CHAIRE DE CYBERDÉFENSE ET CYBERSECURITÉ

SOGETI

Cybersecurity Economics

Expenditures & Cyber Insurance

Pierre-Luc REFALO
Capgemini / Sogeti
Global Head of Strategic Consulting

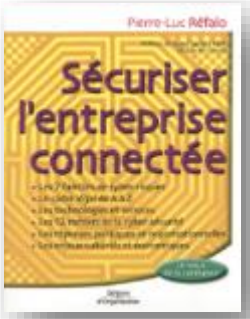
Paris - Hôtel des Invalides
14th, November 2016 (V1)

The speaker: Pierre-Luc REFALO

25 years in Information & Cyber Security consultancy

CISO for SFR & Vivendi Universal (1997 – 2002)

Author



2002

2012

2013 Award

Teacher

utt université de technologie Troyes

ESIEE PARIS

TELECOM & Management SudParis

Speaker

lesassises de la sécurité et des systèmes d'information

FIC 2013

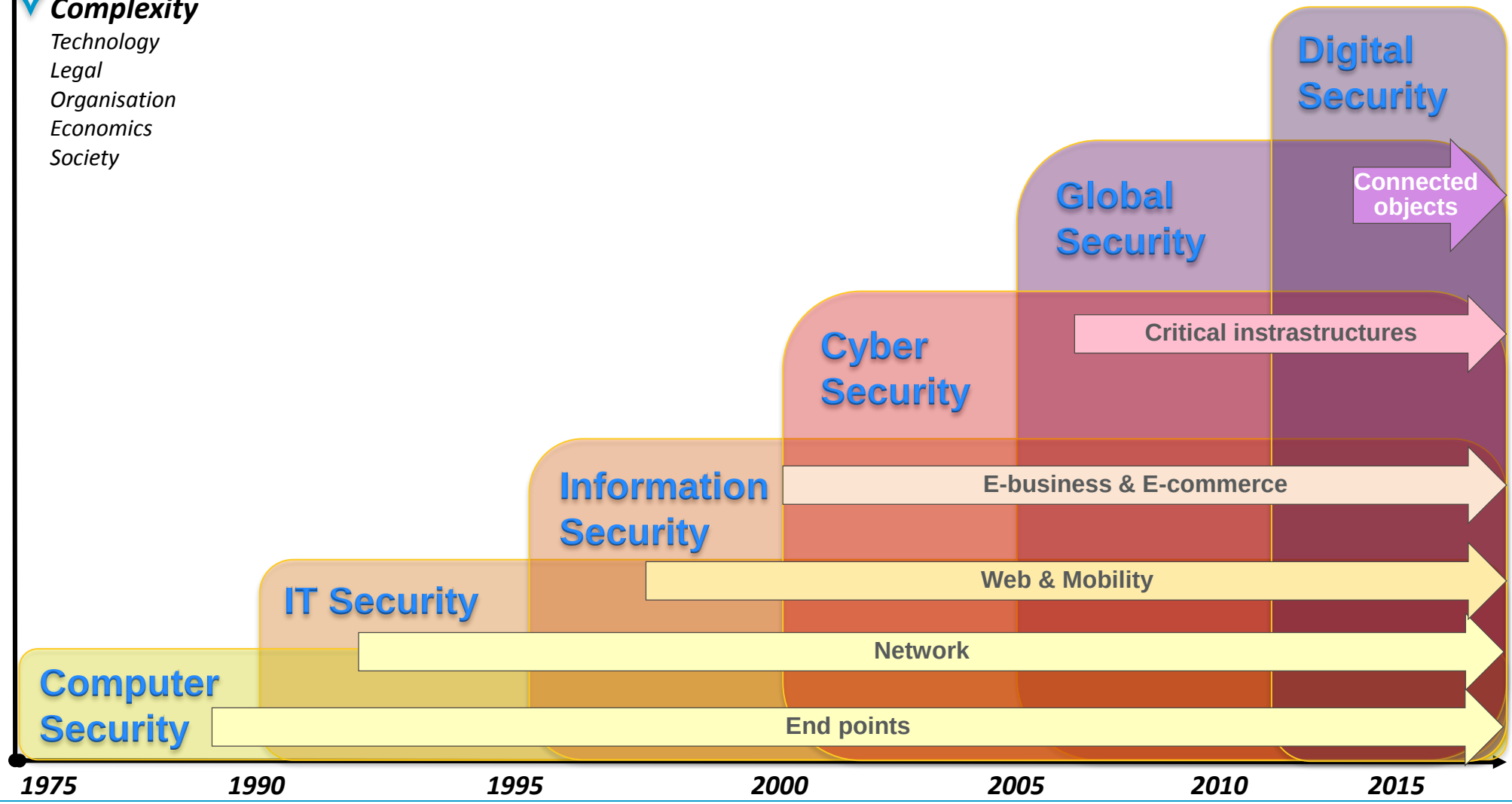
NET FOCUS

ISACA Trust in, and value from, information systems

Gartner

CSI COMPUTER SECURITY INSTITUTE

The new Digital Security Age: Full Business Transformation



What is (cyber) security?
In real: no single definition exists…

Risk based (assessed)

Transparent / Invisible (few contrainsts)

Integrated (limited « over cost »)

Ethical (invididual rights)

Control based (evidences)

Focused (vs stakes and business)

Mesureable (vs risks)

Human based (economics)

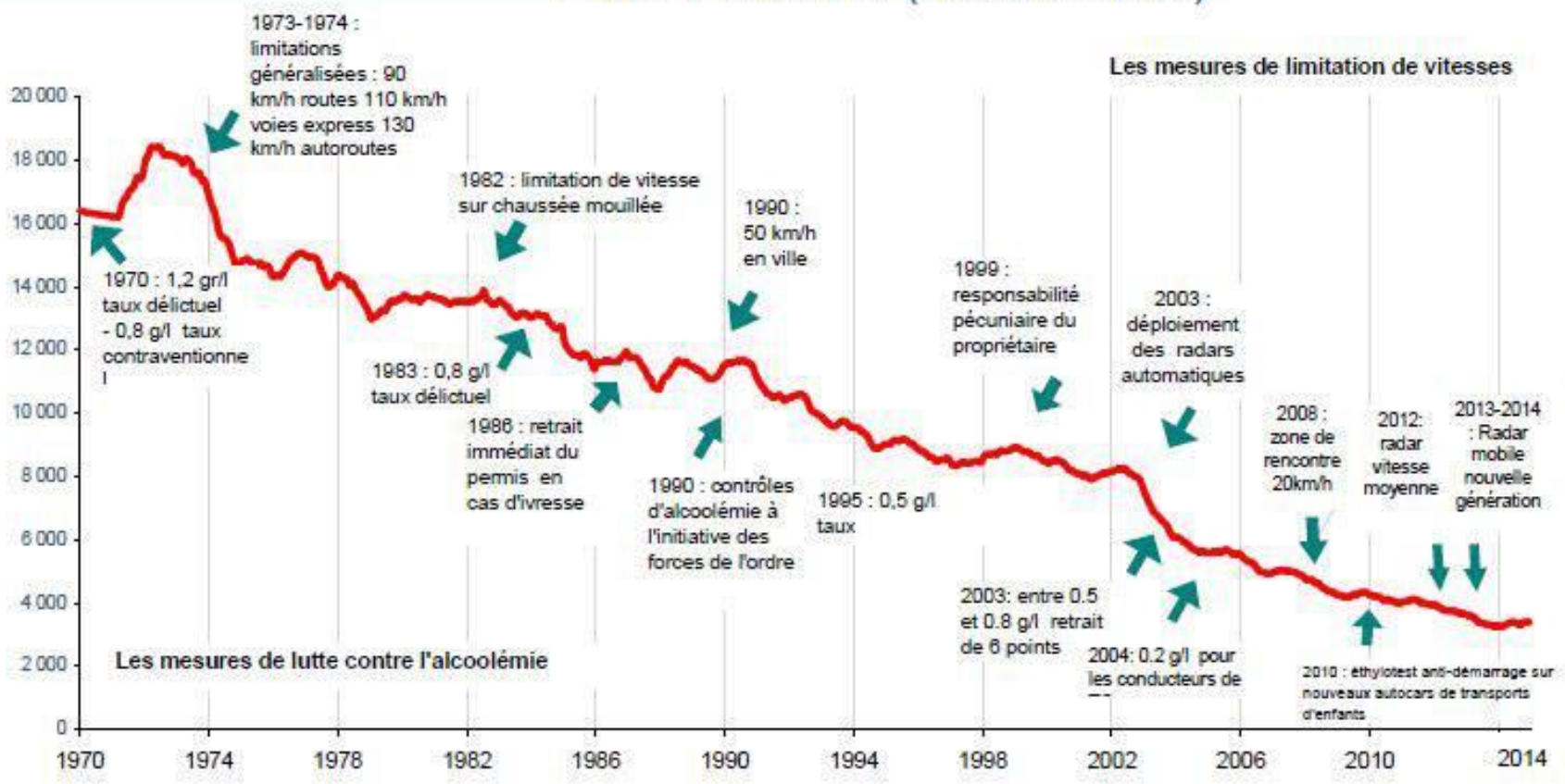
Visible (for confidence)

Operationnal (outcomes)

Something that cannot be measured does not exist!

« *La vie ne vaut rien, mais rien ne vaut une vie* » A. Malraux

Evolution de la mortalité routière en France (Source ONISR)

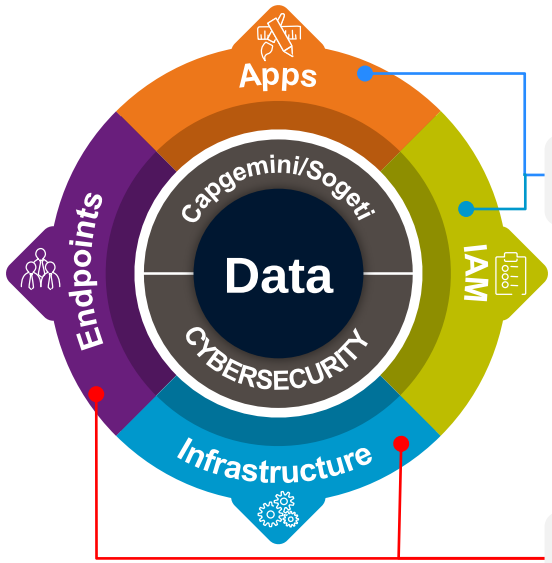


What will be the security cost of a connected car?

The best analogy: What is the cost of an Airport Digital Security?

Including (cyber) security, privacy and safety (for IT, OT and IoT)

The new Digital Landscape – IT & OT



Digital Factory

Level 4
Corporate IT System

ERP
Data Warehouse
Billing

Corporate IT System

Level 3
Operations Management

MES
DMS, EMS
MDM

Level 2
Supervision and Control

Acquisition
Historian
Supervision

Industrial Control System

Level 1
Automation

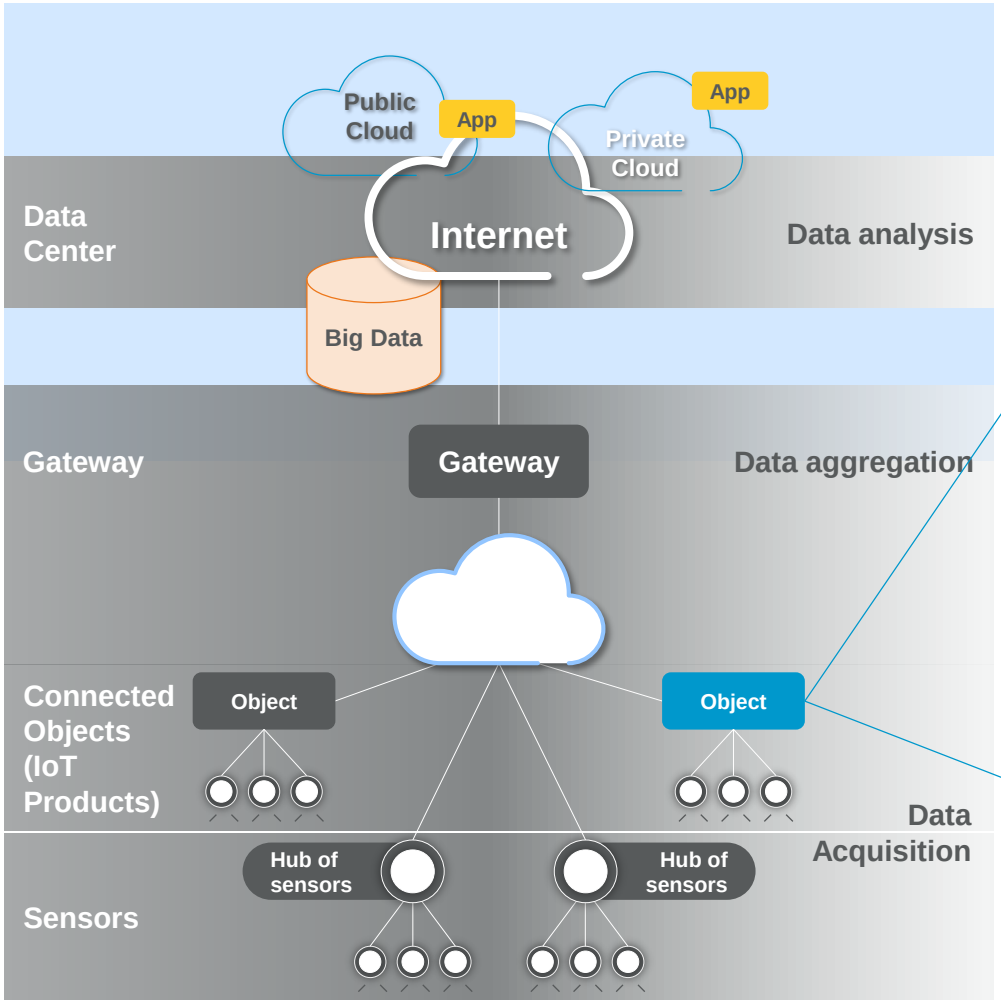
Digital bus
Controller
Controller
Point-to-point connection

Controller
Digital Bus
PC Industriel
Distributed IOs
Industrial wireless
Point-to-point connection

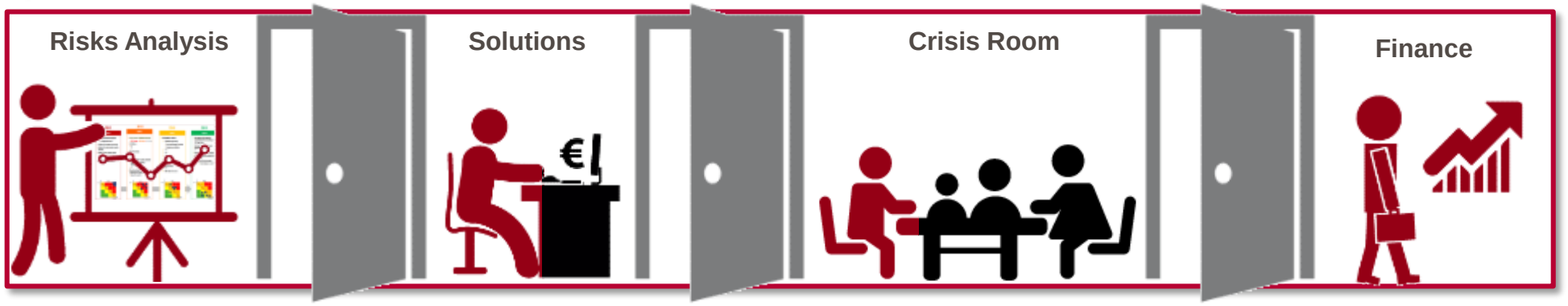
Digital bus
RTU
Controller
Remote systems
Point-to-point connection

Level 0
Sensors and Actuators

The new Digital Landscape – IT & IoT



Cybersecurity economics answers the four aspects that structure the top management decision-making



Risks Analysis	Solutions	Crisis Room	Finance
What is the financial impact of a cyber risk? What would be unbearable for the organization?	How much do we spend to secure our digital assets? Is this consistent and balanced?	In case of a security / data breach, what is the real economic impact? What are the most critical incidents?	How to optimize the company's expenditure? Is Cyber Insurance a relevant solution?
Analyze and anticipate risks	**Take measures to prevent & protect and to detect & react**	**Measure the impact of security and data breaches**	**Optimize budgets and spending**

Cybersecurity economics aids decision-making

Analyze and anticipate risks

I have elaborated a risk matrix based on business & IT challenges of my digital strategy

What is the impact of a major cyber risk on my crown jewels?

Benefits of connectivity and security costs

"The annual costs of cyber disruptions begin to reduce the incentive for doing business in a connected world."

* The startling economic truth about cyber risks" Atlantic Council and Zurich Insurance group. Sept. 2015

Take measures to prevent & protect and to detect & react

I have defined a Cybersecurity Strategy based on the most critical risks…

How much & where do I spend money exactly to protect my digital crown jewels?

Worldwide Spending

*"**Worldwide spending** on information security will reach **$75.4 billion in 2015**, an increase of 4.7 percent over 2014**". "**$50 billions are spent on services".*

*Gartner Inc, Press release, 2015

Cybersecurity Economics

Optimize budgets and spending

I need to combine current expenditures with a Cyber Insurance to optimize my spending

How can I optimize the company's Cyber Security spending in the future?

Towards a Cyber Insurance policy

"Cyber Insurance is not there to replace sound risk management; it is there to supplement it"

*Toby Merrill, vice president of insurer ACE Professional Risk

Measure the impact of security and data breaches

I have been victim of a security incident...

What is the real economic impact on my reputation and business processes?

Average Annual Losses

*"The cost to businesses of cyber crime continues to climb. **Average annual losses to companies worldwide now exceed $7.7 million,** with studied companies losing up to $65 million".*

*Ponemon Institute., *2015 Cost of Cyber Crime Report*

Security costs to be measured (or not)

Governance (*: requires specific tools or third party services)

ORGANIZATION		Internal	Out Sourced
Digital Risk Officer CSO / CISO / DPO office	Internal team (FTE) Correspondent network (FTE) Communication & Awareness (*) Community management Dashboard management (*)	✓	✓
Digital Risk Management	Risk analysis / matrix (*) Threat intelligence (*) Crisis management Cyber Insurance (*)		✓
Strategy & Planning	Strategy / Roadmap / Transformation Security & Privacy Program management Organization transformation		✓
Operations	Policies and procedures ISMS implementation / management (*) Training plan (*) Incident management & forensics	✓	✓
Assessment & Audit	Pen test (*) Vulnerability assessment (*) Code audit / Application security testing (*) Organization audit Compliance audit (*)	✓	✓

Security costs to be measured (or not)

Protection services

PROTECTION		HW	SW	Build / Run
Infrastructures	Firewalls, IDS, IPS, VPN Anti malware gateway NAC, Network segmentation, segregation Secure protocols, routing Hardware hardening Public Key Infrastructure	✓	✓	MSSP
End points	Security suite (FW, Anti malware, HIPS) Application management, Patch management IOCs discovery tool, remediation tool		✓	MSSP
User Id & Access	2FA device SSO & IAM Risk based authentication Privilege account management	✓	✓	MSSP
Applications	Secure coding lifecycle, OWASP review WAF, database firewall Security testing, pentesting Patch management Database hardening		✓	MSSP
Data	Laptop encryption Email encryption Tokenization & Data masking Data destruction Cloud encryption	✓	✓	MSSP

Security costs to be measured (or not)

Monitoring services

SUPERVISION		HW	SW	Build / Run
Infrastructures	Log management Sand boxing DNS supervision SIEM SOC CERT	✓	✓	MSSP
End points	End point Log management SOC	✓	✓	MSSP
User Id & Access	AD log management SOC	✓	✓	MSSP
Applications	Application log management Analytics and fraud management SOC	✓	✓	MSSP
Data	Data leak prevention SOC	✓	✓	MSSP

Some figures (1/3)

%

Prevent Protect **85 %**

Detect React **15 %**

Techno **50 %**

Service **50 %**

IT Security Budget **4 %** **10 %**

Market Growth **5 %** **10 %**

Key figures (2/3)

€ / user

3 FTE / 1000 user

1 FTE / 1000 user

0,2 FTE / 1000 user

5000 users — **20 000 users**

25 € / user

5 € / user

3 € / user

Le Cercle Européen de la Sécurité - 2011

Key figures (2/3)

€ / endpoint

	5000 users	20 000 users
	25 €	12 €	2,5

	5000 users	20 000 users
	50 €	35 €	10 €

	5000 users	20 000 users
	30 €	16 €	5 €

Le Cercle Européen de la Sécurité - 2011

Cyber Insurance can complement cybersecurity measures by transferring part of the risks

Compliance

Continuity

Reputation

Ensuring compliance, business continuity, and safe-guarding reputation means choosing the right mix of investing in cybersecurity measures and transfering risks to Cyber Insurance.

Cybersecurity economics ensures that spending is allocated to the most effective measures.

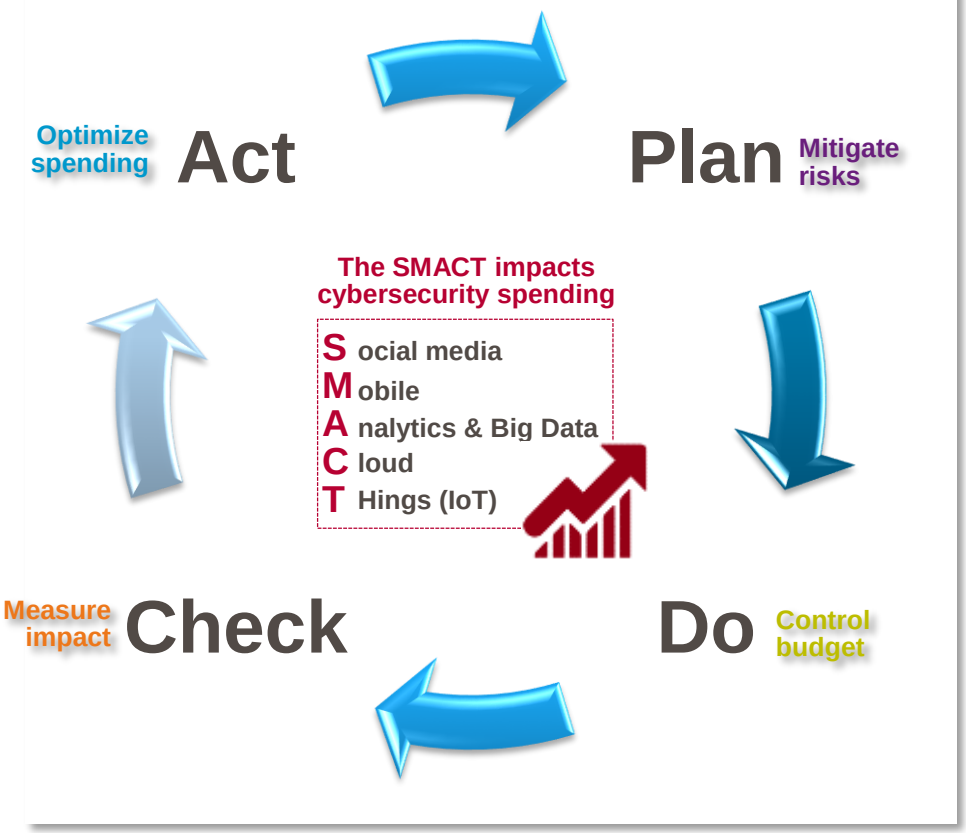
Balance between prevention / protection and detection / detection

In many cases optimization is best reached by transferring (part of) the risk to an insurance policy.

Transfer risk to a Cyber Insurance policy

Cyber Insurance
What are we speaking about?

Companies spend money to ensure cybersecurity



What is the breaking point?

When cybersecurity spending weighs too much or negatively counterbalance savings from digital transformations, companies can decide to transfer the risk to an insurance policy

Examples of Insurance Policy Benefits

Mitigate risks	Protection against main risks identified by the insurance company (depending on type, sector, etc)
Control budget	Decreasing in the company's internal spending and re-allocation to an Insurance Policy
Measure impact	Possibility to get Insurance support in crisis management
Optimize spending	Recommendations to mitigate risks and avoid new cybersecurity incidents

What is Cyber-risks & Cyber Insurance?

Il s'agit des atteintes aux systèmes et aux données qui peuvent être consécutives à de nombreux facteurs: un acte malveillant ou terroriste, une erreur (plus de la moitié des attaques sont facilitées par la négligence humaine), une panne, des problématiques techniques, un événement naturel ou accidentel.

Quant aux conséquences, elles peuvent englober les dommages corporels, matériels et immatériels, la mobilisation de ressources internes ou externes, susceptibles de susciter des frais, ainsi qu'une atteinte à la réputation.

Le périmètre englobe les sous-traitants d'une entreprise donnée.

MOTS / CONCEPTS CLE

Couverture
Scénarios
Dommages
Exclusion

Contrats / Polices
Dommages
Responsabilité civile
« Tous risques informatiques »
Fraude
Ou Spécifiques

Services
Assessment / Diagnostic
Expertise / Incident
Gestion de crise
Assistance juridique

The “Target case”

How Cyber Insurance has decreased financial losses of a Cyber attack

When the risk gets real…

- Social engineering (human factor)
- Intrusion with Advanced Persistent Threats Attacks (APT)
- Data leak (client data)
- Etc.

40 millions of financial data & 70 millions of personal data stolen

Companies face major consequences…

- Reputation (visits decrease & trust is harmed)
- Financial losses (need to strengthen security & material)
- Law suits
- Etc.

Loss of revenue (Q4 2013) $252 millions

TARGET Net loss = $105m (0,1% of 2014 sales)

… and optimization can limit the financial impact

- Combination of specific cyber security spending and Cyber Insurance Policies can help limiting financial losses

Reduced taxes: $57 m
Insurance reimbursement = $90m

*Source: Columbia University, Benjamin Dean

Takeaways (1/2)

Takeaways (2/2)

Digital Crown Jewels **International regulations**	**Contracts / Clients** **Local / vertical regulation**	**Baseline** **Minimum Standards**
Executive Committee **Risk Manager**	**Business Owners** **Digital Risk Officer**	**CSO / CIO** **CISO / DPO**

About Capgemini Consulting and Sogeti

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

www.capgemini-consulting.com

www.sogeti.com/cybersecurity