A Cost Model for Malicious Insider Cyber Crime in the Financial Industry

Vincent C S Lee

19 November 2014

Acknowledgment

- Dr Peter Ware, Director, Swift Institute for sponsoring my presentation
- Professor Graham Farr, Monash University for granting leave of absence
- Dr Mike Loginov (Moderator), Dr Chris Hurran and Professor Richard Benham for including me in the panel

Disclaimer

All references used are extract of open source data and news information. Contents of this presentation do not represent view points of any institution.

What we hope to know for risk mitigation?

Agenda

- Economic Impact of Cyber Crime
  - Motivation of cybercrime cost study
  - Arbor Networks' Solution for countermeasure and Financial Calculator
  - Security Strength-Cost model
  - Online cost simulator

Motivation

- Better understanding to quantify the economic impact of cyber attacks and observe cost trends over time;
- Develop a scenario simulation model for estimating minimum cyber attacks cost; and
- Determine the minimum appropriate amount of investment and resources needed to prevent or mitigate the consequences of an attack.

$$\text{Max } \{\text{Value of CM)}\} = \text{Max } \{\text{ALE (original)-ALE (with CM)} - \text{CM}\}$$
$$= \text{Min } \{\text{ALE (with CM)} + \text{CM}\}$$

As search vulnerability is a high cost activities for non-insider, the attackers prefer to use insider as agent to launch attacks.

Key takeaways from 2013 cost of cyber Crime study (Global study of six countries) – by Ponemon Institute sponsored by HP Security

- Cyber crimes are costly (average annualised cost of 234 organisations is US$7.2 millions per year, US$375,387 – US$58 million, 30% increase from 2012)
- Cyber attacks have become common occurrences (343 successful attacks, increased from 262 successful attacks from 2012 for 234 companies per week or 1.4 successful attacks per company per week)
- The most costly cyber crimes are those caused by malicious insiders, denial of service and web-based attacks

Banks Challenged by Cybersecurity Threats, State Regulators Acting

The basic Five Key Pillars of An Information Security Framework:

1. A written information security policy,
2. Security awareness education and employee training,
3. Risk management of cyber-risk, inclusive of identification of key risks and trends,
4. Information security audits, and
5. Incident monitoring and reporting

Observation:

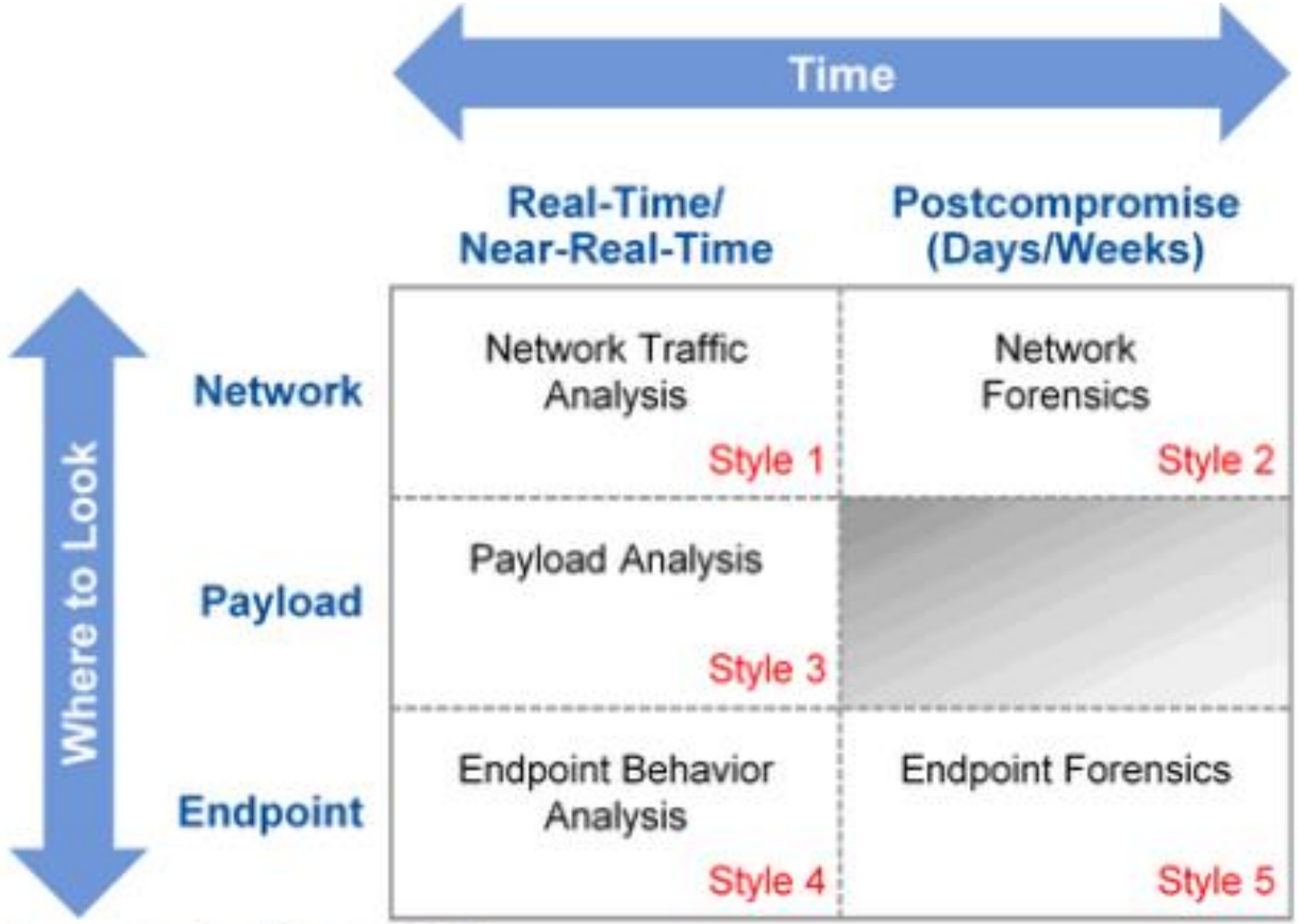
Average cost of a security breach is US$200 per record. Many breaches involves thousands and thousands of records. Cyber security costs soar at global financial institutions: experts

Cyber Attacks trends

- Turning from infrastructural to work stations, where security patches are not consistently applied
- Making use of social median to gather intelligence of targeted firms (trick employees into allowing attackers access into the systems; malware attacks launched via social media sites such as Facebook or LinkedIn
- Malware is getting smarter and nastier, example it can change signature. Major commercial anti-virus programs would not identify the malwares without intelligent tools and human and finance resources.

Source: Thomas Lewis (2014), "How to protect yourself from the rising tide of cyber attacks on financial institutions" Partner, LBMC Security Services

Five Styles of Advanced Threat Defence



Source: Gartner (August 2013)

http://www.gartner.com/technology/reprints.do?id=1-1IS72Q5&ct=130823&st=sb

CFO's interest: Comparison between most and security projects

Measures	Most Projects	Security Projects
Justification	Through Return on Investment (ROI)	Compliance or Annualised Loss Expectancy (ALE)
View	Investment	Required Cost
Benefit	Measurable	Impact measurable, Benefit is not
Issues Addressed	Long Standing	New and evolving
Incentive	Improve ROI and minimise ROI time	Minimise Cost for a given incidence

Source: Arbor Networks, Inc.

Agenda

- Economic Impact of Cyber Crime
  - Motivation of cybercrime cost study
  - Arbor Networks' Solution for countermeasure and Financial Calculator
  - Security Strength-Cost model
  - Online cost simulator

Asset Value of Enterprise Information Asset= AV

Annual Rate of Occurrence = ARO = Number of attacks in a year

Single Loss Expectancy = SLE ={Incident Response & Forensics + Customer + IT Support Cost} per incidence

Annualized Loss Expectancy = ALE = ARO * SLE

Exposure Factor = EF = SLE/AV

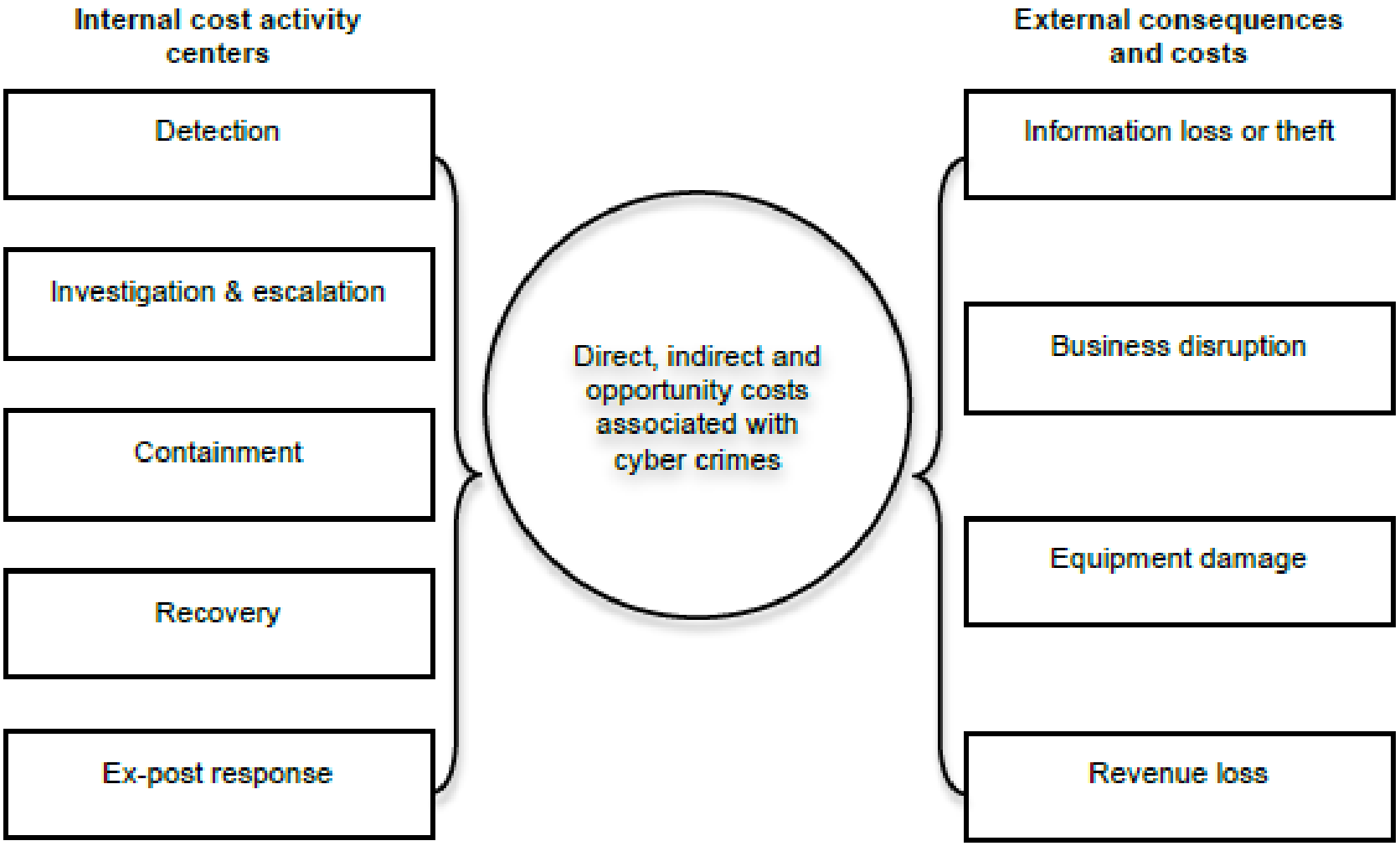
Cost of Countermeasure (CM) = Arbor Networks' solution

Value of CM= $ALE_{original}$ - $ALE_{(with\ CM)}$ - CM

Agenda

- Economic Impact of Cyber Crime
  - Motivation of cybercrime cost study
  - Arbor Networks' Solution for countermeasure and Financial Calculator
  - Security Strength-Cost model
  - Online cost simulator

Figure 24
Cost Framework for Cyber Crime



Source: Ponemon Institute 2013 Cost of Cyber Crime Study; Global Report, published October 2013, sponsored by HP Enterprise Security

The software life cycle of threat disclosure

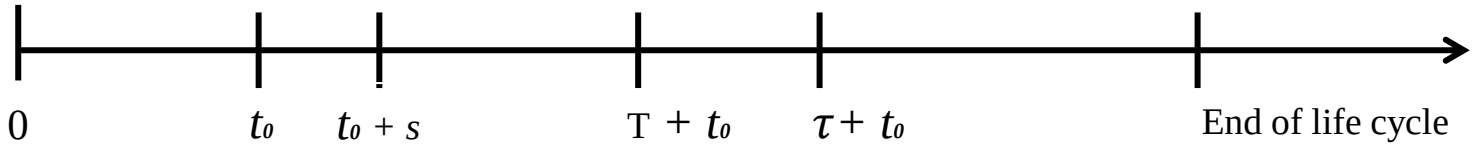


Figure 1– An attacker finds the vulnerability at $t_0 + s$, and the patch is released at $\tau + t_0$. Attackers learn about the vulnerability at $t_0 + s$ or at time T + t_0, whichever is earlier.

Note:
A disclosure policy is the choice of a time T, such that during that time, only the vendor receives vulnerability information. Once time T elapses, information on the vulnerability is disclosed by CERT to the public regardless of path availability. In the above figure a disclosure policy T requires the vulnerability be disclosed at time T + t_0

Vendors provide a patch for this vulnerability at a calendar time $\tau + t_0$

User SLE is a function of T and time sliding window τ and the capture time t_1

$$SLE(\tau,T;t_1)=\begin{cases}\int_0^{\tau} SLE(\tau-s)dF(s:t_0), & when\ \ \tau\le T\\ \int_0^{\tau} SLE(\tau-s)dF(s:t_0)+(1-F(T:t_0))SLE(\tau-T) & when\ \ \tau>\mathrm{T}\end{cases} \quad (1)$$

$$V=C(\tau)+\lambda SLE(\tau,T) \quad (2)$$

where λ is a proportion of user's SLE that the vendor internalizes (through reputation loss or a loss of future revenue).

If $\lambda=1$, the vendor internalizes the entire loss to users, then the social cost, $S=C(\tau)+SLE(\tau,T)$ (3)

The objective is to maximise the value of countermeasure (CM), i.e to minimise the $(SLE_{(with\ CM)}+CM)$. The strategy attackers will use via malicious insider in order to lower the vulnerability discovery cost. The defender has to strengthen the security level, i.e. reduce probability of discover of vulnerability.

As all costs are dynamic, estimation of real costs not likely to be accurately estimated from historical costs data but current costs data should be used to predict next instance for strategic or tactical cost decision making.

$$SLE(\text{with CM})\ (t+1) = SLE(\text{with CM})\ (t) + C_0 \qquad (4)$$

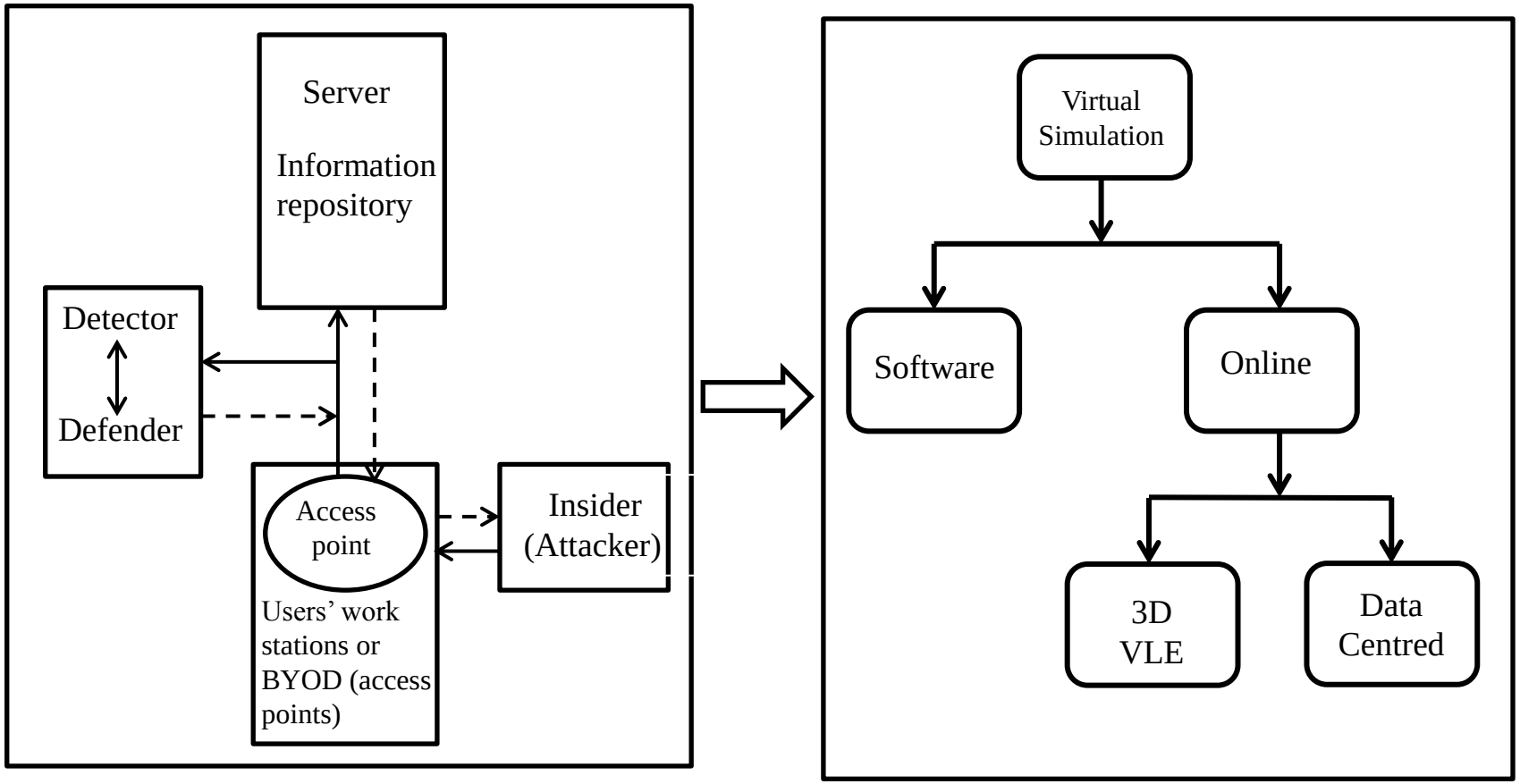
which is AR(1) model.

(4) can be implemented using online cost simulator.

Agenda

- Economic Impact of Cyber Crime
  - Motivation of cybercrime cost study
  - Arbor Networks' Solution for countermeasure and Financial Calculator
  - Security Strength-Cost model
  - Online cost simulator

Cyber Crime Cost Simulation



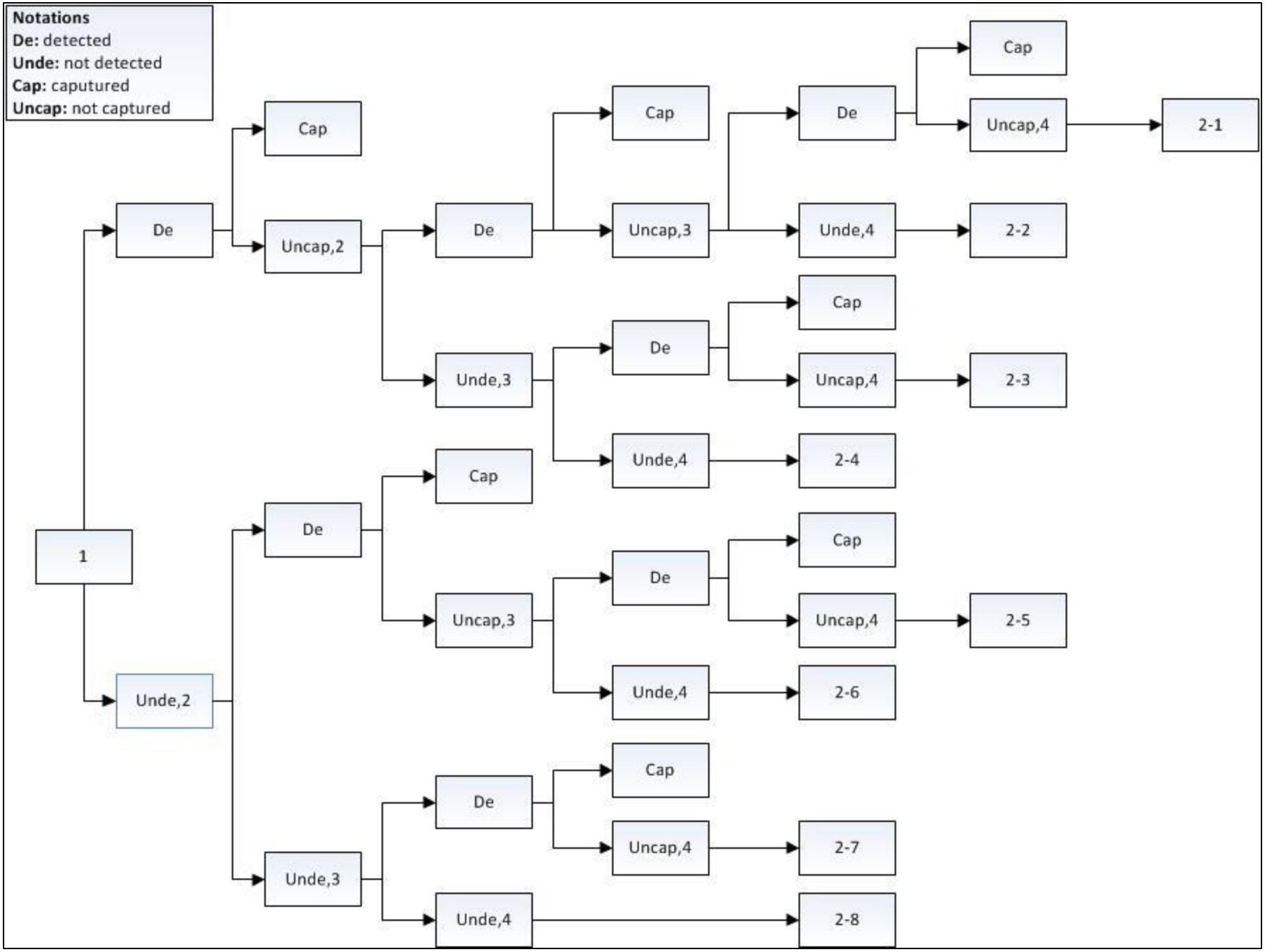
Conceptual model for cyber threat and counter measure

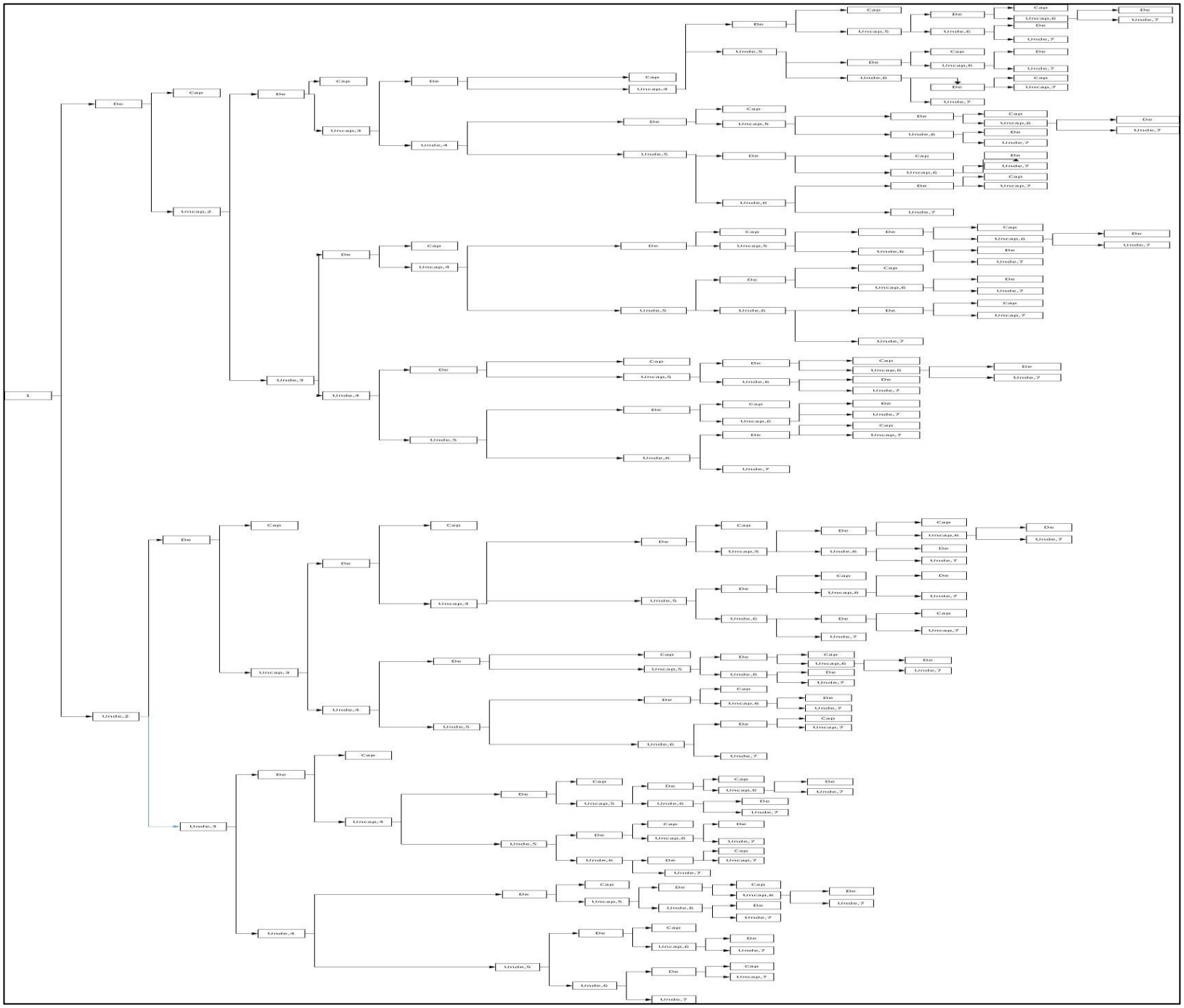
Online software simulation – Dynamic and interactive

Online Simulation Approach:

Based on stochastic games play by attackers and defenders due to information asymmetry. The probabilistic networks are shown in the next two slides.

- Detection of vulnerability by attacker
- Exploitation of vulnerability by attacker
- Attacker will maximise its reward and use the strategy of lowest chance of being captured
- Defender will aim to predict the move of attacker to optimise the defending strategy
- State Transition Probability matrix and Payoff matrix are inputs
- Nash Equilibrium – both reached their optimal strategies (no further change in their strategies will occur)
- Game playing ends when the attacker is captured
- In process computation of various components of internal and external costs to obtain near real time Single Loss Expectancy (SLE).


Notations
De: detected
Unde: not detected
Cap: caputured
Uncap: not captured
1
De
Cap
Uncap,2
De
Cap
Uncap,3
De
Cap
Uncap,4
2-1
Unde,4
2-2
Unde,3
De
Cap
Uncap,4
2-3
Unde,4
2-4
De
Cap
Uncap,3
De
Cap
Uncap,4
2-5
Unde,4
2-6
Unde,2
Unde,3
De
Cap
Uncap,4
2-7
Unde,4
2-8


1
De
Cap
Uncap,2
Unde,3
Uncap,3
Unde,4
Uncap,4
Unde,5
Uncap,5
Unde,6
Uncap,6
Unde,7
Uncap,7
Unde,2

Key take away

A dynamic and interactive cyber crime cost simulation framework which can be used as strategic and tactical decision supports.