

Cyber Risk Quantification: Translating technical risks into business terms

Jesper Sachmann
RSA Denmark

13-06-2018

CYBER RISK QUANTIFICATION:

TRANSLATING TECHNICAL RISKS INTO BUSINESS TERMS

Jesper Sachmann GRCP GRCA

Atos Cyber Security Day

June 13, 2018

IF YOUR CEO ASKED YOU...

How much risk do we have?

How much less risk will we have if...?

How would you answer?

THE COMMUNICATION CHALLENGE

CFO

"How much risk do we have? Are we spending too little or too much on mitigation?"

AUDIT

"Did you fix those high priority issues?"

BOARD/CEO

"We don't want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?"

CIO

"Are we spending our cybersecurity budget on the right things? What is the ROI?"

CISO

"Έχουμε πάνω από δέκα χιλιάδες τρωτά σημεία , είναι συμβατό με το ογδόντα τοις εκατό"



BALD TIRE

How much risk?



**THERE WILL
ALWAYS BE
ASSUMPTIONS IN
ANY ANALYSIS.**

**THE KEY IS TO
SURFACE THEM.**

COMPLIANT... BUT STILL IN THE DARK

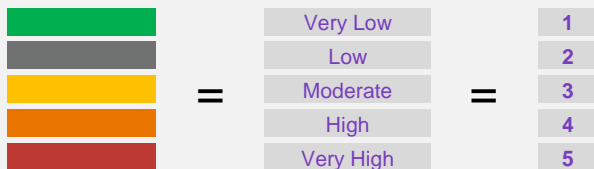
1 Qualitative Checklists & Excel

NIST



2 Governance, Risk & Compliance Tools













No embedded risk analytics capabilities
in most GRC tools



The way most cybersecurity professionals measure risk today fails to quantify cyber risk in terms the business can understand and use

SIDE EFFECT OF THE QUALITATIVE APPROACH

WHICH ONE DESERVES MORE ATTENTION?

<u>Unauthorized Access To Confidential Data</u>	Operational fraud, loss of intellectual property, and loss of customers from damaged reputation resulting from an access control breach		
<u>Executive Sponsorship</u>	The organization lacks an executive management sponsor for risk management leading to poor visibility at the business and corporate management level.		
<u>Least Privilege</u>	The concept of Least Privilege is not used leading to over-authorization of users' roles or access to data, transactions or business systems.		
<u>Performance and Capacity Management</u>	The organization does not have a strategy including application performance and infrastructure utilization planning to properly make use of, and plan accordingly, IT resources resulting in IT resource (application and infrastructure) instability, cost overruns, increased operational maintenance and support costs, under-utilized resources and financial impacts.		
<u>Technology Documentation</u>	The IT organization does not properly document and communicate the use and operation of IT resources (applications, infrastructure, etc.) resulting in poor end user experiences, increased support costs, increased help desk incidents and uninformed maintenance and operations support personnel.		
<u>Bodily Injury due to slips and falls</u>	Loss of employee productivity and injury / possible litigation or workers compensation claims from employees, or from customers or others on-premises.		

Can you compare them?

How can you take a decision based on this report?

THE RISK LANDSCAPE IN A NUTSHELL...

Complex



Dynamic



Limited Resources



Which means...



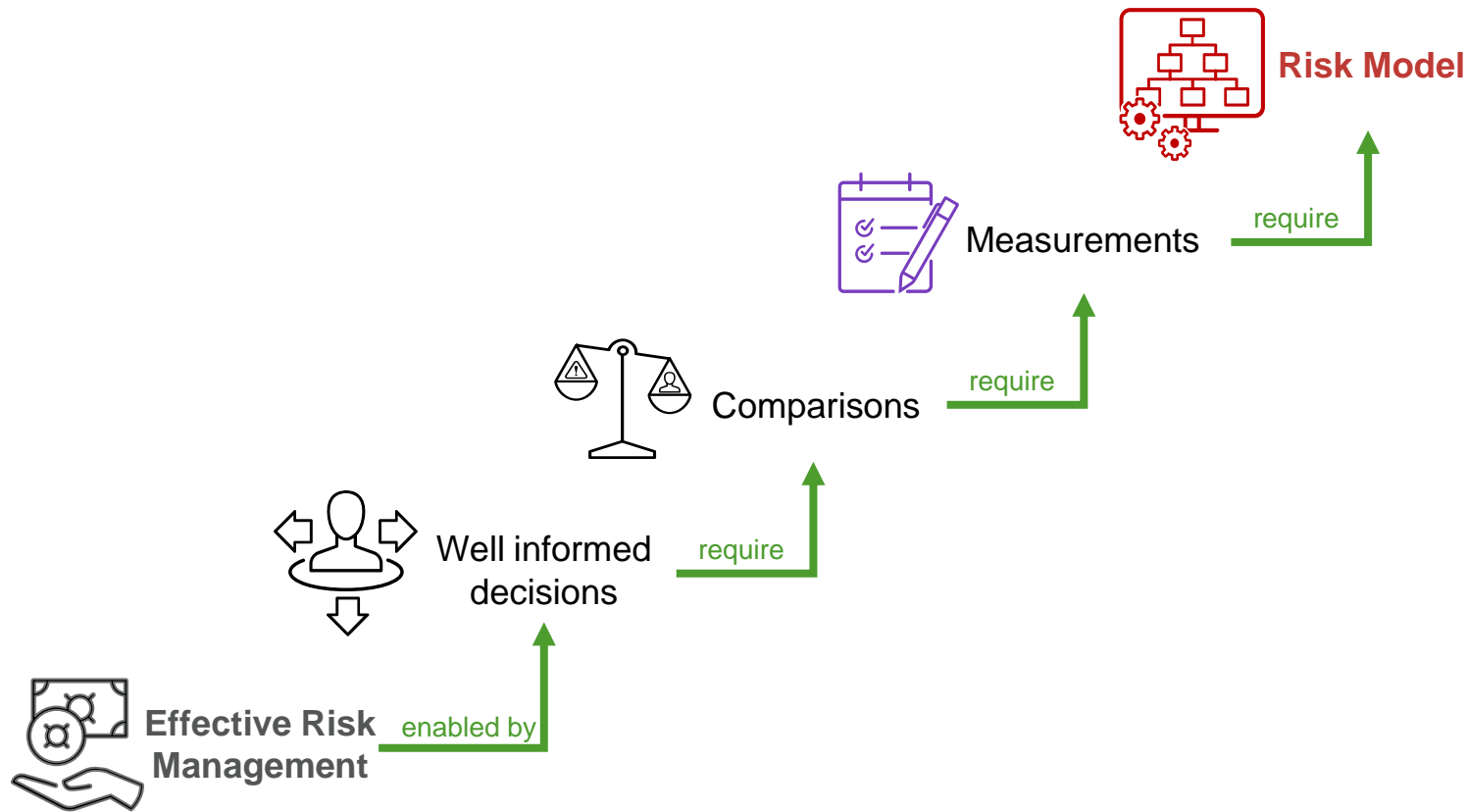
ORGANIZATIONS MUST
EXCEL AT **PRIORITIZING**
THEIR CYBER RISK
PROBLEMS AND
SOLUTIONS.

PRIORITIZATION REQUIRES...

Comparing their various concerns and solution options, which requires...

Measurement

THE RISK MANAGEMENT STACK



CYBER RISK RELEVANCE IS ON THE RISE

THE TOP 10 OPERATIONAL RISK RANKING FOR 2018 OF Risk.net

	2018 position	2017 position	Change
IT disruption	1	1*	→
Data compromise	2	1*	→
Regulatory risk	3	2	↓
Theft and fraud	4	9	↑
Outsourcing	5	3	↓
Mis-selling	6	5**	↓
Talent risk	7	new	
Organisational change	8	6	↓
Unauthorised trading	9	5**	↓
Model risk New Entry	10	-	↑

IN A TYPICAL
ORGANIZATION,
70% TO 90% OF
“**HIGH RISK**” ISSUES,
AREN'T

Why?

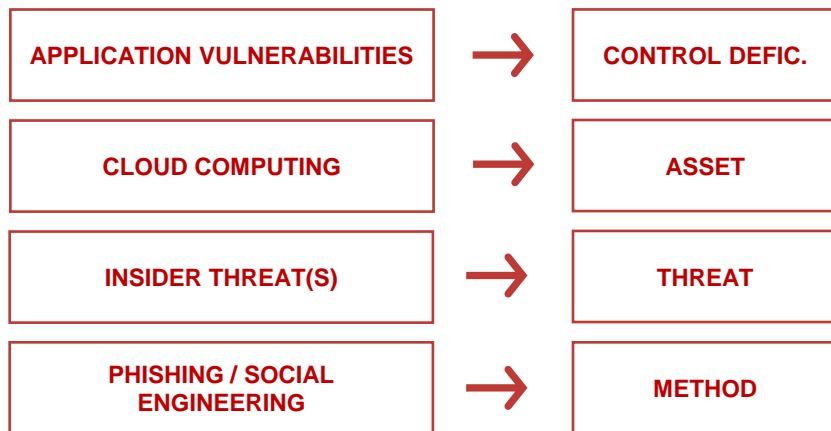
RISK MODELS MATTER

Which Of These Are **Risks**?

POINT OF SALE ATTACKS	HACKTIVISTS
CLOUD COMPUTING	PHISHING / SOCIAL ENGINEERING
INSIDER THREAT(S)	THIRD-PARTY RISK
CYBER CRIMINALS	MOBILE MALWARE
APPLICATION VULNERABILITIES	BUSINESS CONTINUITY

Typical
Top 10 Risk List

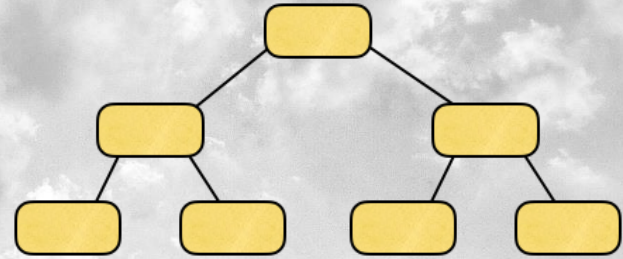
NONE OF THESE ARE RISKS!



WE CAN ONLY ASSESS THE RISK OF LOSS EVENTS

INSIDER THREAT(S)	"LOSS OF AVAILABILITY OF SYSTEMS DUE TO MALICIOUS INSIDER"
APPLICATION VULNERABILITIES	"THEFT OF CUSTOMER PII DATA THROUGH APPLICATION ATTACKS"

FACTOR ANALYSIS OF INFORMATION RISK (FAIR) OVERVIEW



A "FAIR DEFINITION" OF RISK

FAIR – FACTOR ANALYSIS FOR INFORMATION RISK

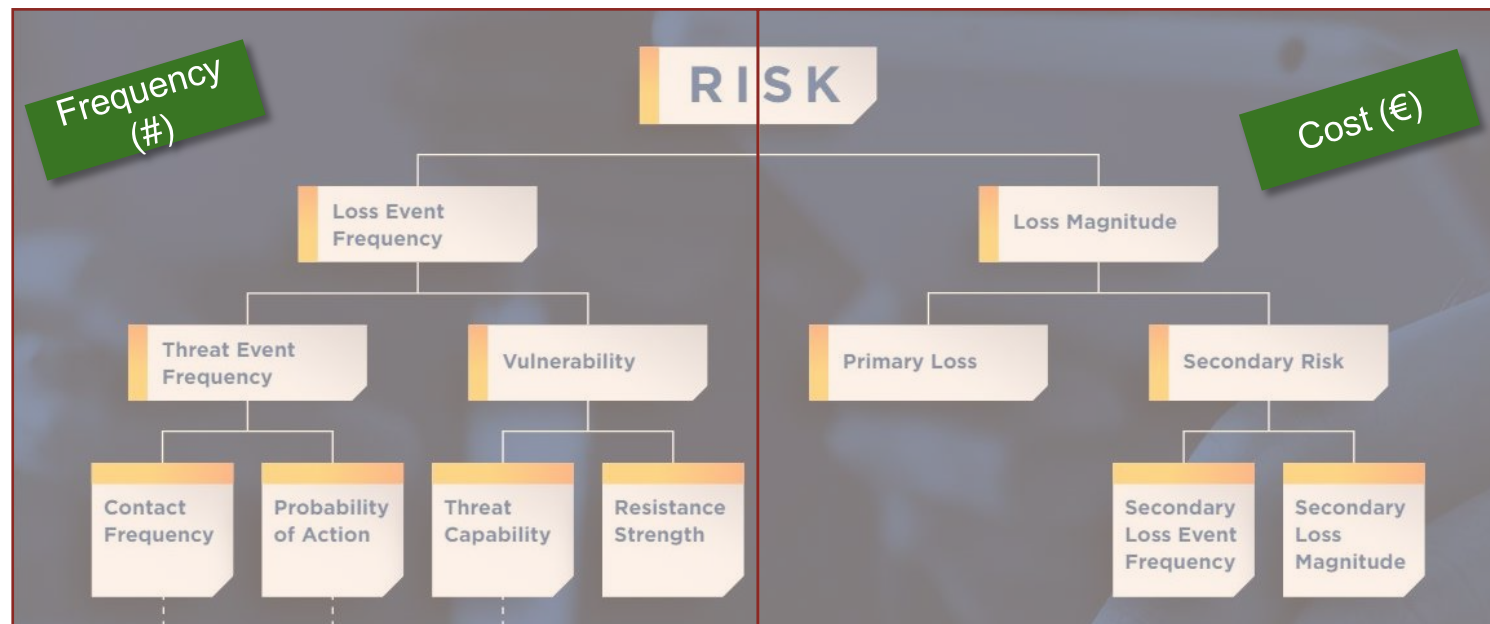
■ The RISK is

■ ***the probable frequency and probable magnitude of future loss (*)***



- Risk is a derived (calculated) value
- To address the inherent uncertainty of risk, probabilistic distributions are used
- The risk is defined in terms of "financial loss exposure"

FAIR: THE ANALYTICS MODEL



Accredited as an
Industry Standard by



Complementary to
Risk Frameworks



Supported by a Fast
Growing Community

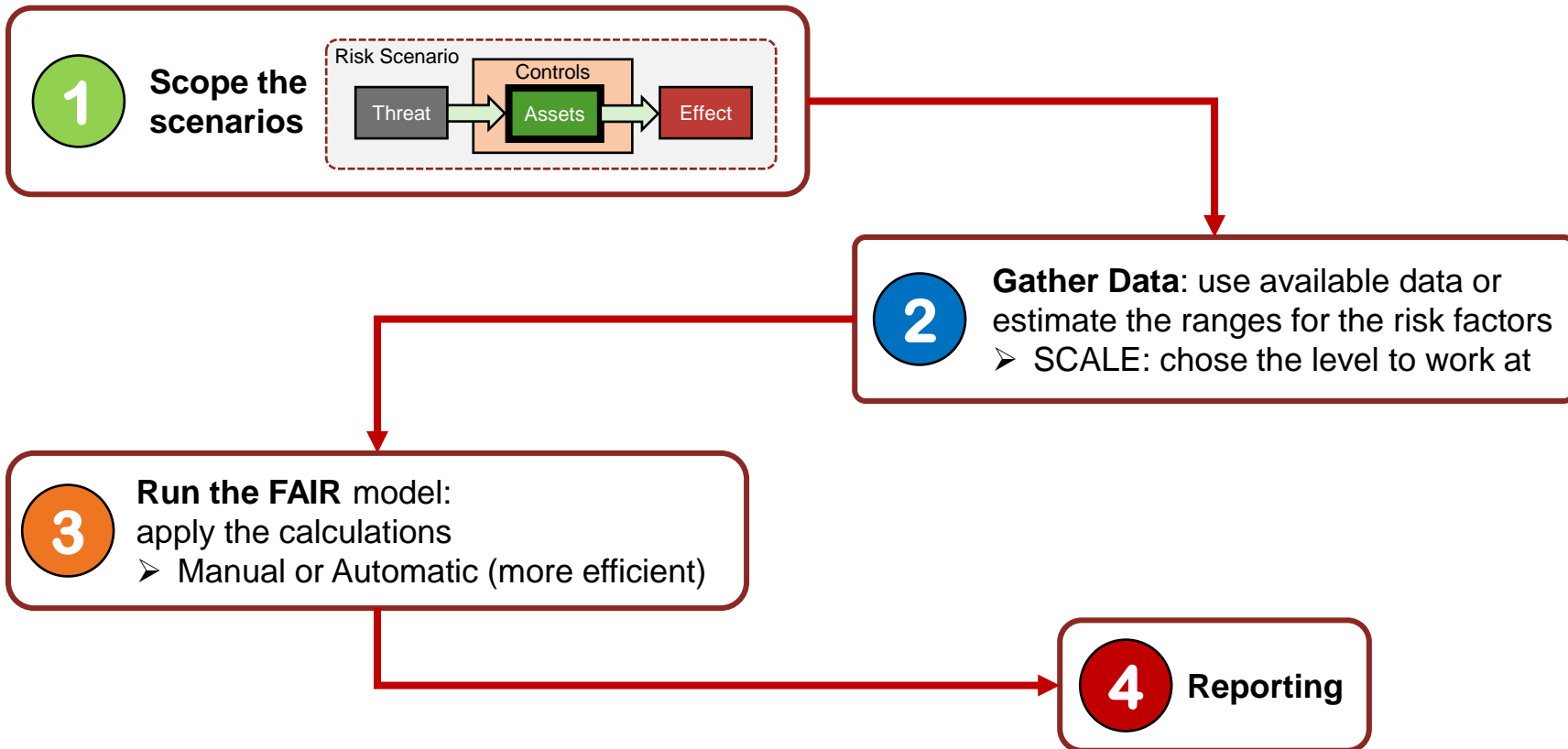


FAIR Book Inducted
in Cybersecurity Canon



RSA BUSINESS-DRIVEN SECURITY™

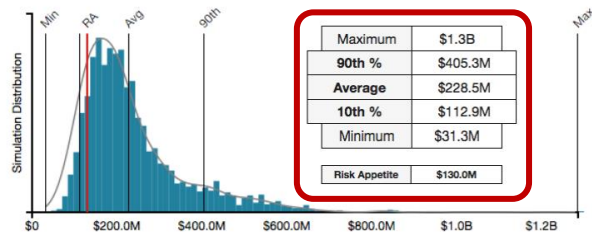
FAIR: THE METHODOLOGY



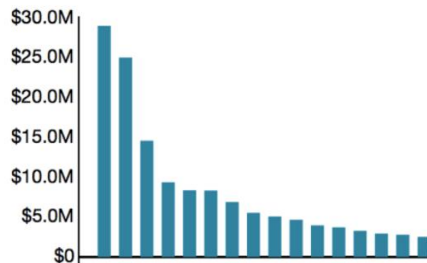
THE OUTCOME: WHAT YOU GET

CYBER RISK IS EXPRESSED IN FINANCIAL TERMS:

"HOW MUCH RISK DO WE HAVE?"



"WHAT ARE OUR TOP RISKS?"

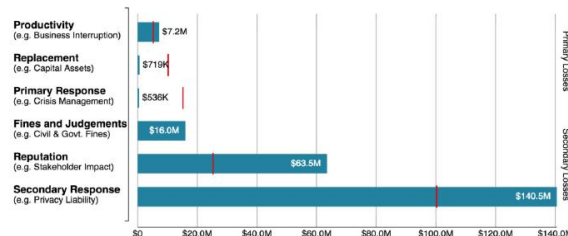


Now you can answer many more questions!

"HAVE WE REDUCED RISK?"



"WHAT TYPE OF LOSS CAN WE EXPECT?"

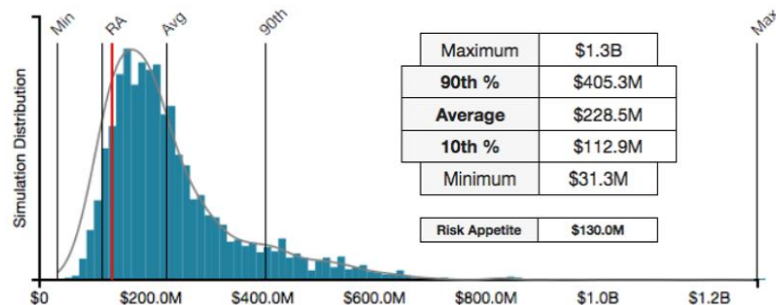


RSA ARCHER CYBER RISK QUANTIFICATION



Key Features

- Built-in risk calibration and analysis engine for cyber risk calculation
- Templated workflow for easy scenario modeling
- On-demand risk analytics for answers to questions on the fly
- Mathematical simulations to build your risk profile with limited data
- Existing loss tables based on industry data
- Easy-to-use SaaS application
- User-friendly interface




RSA ARCHER CYBER RISK QUANTIFICATION

A NEW USE CASE WITHIN RSA ARCHER IT & SECURITY RISK

- IT and Security Policy Program Management
- IT Controls Assurance
- IT Risk Management

➤ Cyber Risk Quantification

- Cyber Incident & Breach Response
- IT Security Vulnerabilities Program
- IT Regulatory Management
- PCI Management
- Information Security Management System (ISMS)

NOTE: the "Cyber Risk Quantification" use case is powered in the backend by the  RiskLens tool which is a (SaaS) product integrated with RSA Archer.



RSA PORTFOLIO



RSA CUSTOMER LEADERSHIP



30,000+
customers

50+ million
identities

1 billion
consumers



→ **97%**



→ **94%**

20 of the
TOP 20



Manufacturing



Consumer product



Financial institutions



Healthcare institutions



Transportation

19 of the
TOP 20



18 of the **TOP 20** Telecom



16 of the **TOP 20** Energy



10 of the **TOP 10** Technology



13 of the **15** Executive Departments
of U.S. Government



All branches of US Military

RSA BUSINESS-DRIVEN SECURITY™

RSA INDUSTRY LEADERSHIP

\$60+ billion

Value of transactions protected per year

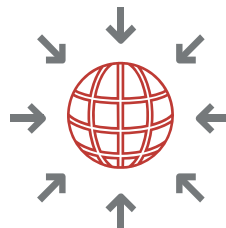
\$8+ billion

Value of fraudulent losses prevented per year

97%



Of malicious sites blocked in less than 30 minutes



1+ million

Advanced attacks detected and stopped



**GSN
Homeland
Security
Award 2015**



Fraud detection rates

6

Gartner
Leaders quadrants



400,000+

Malware samples analyzed per week



**Phishing attack
identified every 30
seconds**

~510 issued patents

~240 pending patents

across current product portfolio

4M

Indicators of compromise actively maintained in **RSA Live Threat Intelligence**



**Technology
Awards**
2016, 2015, 2014, 2013,
2012

THANK YOU

CONTACTS:

ANDERS GREVE, TLF: 3096 4999, EMAIL: ANDERS.GREVE@RSA.COM

JESPER SACHMANN, TLF: 61207022, EMAIL: JESPER.SACHMANN@RSA.COM