MENA Information Security Conference 2017

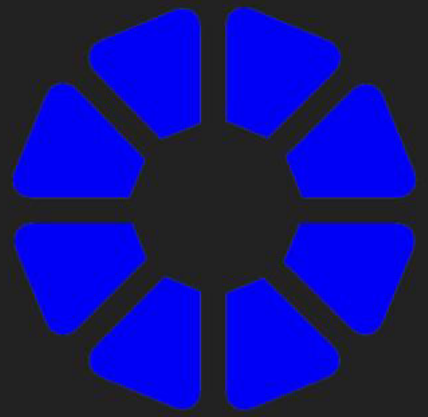
On the Verge:

Combating Cyber Threats leveraging Threat Intelligence, Faster Detection & Automated Response

IRM- INTEGRATING PEOPLE, PROCESS AND TECHNOLOGY

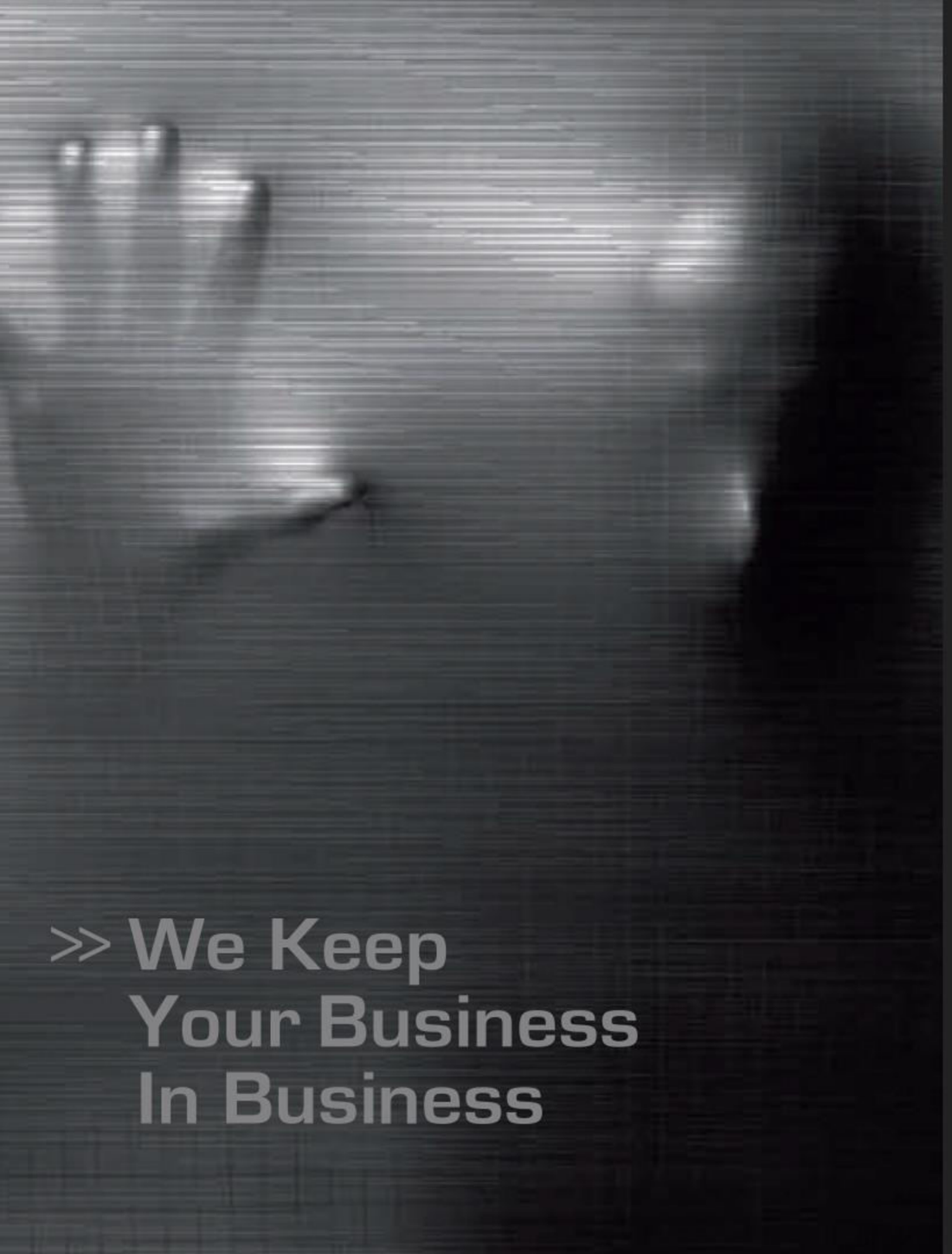
George Patsis

OBRELA
SECURITY INDUSTRIES



OBRELA

SECURITY INDUSTRIES



WE USE SECURITY ANALYTICS AND SOPHISTICATED RISK AND THREAT MANAGEMENT TECHNOLOGY TO DYNAMICALLY PROTECT OUR CLIENTS BY IDENTIFYING, ANALYZING, PREDICTING AND PREVENTING CYBER THREATS

IN REAL TIME_

OUR CORE

ENVIRONMENT

NEW WORLD ORDER

Users

Connected to Internet

Devices

IP connected Devices

Traffic

Per month

Cyberspace

Volume of Data

BN $

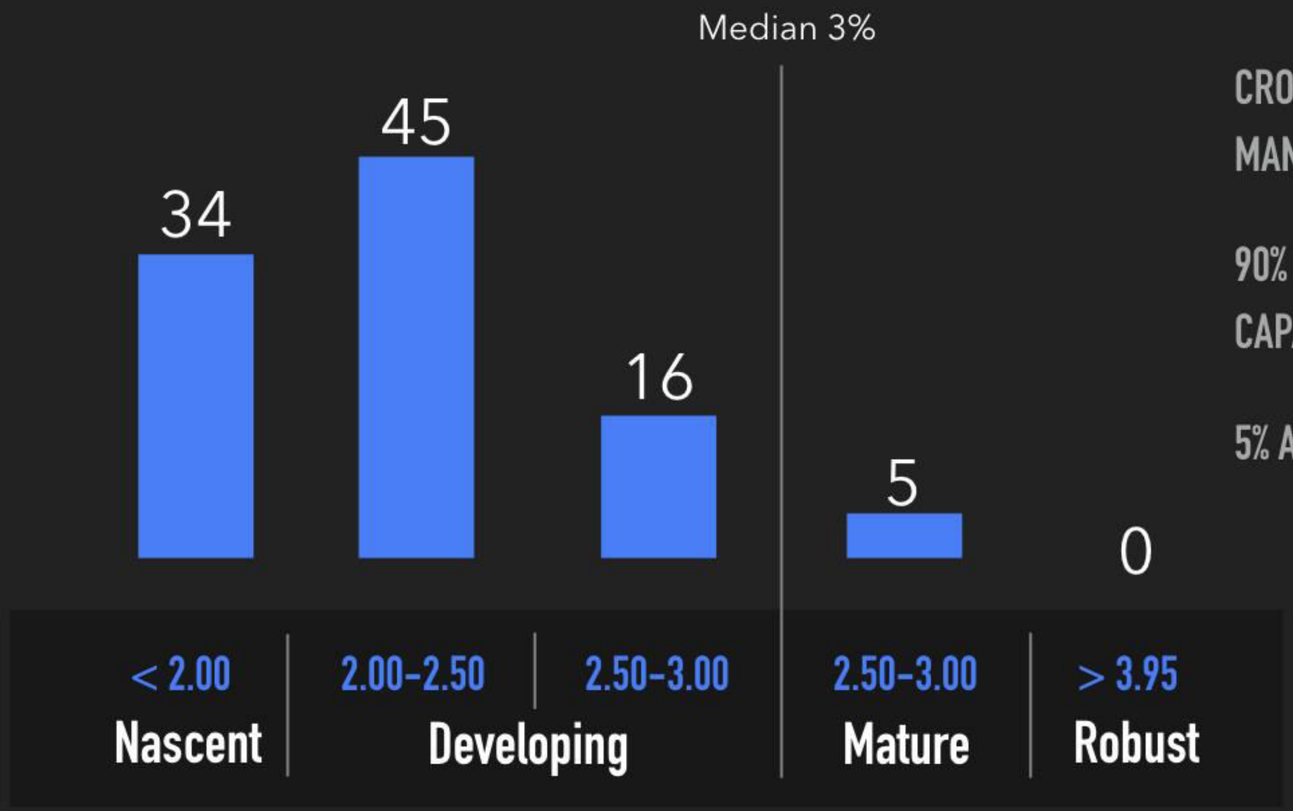
300

CYBERCRIME IMPACT

per year is the estimated economic impact of cybercrime and espionage in the global economy

*SOURCE, GARTNER 2017

LACK OF CAPABILITY



Maturity level on a scale of 1 to 4, where the 4 is the strongest, % of companies

CROSS-SECTOR GAPS IN RISK MANAGEMENT CAPABILITIES

90% HAD NASCENT OR DEVELOPING CAPABILITIES LEAVING ONLY

5% AT MATURE STATE

*SOURCE, MCKINSEY CYBER RISK MATURITY SURVEY (CRMS)

THE PERFECT STORM CONDITIONS

- Growing Cyberspace — An increasingly growing attack surface
- Cybercrime Evolution — Cybercrime a low risk, low cost, high return activity
- Enterprise Security — Lack of Capability
- Enforcement — Lack of judicial cooperation

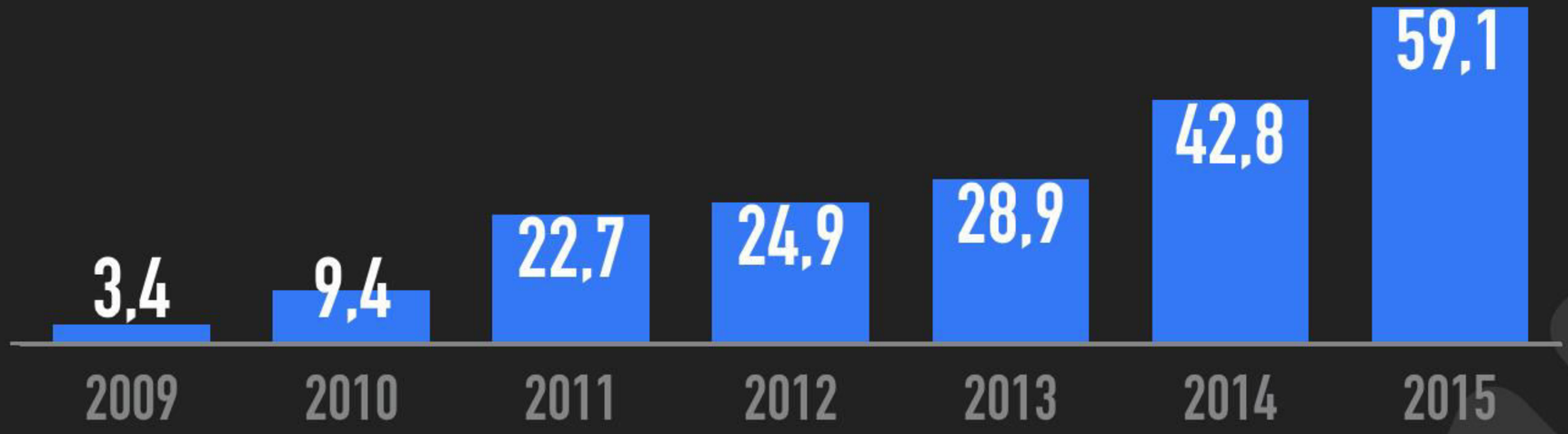
THE SECURITY MARKET IS FAILING

THE PROBLEM

WORLDWIDE SECURITY SPENDING IS INCREASING

*SOURCE, GARTNER IN BILLIONS

. . . BUT CYBERCRIME KEEPS CLIMBING*



*SOURCE, MORGAN STANLEY 2016 IN MILLIONS

US DOLLARS

1TN

SECURITY SPENDING

will be spent globally on cybersecurity from 2017 to 2021*

*SOURCE, GARTNER 2017

70

SECURITY 'SPRAWL' NOT SUSTAINABLE

different security vendors provide services and products on average per enterprise

*SOURCE, GARTNER 2017

DAYS

240

LACK OF CAPABILITY

average time to detect and react to cyber breaches today

*SOURCE, GARTNER 2017

CYBERCRIME DEMANDS A NEW APPROACH

ITS TIME FOR A CHANGE

01

PROBABILITY

It is a mathematical certainty that every security model will inevitably fail at least once, regardless of the defence and technology sophistication involved.

*SOURCE, GARTNER 2017

TECHNOLOGY IS NOT THE SOLUTION

- We cannot rely entirely on security products to identify and prevent threats without contemplating complexity and the human factor risks.
- The common approach to cyber – adding more and more layers – is not sustainable.

PEOPLE AND HUMAN INTELLIGENCE – THE HEART OF CYBERSECURITY

- Properly balanced security controls that engage technology as much as people are essential for Enterprise information security.
- People are indispensable to evaluate an incident and decide the response strategy during a crisis.

ONE (BIG) DATA POOL

SECURITY RELATED DATA

Structured and Unstructured data, coming from various sources like Firewalls, SIEM, WAF, IDS etc. that need to be normalized, categorized and correlated

ONTOLOGY

A set of entities designed to organise the security related data, while also providing an open-schema for users to define their own attributes

ONTOLOGY BASED DATA MODEL

Analytics
Data Analysis,
User Behaviour

Universe
Information Assets,
Geolocation, Classification

Exposure
Vulnerabilities,
Remediation, Severity

Event Management
Events, Criticality

Threat Intelligence
Threat Intelligence Related Data

Operational Security
Workflows, Tickets, Activity

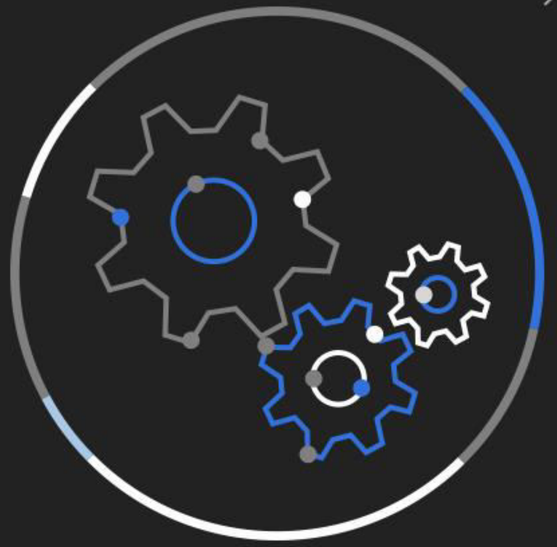
Compliance
Remediation, Tracking
and Planning

Policy
Content, Standards, Policies,
Procedures, Guidelines

ONE WORKFLOW

Event Management
Events, Criticality

Compliance Management
Remediation, Tracking and Planning



Operational Security
Workflows, Tickets, Activity

Asset Management
Information Assets Types, Geolocation, Classification

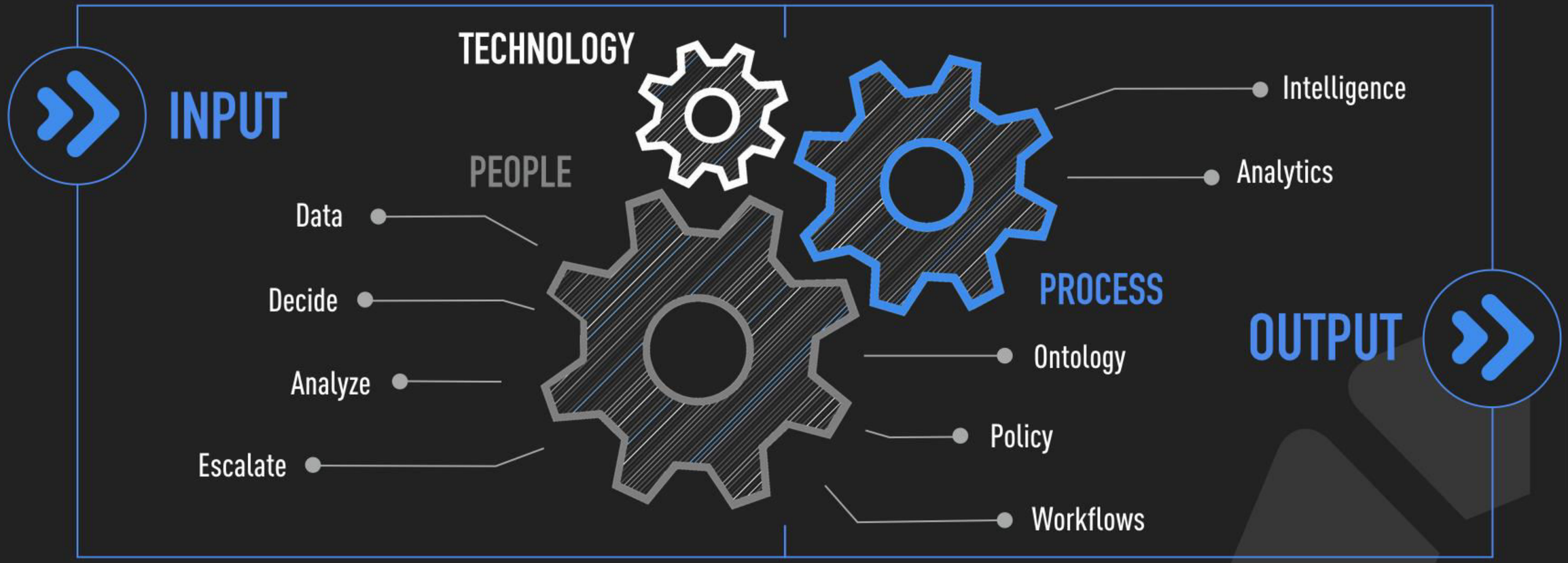
Exposure Management
Vulnerabilities, Remediation, Severity

Governance
Content, Standards, Policies, Procedures, Guidelines

UNVEIL INVISIBLE FRAGMENTS

- Process automation and the introduction of a security application workflow can produce invaluable security related data and records, that we were never able to use before;
- Extremely valuable security related structured and unstructured data and metadata within the organization which are unused, fragmented, isolated and mostly static – now can help us enrich our knowledge, measure our performance and assess our risks.

A MINDSET SHIFT >> INTEGRATED RISK MANAGEMENT



50%

BY 2021

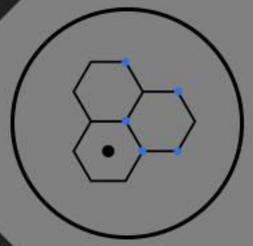
of organizations will be using an IRM solution to support their critical decision making capability

*SOURCE, GARTNER 2017

BENEFITS OF IRM

AGILITY

Agility is one of the key security attributes that is however very hard to accomplish if the objectives of the security strategy remains unchanged.

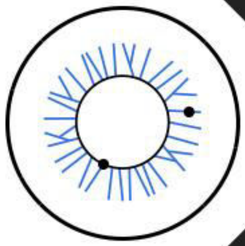


INTER OPERABILITY

By bringing all three elements together Information security becomes a single system.

VIGILANCE

Next generation security models must have the ability to integrate advanced security intelligence to anticipate threats, evaluate risks and make the proper decisions to contain impact.



INTEGRATED RISK MANAGEMENT

THE KINGDOM MUST EMBRACE, ADOPT AND LEAD IRM

- Addresses the problem for lack of capability as knowledge becomes a key element that can be embedded and maintained as content and context
- Unveils a unique potential for enterprise 3Dimension Security – Fraud, Cybersecurity, Physical Security integrated
- Will enable a new era of Holistic Cyber Security Service Providers

OBRELA
SECURITY INDUSTRIES

THANK YOU

GEORGE P. PATSIS, CEO

ATHENS | LONDON