A Flood-prone area in Germany	Protection and flood management measures;	Publicly acceptable and effective area protection
5. Cyber security	ICT threats to major energy infrastructures / SCADA system	Policy and procedural measures and standards across Europe	Setting new policy for central certification and monitoring



New Approaches

SEconomy Framework

Recommendation of Protection Services

Today's Deficits

- **Ensuring certain security levels** is not a straightforward task due to number of participants potentially managing sensitive information or critical tasks
 - Important to map systems and processes and their correlations as well as related costs
- **Several protections** and configurations available on the market
 - Not trivial to choose one in order to achieve a proper level of cybersecurity, while reducing end users costs
 - *E.g.*, acquisition, deployment, configuration, and management
- **Cyber insurance** can benefit from new and profitable market
 - Hard to quantify risks and exposure to cyberattacks

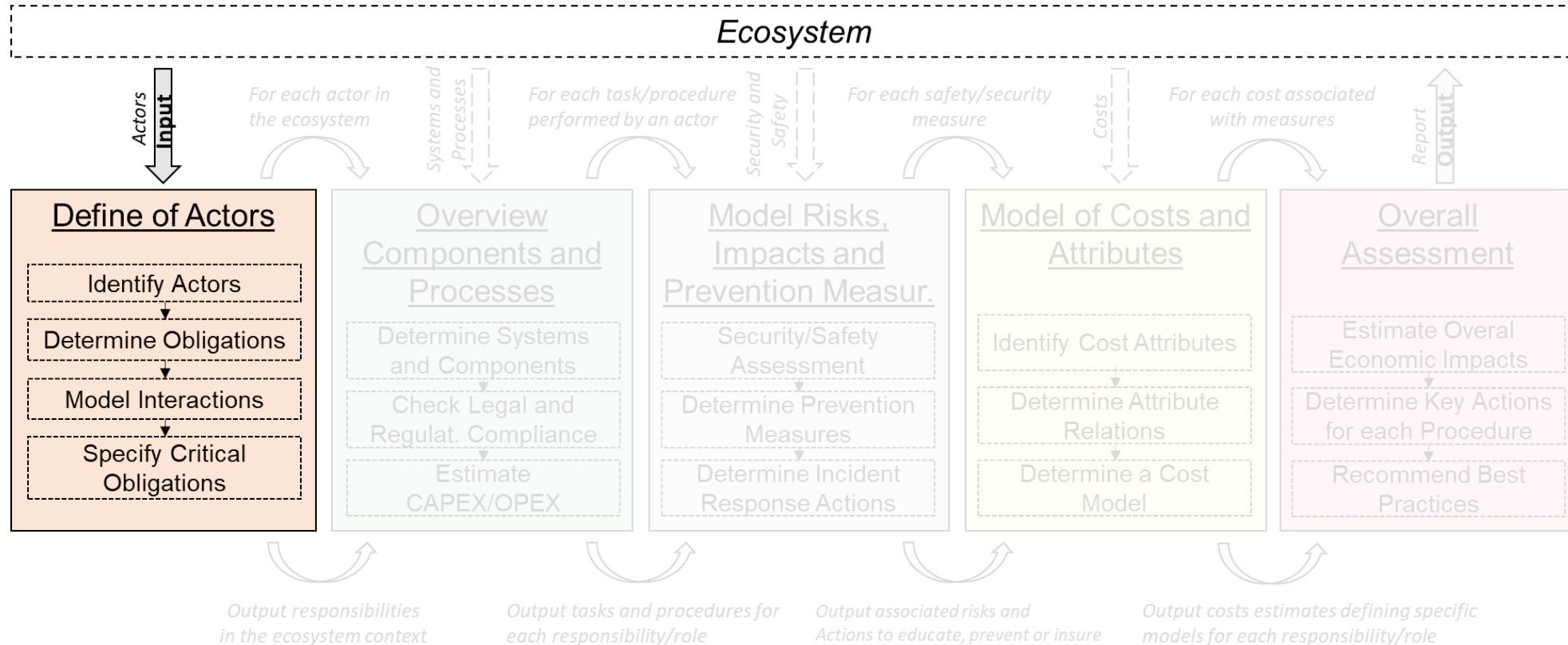
New Approaches

SEconomy Framework

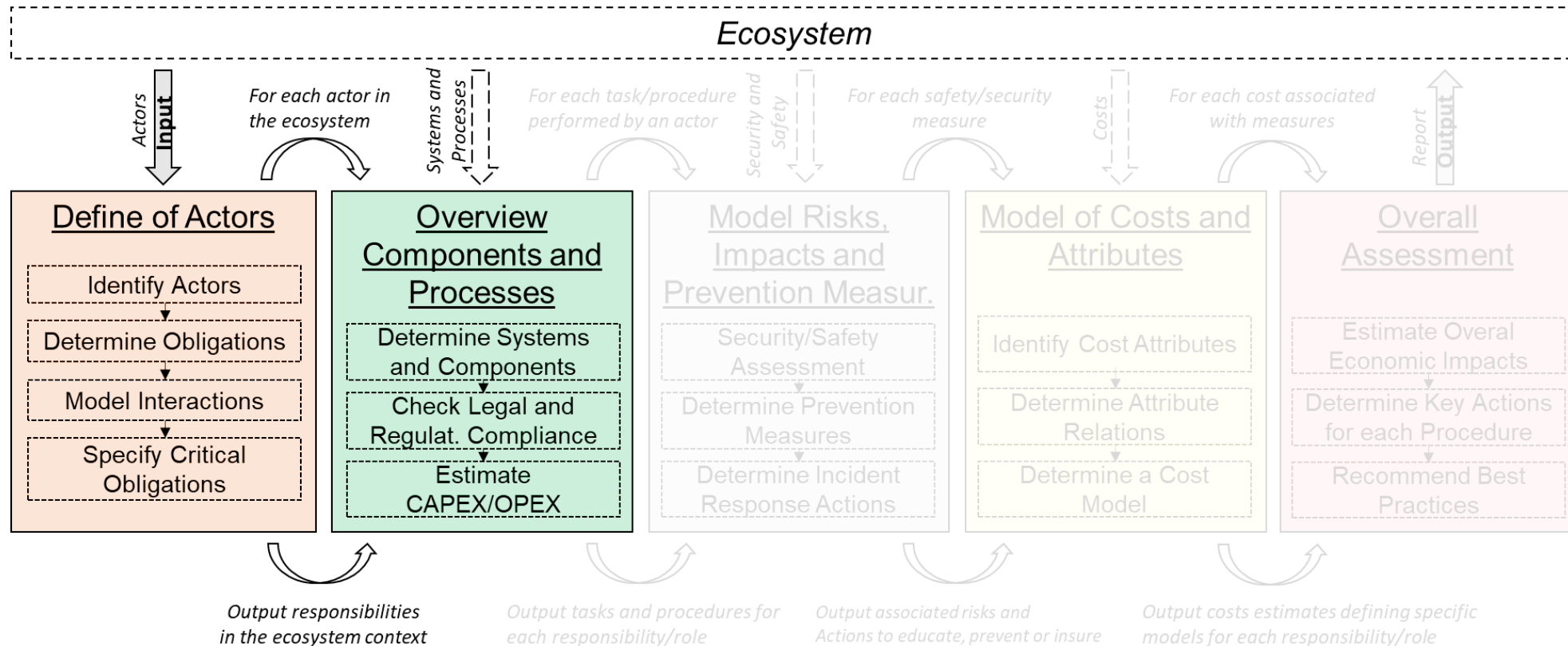
SEConomy Framework Overview

- Identify security risks and associated costs
 - Mapping/modelling specific attributes and their relation
- Determine impacts of cyber (in)security in the economy
 - Education, prevention, remediation, insurance
- SEConomy is a framework to **assess cybersecurity economics**
 - Structured view on critical actors, roles and processes, and their associated critical tasks
 - Map of risk-dependencies between systems and related systems/subsystems
 - Associate time-dynamics with classes of costs

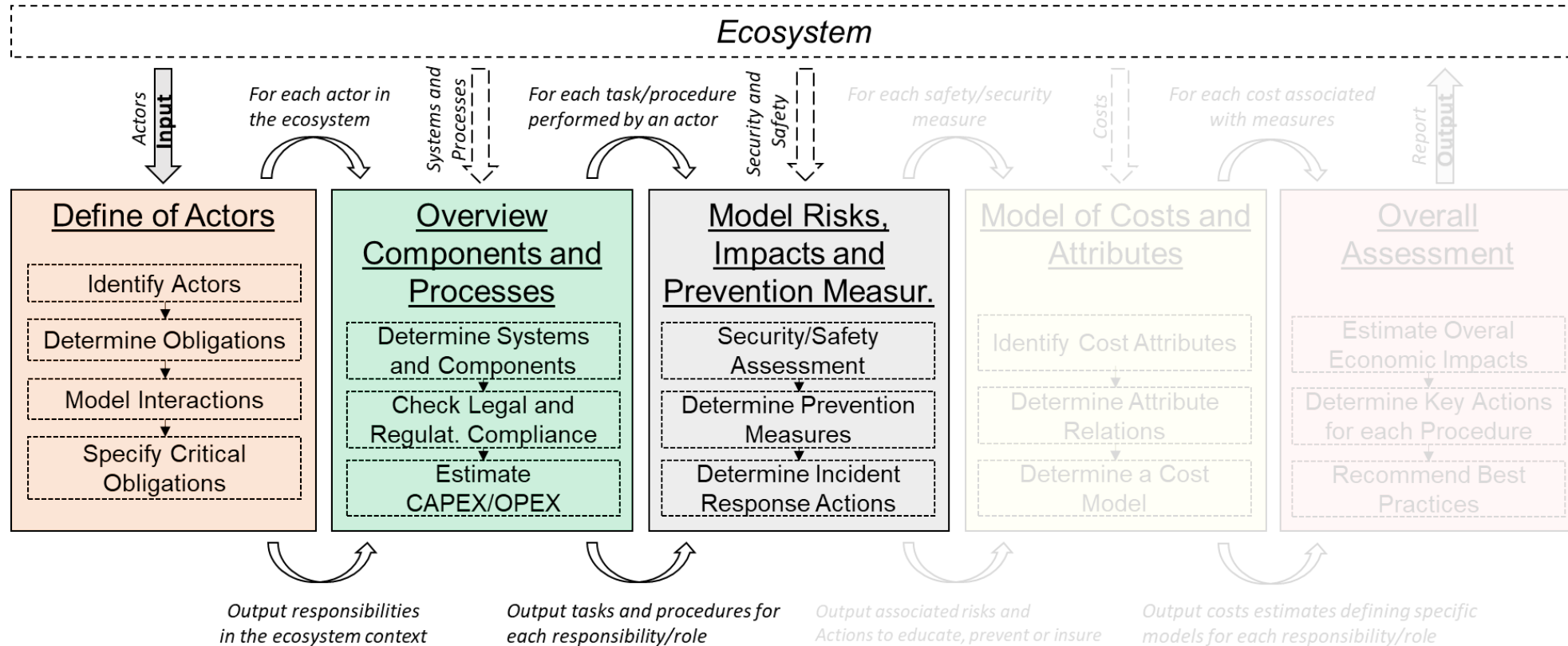
Step-based Approach



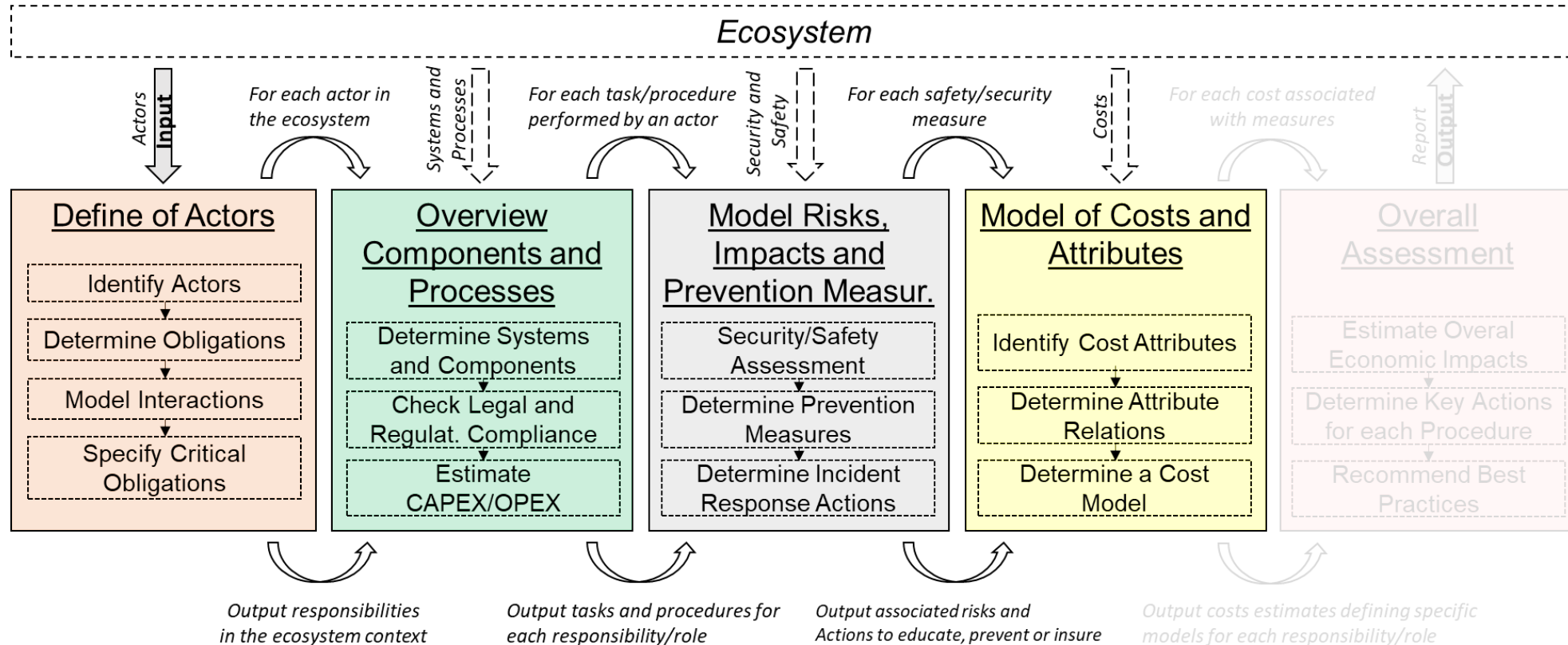
Step-based Approach



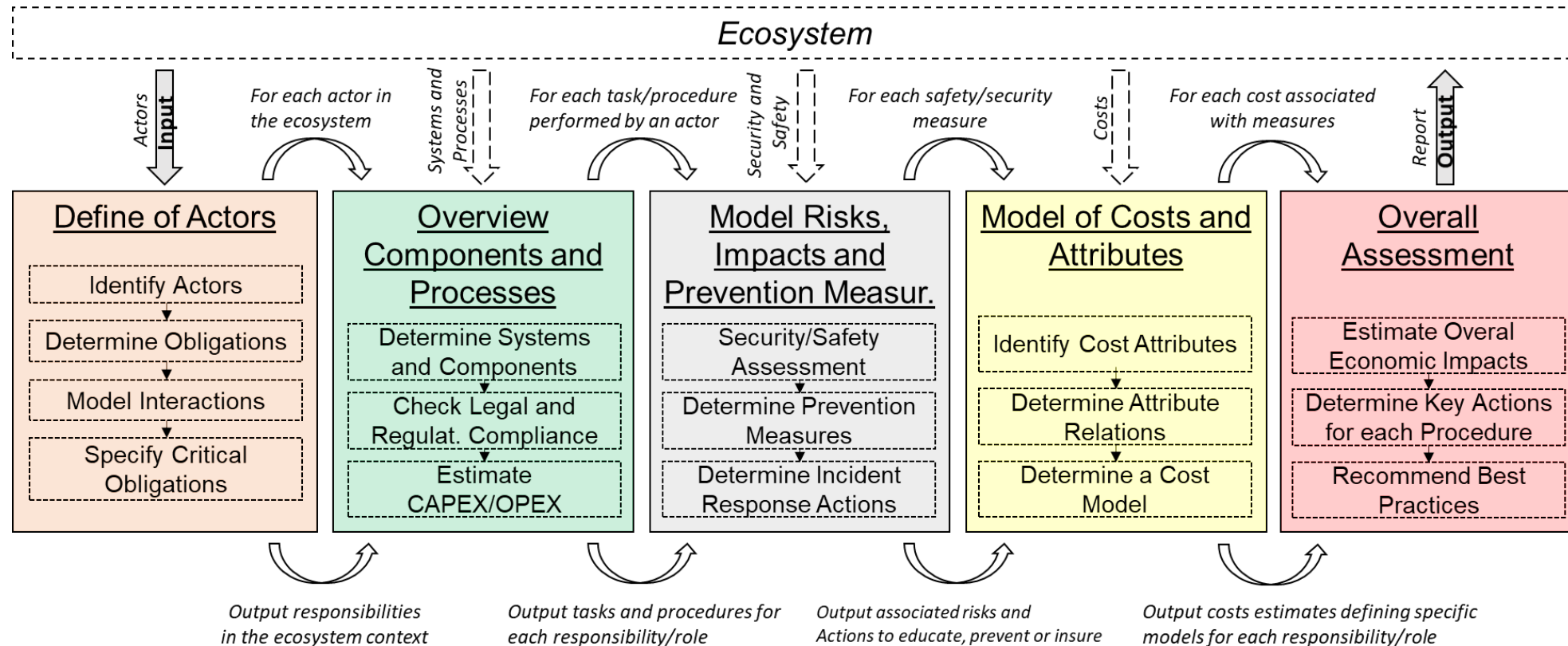
Step-based Approach



Step-based Approach



Step-based Approach



Overall Cost Assessment

Algorithm 1: Overall Economic Assessment (OEA)

```

1 begin
2   for each Actor ∈ Ecosystem:
3     for each Role ∈ Actor:
4       for each System ∈ Role:
5         /* Correlation between linked systems in Equation 1 */
6          $p(x) \leftarrow dependence(System, \forall linkedSystems)$ 
7         /* Estimate exposure costs in Equation 2 */
8          $threat_{costs} \leftarrow T_{costs}(A, p(x))$ 
9         /* Estimate mitigation (Proactive and Reactive) costs
           in Equation 3 */
10         $mitigation_{costs} \leftarrow PMC_{costs}(A)$ 
11         $mitigation_{costs} \leftarrow RMC_{costs}(A, p(x))$ 
12        /* Get Overall Economic Assessment (OEA) in Equation 4
           */
13         $OEA \leftarrow ROSI(threat_{costs}, mitigation_{costs}, InitSecCost)$ 

```

$$ROSI = \Delta T * \sum_{i=1}^{N_{System}} \frac{(T_{costs} * RMC) - PMC}{PMC}$$

Instantiated Use Case: Ransomware Analysis

- Initial evaluation of SEConomy Framework based on a real case
 - Further evaluations can follow as Concordia requirements arise
- Actors and Roles
 - **Company** wanting to protect itself from cyber threats
 - **Insurer** wanting to make profit and minimize risk
 - **Competitor** of company working as business antagonist
 - **Malware operator** wanting to extort money

Return On Security Investment (ROSI)

- For doing backups:

$$ROSI_{backups} = \frac{\text{Loss Expectancy} - \text{Solution's costs}}{\text{Solution's costs}}$$

$$ROSI_{backups} = \frac{downtime[d] * daily\ revenue[\$/d] - data[TB] * backup\ cost[\$/TB]}{data[TB] * backup\ cost[\$/TB]}$$

- For insurance:

$$ROSI_{insurance} = \frac{RMC - (PMC + (1 - coverage\ factor) * RMC)}{PMC + (1 - coverage\ factor) * RMC} = \frac{coverage\ factor * RMC - PMC}{PMC + (1 - coverage\ factor) * RMC}$$

$$= \frac{coverage\ factor * downtime[d] * daily\ revenue[\$/d] - insurance\ cost[\$]}{insurance\ cost[\$] + (1 - coverage\ factor) * downtime[d] * daily\ revenue[\$/d]}$$

- For backups with insurance present:

$$ROSI_{backups|insurance} = \frac{insurance\ cost[\$] + (1 - coverage\ factor) * downtime[d] * daily\ revenue[\$/d] - (PMC_{backups} + insurance\ cost[\$])}{PMC_{backups} + insurance\ cost[\$]}$$

$$= \frac{(1 - coverage\ factor) * downtime[d] * daily\ revenue[\$/d] - data[TB] * backup\ cost[\$/TB]}{data[TB] * backup\ cost[\$/TB] + insurance\ cost[\$]}$$

Use Case's Numerical Assessment

$$ROSI_{backups} = \frac{\overbrace{downtime[d] * daily\ revenue[\$/d]}^{\text{Loss Expectancy}} - \overbrace{data[TB] * backup\ cost[\$/TB]}^{\text{Costs}}}{data[TB] * backup\ cost[\$/TB]}$$

- 23.1 days downtime
- Daily revenue of \$9,095.59 USD (Gibson/Banik 2017)
 - Hotel in Marriott chain
- \$48 USD/TB backup cost
- 11.1 TB business data
- **ROSI** of 393.35 (> 1)

New Approaches

Recommendation of Protections

Recruitment Overview

- Assisting network measures to protect
- Indicating protection profile and (b) customer

Parameter
Type of Service
Type of Attack
Attack Details
Region
Deployment Time
Leasing Period
Budget

```

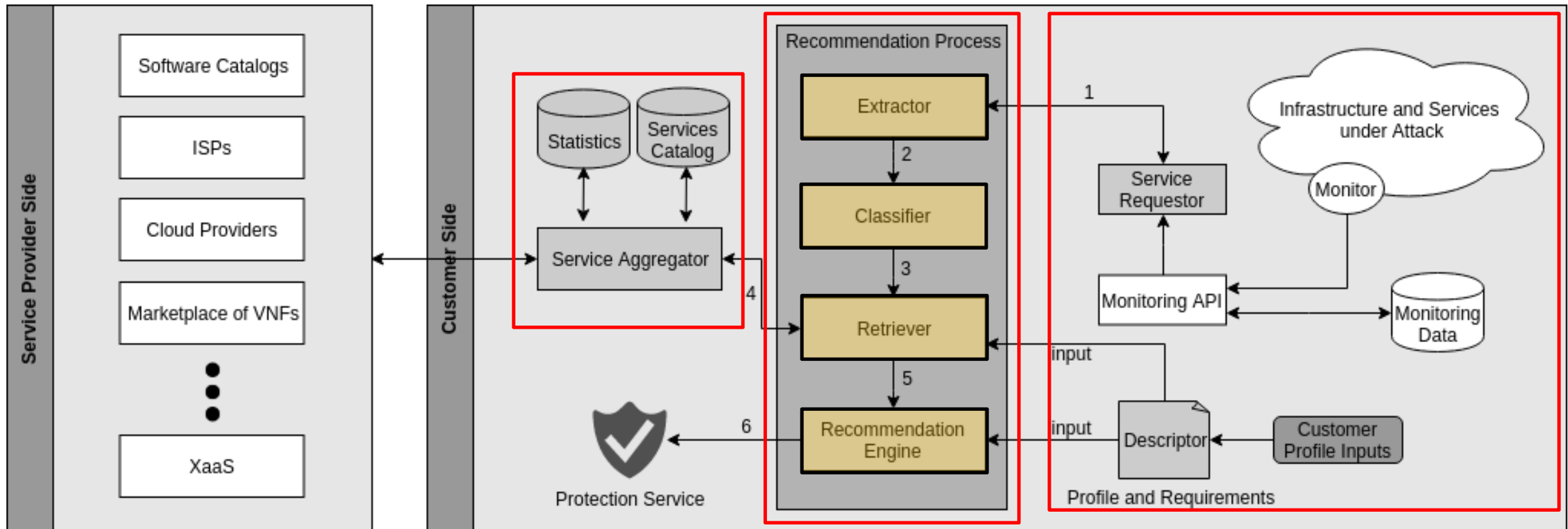
{
  budget: "200 USD",
  requirements: {
    protection_type: "Reactive",
    region: "Europe",
    deploymentTime: [
      "minutes"
    ],
    leasingPeriod: [
      "days"
    ],
  },
  infrastructure: {
    technology: "Openstack",
    services_running: [
      "Apache Web Server",
      "MySQL Database"
    ],
    protection_running: [
      "IPtables"
    ],
    priority: "high"
  },
  attack: {
    type: "SYN Flood",
    log_file: "attack.pcap",
    fingerprint: "attack.json"
  }
}

```

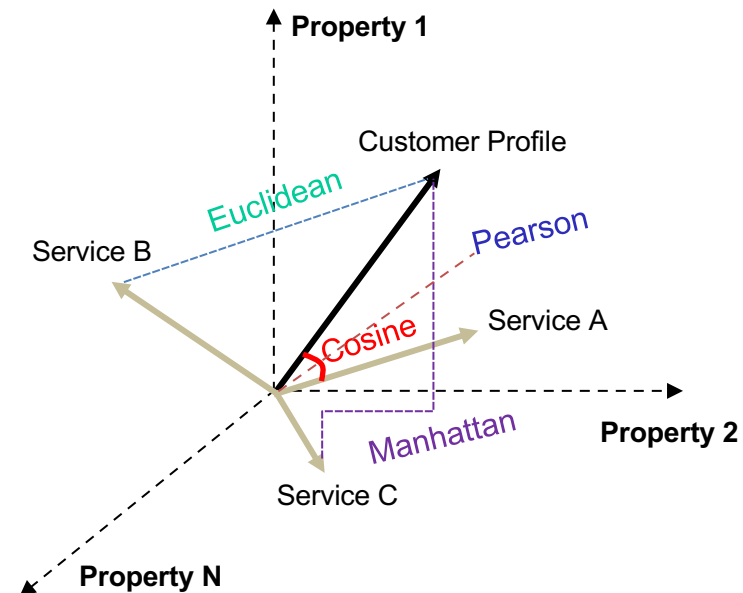
on process on
and data
account (a) customer

ck

Recommendation Architecture



Recommendation Engine: Measurement Correlations



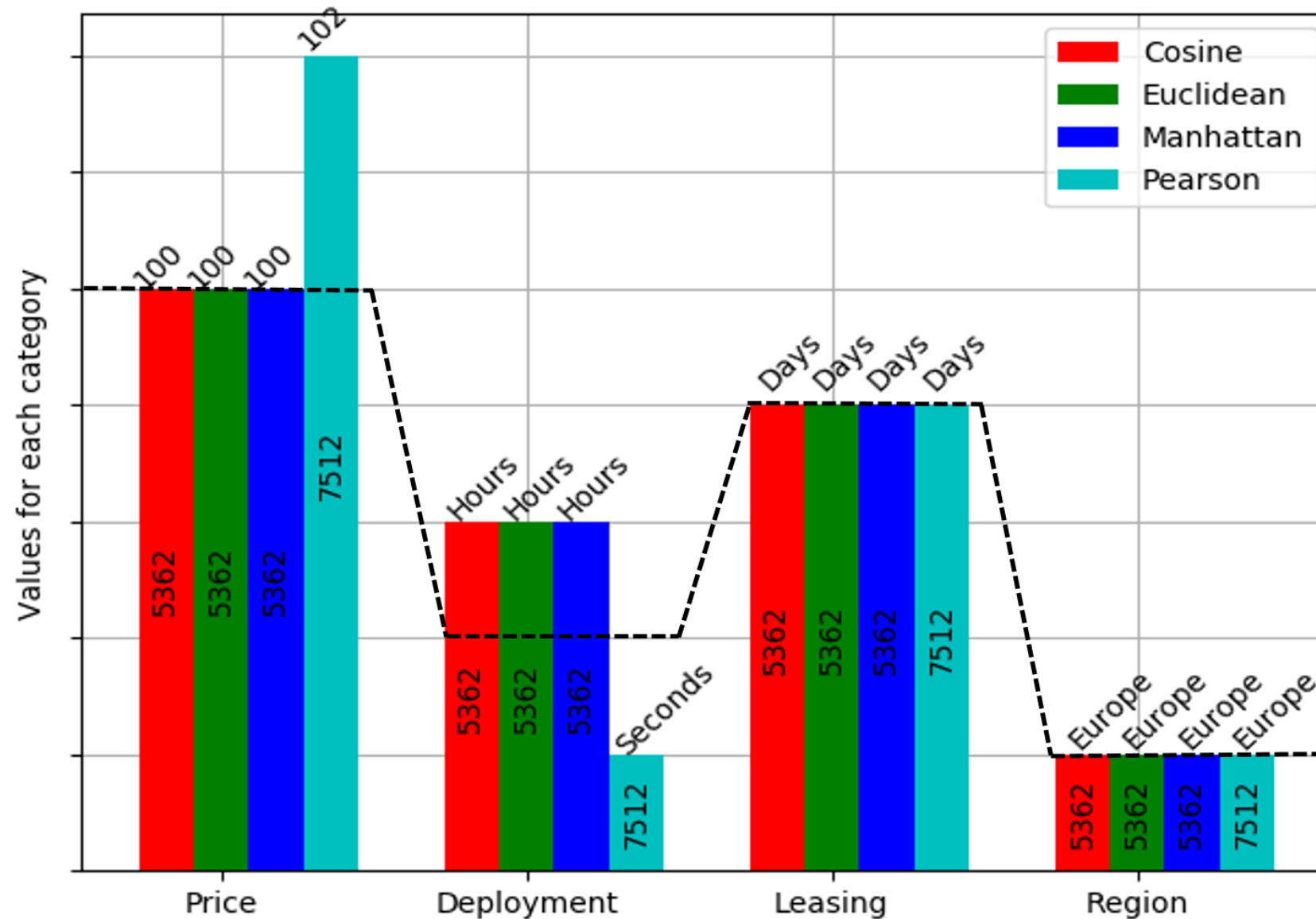
Demonstration (Proof-of-Concept)

- Customer profile representing a request for a reactive protection against a DDoS attack
 - Europe, deployment time in minutes, leasing period in days, and maximum budget up to € 5000
- Hands on

Evaluation

- Simulations cover wider and evaluate broader scale
 - However, still hard/impossible to get real data of protections available
- Scenario: **10,000 randomly generated** protections services
 - Type: Reactive, proactive
 - Price: Range from € 100 to € 1,000
 - Deployment time: Minutes, hours, days
 - Leasing period: Hours, days, months
 - Region: Europe, South America, North America

Findings



Discussion and Conclusions

Conclusions

- Cybersecurity economics involves a broad of activities
 - Education, prevention, monitoring, maintenance, remediation, insurance
- It is critical to **map systems and processes** and their correlations as well as related costs
 - Novel frameworks, standarizations, and techniques
- Approaches that help during the **decision process and planning** of cybersecurity are crucial for stakeholders
 - e.g., Customers, companies, and cyber insurers
- Future: **Blockchain** might have an important role in the future of cybersecurity economics
 - Cyber Insurance models based on Smart Contracts
 - Immutable systems of record like blockchain used to validate recovered data
 - Marketplaces and reputation systems for protection services

Thank you for your attention.