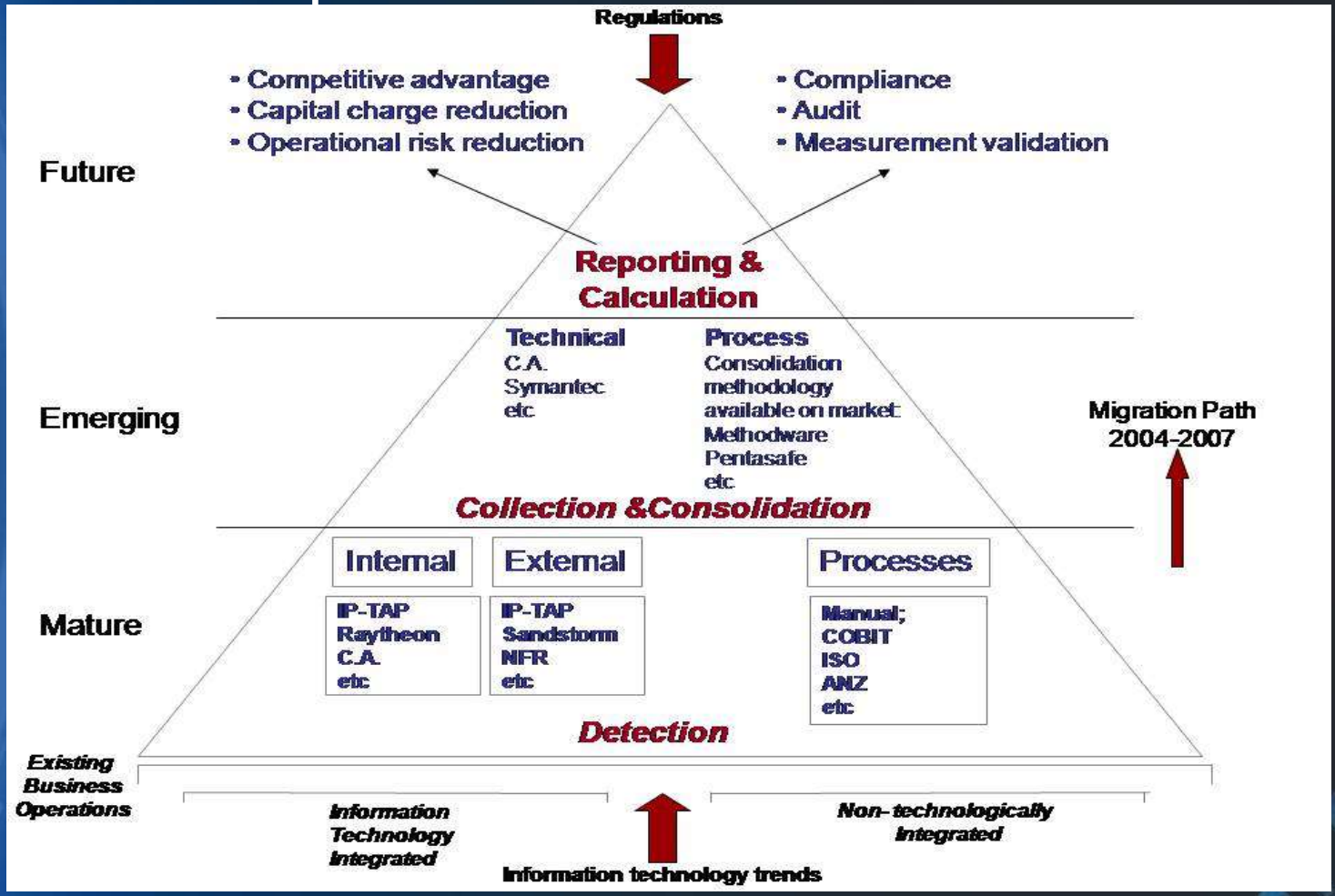
n-ORM™ Presentation

Phillipe Evrard

March 2008

The New Environment



info@ip-tap.com

The New Environment

- Banks – mandated under Basel II to quantify and value operational risks
- Insurance mandated under Solvency II to quantify and value operational risks
- Companies listed in the U.S. mandated under SOX to quantify and value operational risks
- All companies active in risk management programmes
- All companies increasingly seeking to create an internal risk-aware organisational culture.

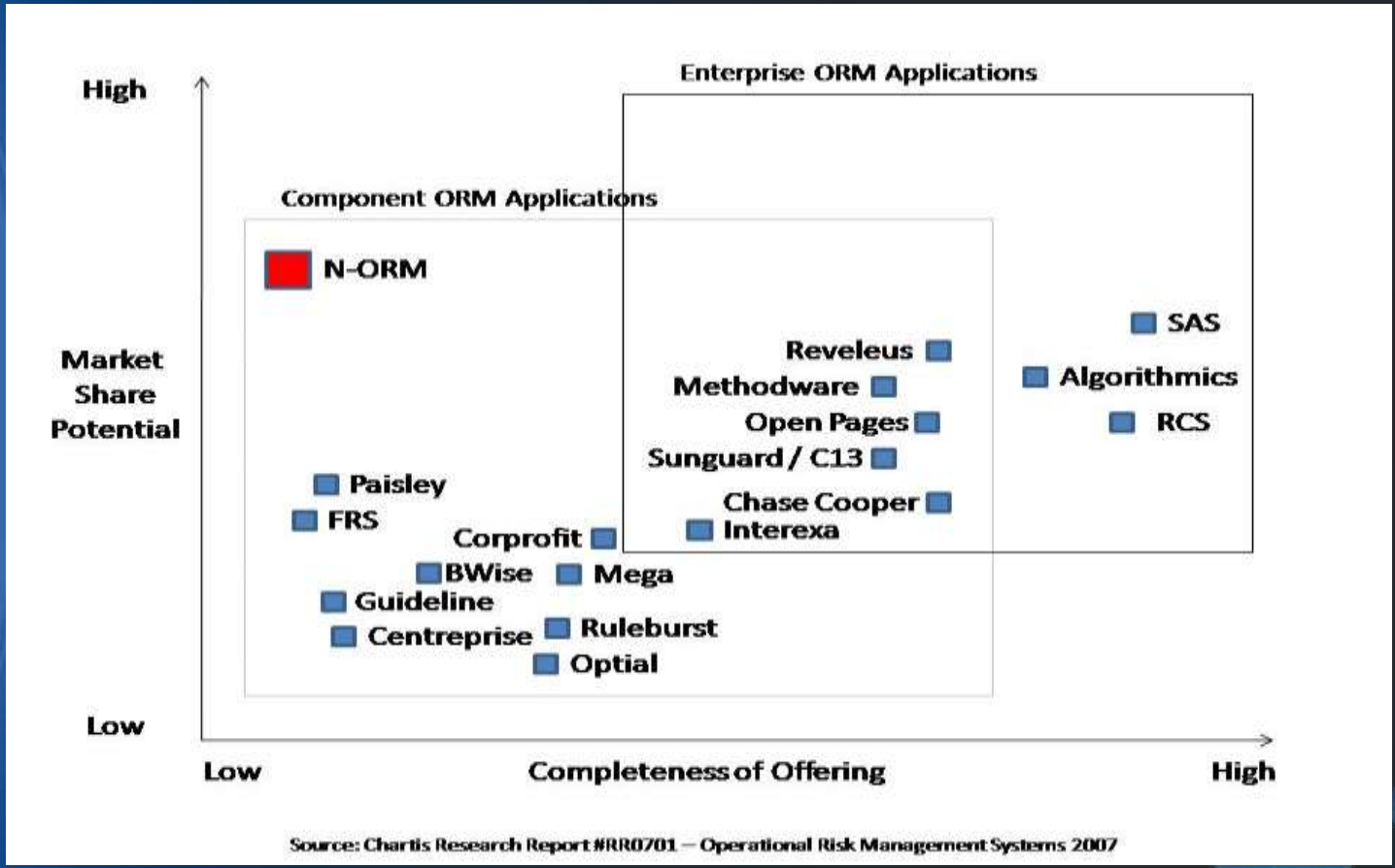
iP-TAP
info@ip-tap.com

The Risk Business Case

- Shift from 'avoid risk' to 'think risk' – competitive advantage through enhanced operations/processes.
- Security is no longer a sunk cost but a means of creating sense of confidence for clients/suppliers working with a risk-aware organization- same as per ISO certification.
- Audit & compliance – no assumption all is well; now a need to prove it and how achieved – show us how you will stay in business and not have a security issue.
- Risk now falls within the Boardroom via the strategic planning process – align the company to the risk profile/appetite

iP-TAP
info@ip-tap.com

Overall Landscape for Risk Applications



Source: Chartis Research Report #RR0701 – Operational Risk Management Systems 2007

info@ip-tap.com

What is n-ORM™?

- n-ORM comprises 2 elements;

- A traffic collector
- A system that quantifies the value at risk arising from connecting a corporate network to the internet

- It is also a compliance tool for Basel II / SOX / Solvency II

- A risk assessment tool as part of an overall risk management methodology

- A means of creating a company-wide threat database

iP-TAP
info@ip-tap.com

What is nOpVaR™?

- The output from n-ORM labelled network operational value at risk (nOpVaR ™).
- Derived from data + algorithmic models within the n-ORM / traffic capture systems
- Company-specific/unit-specific configured output derived from a combination of automated internal /external data and manually input data
- A monetary value to be used within the overall risk assessment program of an organization.

iP-TAP
info@ip-tap.com

What are we looking for?

1. Operational network data to field test:The software
2. The hardware over time (so far 1 year live)
3. Validating of the algorithms
4. User feedback as to ease of use
5. Consolidated data for research into the risks arising from networks
6. Multi-country/company data to compare
7. Validation of the current integration development

iP-TAP
info@ip-tap.com

Benefits to Acerta

1. Its free and without risk!

2. Required exercise for internal risk management

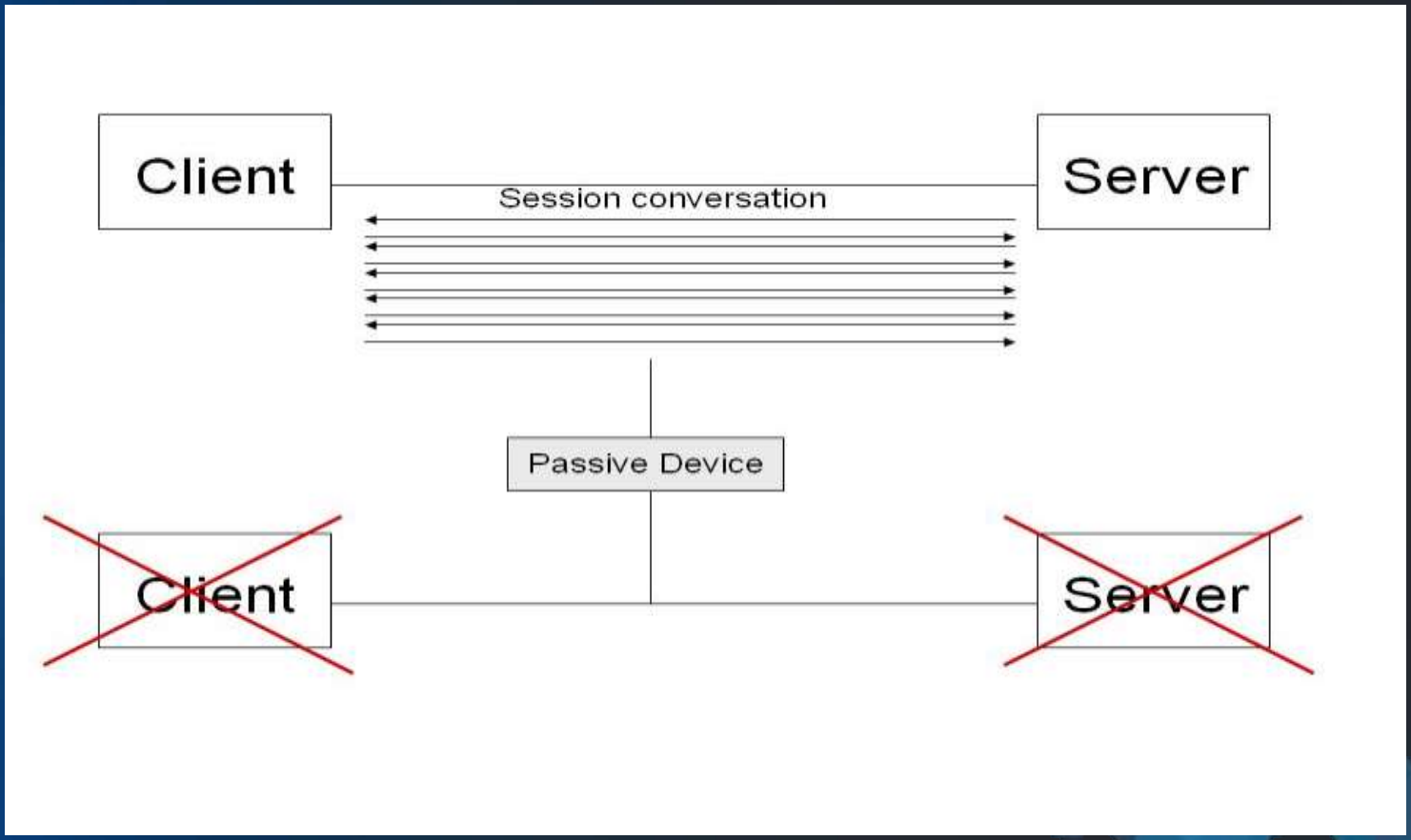
3. A step towards fulfilling future regulatory requirements

4. Validation of the current approach to managing network risks in terms of valuation

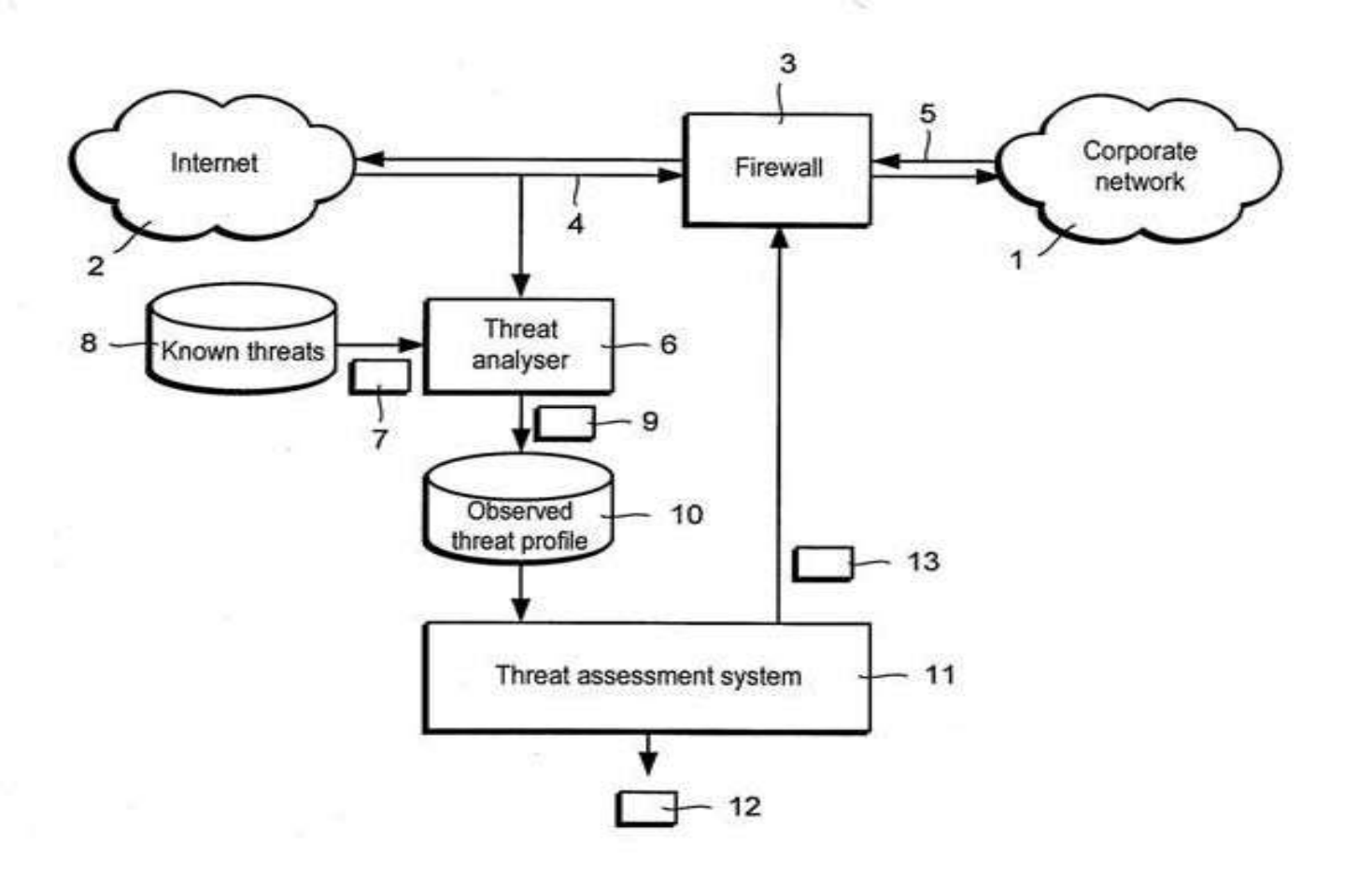
5. A tool to create an environment of a risk aware organization

iP-TAP
info@ip-tap.com

Basic Copy Model



Installation Positioning



iP-TAP
info@ip-tap.com

Operational Requirements

- For IP TAP - 2 x 1U profile servers
- Removal mass storage devices (hot swap HD's)
- Min 8Gb RAM / 2.6Ghz Processor
- Other technical specifications can be given at appropriate time
- For n-ORM – desktop PC, Windows XP or above + 2Gb RAM + installation of n-ORM + Dongle + JVM2.x + internet connection

Installation Options - Hardware

Two primary options:

- 1. We supply the installation CD's and each business unit installs according to the specifications but on the machines of their own choice
- 2. We supply the system pre-installed on machines of our choice (with ownership remaining with us)

info@ip-tap.com

Installation & Licence

- Can be installed by internal personnel with network admin experience
- Can be installed by Loughborough personnel
- Can hold a centralized training day for internal personnel
- Can hold company-specific training per location if small number
- Control of use is controlled by Dongle under specific rights and obligations

iP-TAP
info@ip-tap.com

XML Threat Data

- <Crimson Version="1">–
- <ObservedThreats ObservationStart="2008-02-25T00:00:00" ObservationEnd="2008-03-03T00:00:00">

- <Threat ID="DOS MSDTC attempt" Category="Indiscriminate" Target="Unknown" SeverityScore="7">
- <Observation Day="Monday" From="00:00:00" To="00:59:59" Count="52"/>
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="32"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="56"/>

- <Threat ID="WEB-MISC http directory traversal" Category="Indiscriminate" Target="Unknown" SeverityScore="7">
- <Observation Day="Monday" From="00:00:00" To="00:59:59" Count="247"/>
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="152"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="266"/>
- <Observation Day="Monday" From="03:00:00" To="03:59:59" Count="437"/>

iP-TAP
info@ip-tap.com

What Does theThreat Data Mean?

- <Crimson Version="1">–
- <ObservedThreats ObservationStart="***2008-02-25***T00:00:00" ObservationEnd="***2008-03-03***T00:00:00">

- <Threat ID="***DOS MSDTC attempt" Category="Indiscriminate" Target="Unknown" SeverityScore="7">***
- <Observation Day="Monday" From="00:00:00" To="00:59:59" ***Count="52"/>***
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="32"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="56"/>

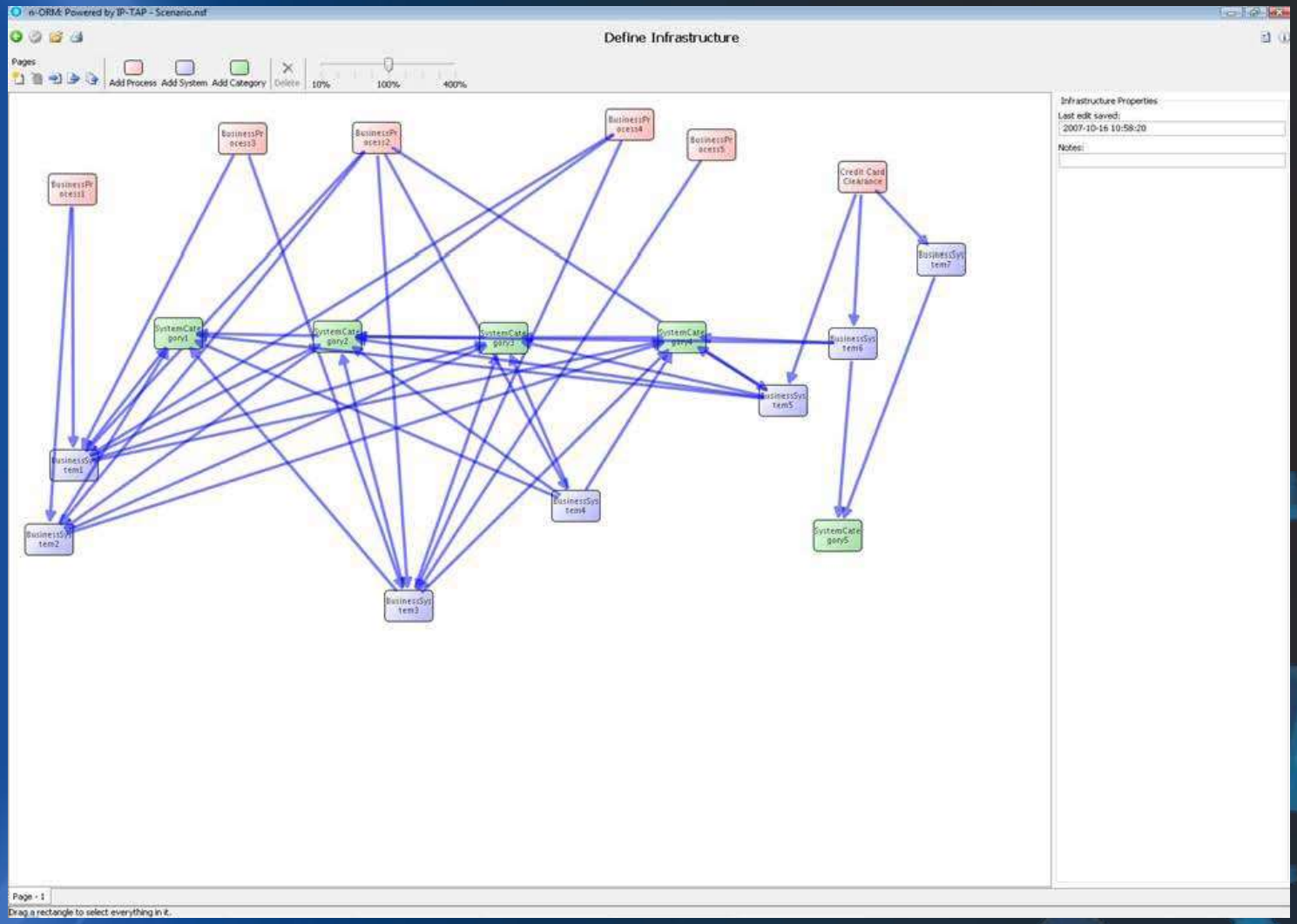
- <Threat ID="***WEB-MISC http directory traversal" Category="Indiscriminate" Target="Unknown" SeverityScore="7">***
- <Observation Day="Monday" From="00:00:00" To="00:59:59" ***Count="247"/>***
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="152"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="266"/>
- <Observation Day="Monday" From="03:00:00" To="03:59:59" Count="437"/>

Process Manager

- Processes, systems and categories are mapped in their relationships by internal personnel
- The output from the process manager is input into the main application
- Multiple instances of process manager can be given to individual workgroups, process managers etc
- Drag and drop functionality reduces training requirements to minutes.

info@ip-tap.com

Process Manager



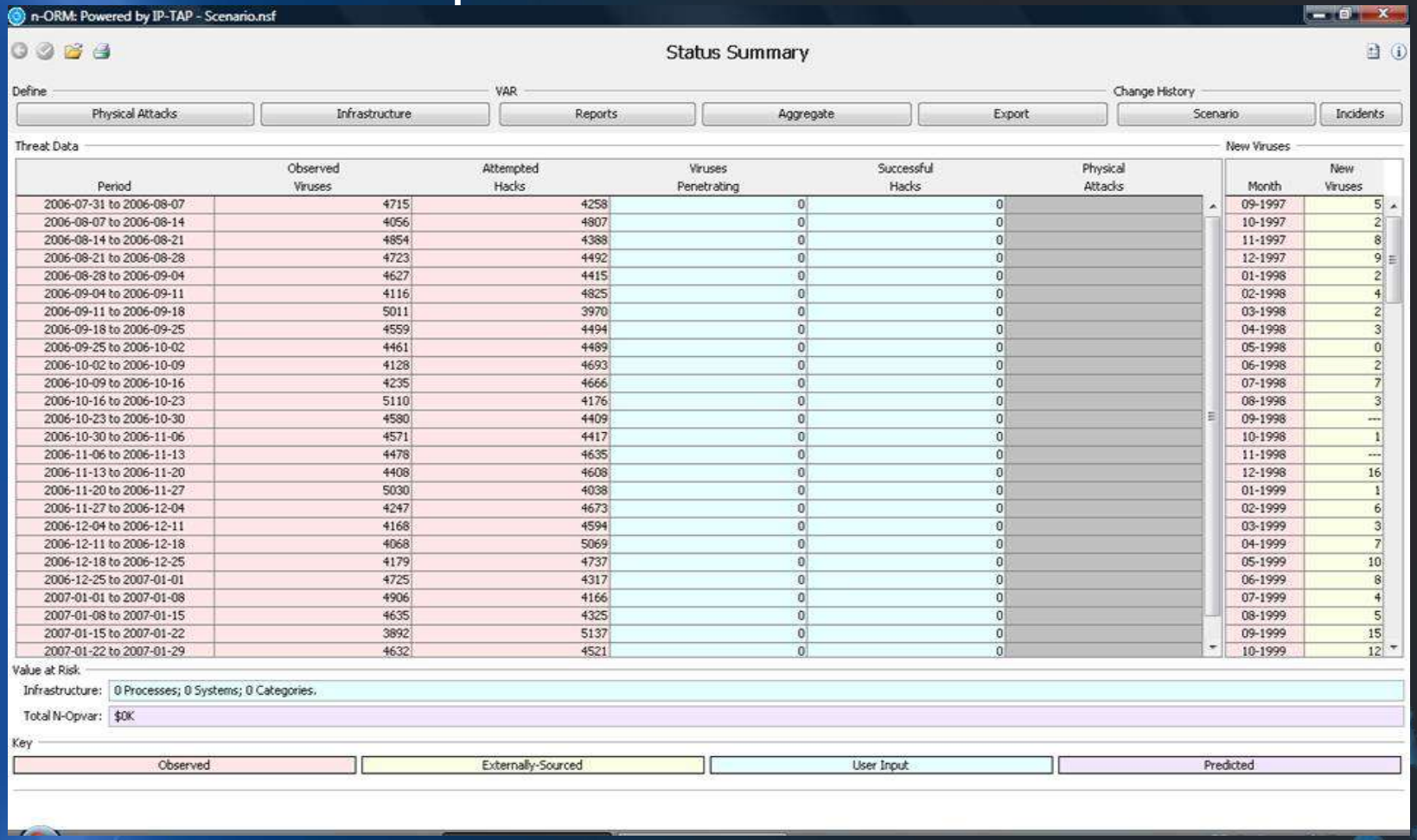
info@ip-tap.com

Main Screen

- Gives a total aggregated risk and value at risk
- Simple to understand
- Audit and compliance focussed
- Reporting and record maintenance of changes create clarity to Supervisors
- Intuitive ease of use requires little training
- Multiple options in the calibration of basic inputs, such as currency, language

info@ip-tap.com

The Main Screen



Period	Observed Viruses	Attempted Hacks	Viruses Penetrating	Successful Hacks	Physical Attacks
2006-07-31 to 2006-08-07	4715	4258	0	0	
2006-08-07 to 2006-08-14	4056	4807	0	0	
2006-08-14 to 2006-08-21	4854	4388	0	0	
2006-08-21 to 2006-08-28	4723	4492	0	0	
2006-08-28 to 2006-09-04	4627	4415	0	0	
2006-09-04 to 2006-09-11	4116	4825	0	0	
2006-09-11 to 2006-09-18	5011	3970	0	0	
2006-09-18 to 2006-09-25	4559	4494	0	0	
2006-09-25 to 2006-10-02	4461	4489	0	0	
2006-10-02 to 2006-10-09	4128	4693	0	0	
2006-10-09 to 2006-10-16	4235	4666	0	0	
2006-10-16 to 2006-10-23	5110	4176	0	0	
2006-10-23 to 2006-10-30	4580	4409	0	0	
2006-10-30 to 2006-11-06	4571	4417	0	0	
2006-11-06 to 2006-11-13	4478	4635	0	0	
2006-11-13 to 2006-11-20	4408	4608	0	0	
2006-11-20 to 2006-11-27	5030	4038	0	0	
2006-11-27 to 2006-12-04	4247	4673	0	0	
2006-12-04 to 2006-12-11	4168	4594	0	0	
2006-12-11 to 2006-12-18	4068	5069	0	0	
2006-12-18 to 2006-12-25	4179	4737	0	0	
2006-12-25 to 2007-01-01	4725	4317	0	0	
2007-01-01 to 2007-01-08	4906	4166	0	0	
2007-01-08 to 2007-01-15	4635	4325	0	0	
2007-01-15 to 2007-01-22	3892	5137	0	0	
2007-01-22 to 2007-01-29	4632	4521	0	0	

Month	New Viruses
09-1997	5
10-1997	2
11-1997	8
12-1997	9
01-1998	2
02-1998	4
03-1998	2
04-1998	3
05-1998	0
06-1998	2
07-1998	7
08-1998	3
09-1998	---
10-1998	1
11-1998	---
12-1998	16
01-1999	1
02-1999	6
03-1999	3
04-1999	7
05-1999	10
06-1999	8
07-1999	4
08-1999	5
09-1999	15
10-1999	12

info@ip-tap.com

The Algorithmic Models

- Investigation undertaken into the most appropriate based upon test data
- Options were: Weighted Linear Extrapolation; Bayesian Networks; Markov Model; Autoregression.
- Selection based upon a simple approach for customers and Supervisors to understand as well as best fit to trial data.
- Autoregression may be implemented with greater volumes of data to test

Product/Service Offering

- Complete system
- Volume pricing licensing for 'process manager' element
- Consultancy based upon initial installation, configuration and training
- Subsequent consultancy based upon third party validation of VaR attributed
- System has audit/control report functionality for regulatory compliance
- Historical data analysis for accurate assessment and valuation of risk

iP-TAP
info@ip-tap.com

Support Structure

- Project support via – NSC (front end) + LUEL (backend)
- Anticipate few requirements for support
- Debugging already undertaken with test site (1year)
- Non-critical/real-time system
- Data confidentiality by all parties (only patterns IN the data, NOT viewable data content)
- NSC – military intelligence background i.e. high degree of confidentiality

Next Steps

- Timeline & options preferred for implementation of backend?
- Timeline for process manager inputs?
- Timeline for calibration of n-ORM utility?
- Agreement on overall period of free installation and use/field trials
- Language support required

iP-TAP
info@ip-tap.com