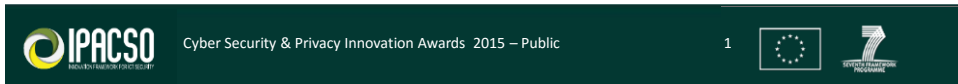


#IPACSOawards2015

Wifi : LT\_Visitors

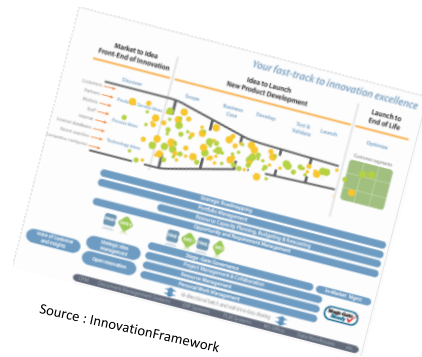


## Welcome & Introduction

Ulrich Seldeslachts  
LSEC – Leaders In Security






# About IPACSO

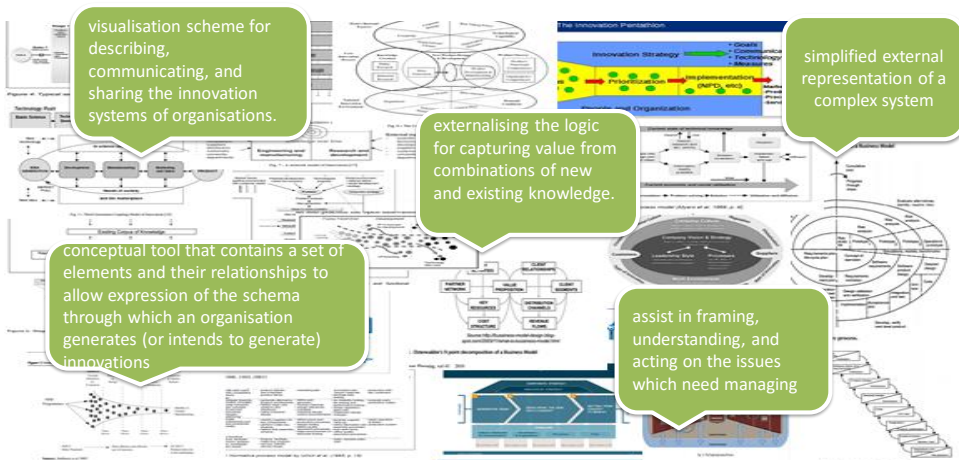





## “Innovation Framework for Privacy and Cyber Security Market Opportunities”

develop a structured knowledge and decision-support innovation framework for identifying, assessing and exploiting market opportunities in the privacy and cyber security technology space. ...


 Cyber Security & Privacy Innovation Awards 2015 – Public
 


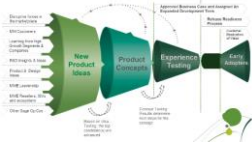
# Innovation Models




 Cyber Security & Privacy Innovation Awards 2015 – Public
 


# Supporting Trustworthy ICT

Analyze the innovation process in privacy and cyber security technologies






Identify obstacles



Propose improvements, market conditions and economic incentives to invest in ICT security



Source : Sage, Innovation Process; Cranfield, Advanced Marketing Planning, InnovationCrescendo


 Cyber Security & Privacy Innovation Awards 2015 – Public
 5



## Targetted to

Cyber Security & Privacy Innovators and Entrepreneurs



Cyber Security & Privacy Researchers






Business Brokers & PE



Policy Makers & Research Agenda




 Cyber Security & Privacy Innovation Awards 2015 – Public Board
 6





## For Innovators

- Innovation Management Support Tools
  - Provide access to State of the Art Innovation methodologies, applied to ICT Security
  - Innovation Use Cases & Best Practices
  - Innovation Framework for Cyber Security & Privacy
- Marketing Support
  - Provide access to Cyber Security & Privacy Market Assessment
  - Market and Regulatory Environment Analysis Support
  - Cyber Security & Privacy Market knowledgebase
  - Cyber Security & Privacy Technology & Research Spectrum
- Facilitating identification of Inhibitors and Incentives
  - Cyber Security & Privacy Economic Incentives
  - Access support to State of the Art Cyber Security & Privacy Research
- Training & support
  - Innovation Bootcamps and training packages
  - Access to Brokers and Corporate Development Support
- ICT Innovation Awards
  - Marketing of ICT Security Innovators – publishing cases and case studies
  - Representation towards Private Equity industry



Source : Innovationmanagement.se

**MORE THAN 6000** visitors per month

**13** BOOTCAMPS with over **100** cyber security starters **TRAINED**

**Over 300** European cyber security innovators registered for **Innovators Awards**

**Digipass BT**  
**VASCO**  
THE AUTHENTICATION COMPANY

**96** **TOOLS**  
For starters

Innovations materialized using the innovation framework

**IPACSO Bootcamp**

# The Framework



10

# IPACSO Bootcamp

## Market Analysis –

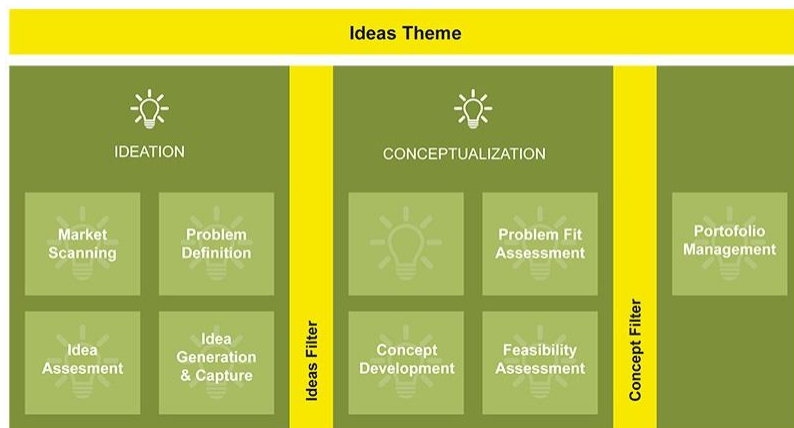
- Trends & Challenges
- Market Overview
- Science & Technology
- Policy Framework & Legislation


## Economics –

- Cyber-Security
  - Introduction & Basics
  - Research Field
  - Decision Models
  - Indicators & Metrics
- Privacy
  - Introduction & Basics
  - Research Field
  - Preference Measurement
  - Privacy Metrics
- Economic Incentive Schemes



# IPACSO Bootcamp






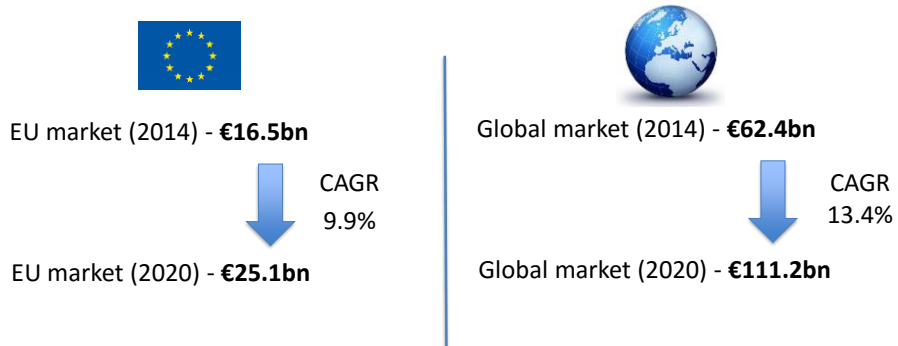
# IPACSO

CYBER SECURITY

## Why IPACSO?




 Cyber Security & Privacy Innovation Awards 2015 – Public 13  

## PACs Market Growth



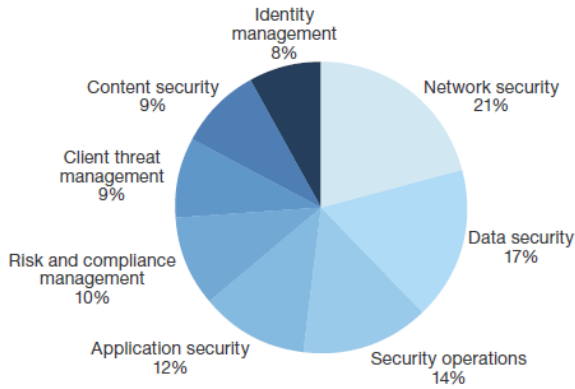
~26% share of global market at present  
Decrease to ~23% predicted by 2020

Source: Frost and Sullivan (2014)

 Cyber Security & Privacy Innovation Awards 2015 – Public 14  

# Security Spending

Percentage of Annual Security Budget – Which tech?






57% - want to buy their security from one vendor

-have best-in-breed, simplify integration!

-M&A driver

-small PACs vendors – need pipeline, large tech vendors need access to new tech

Source: Forrester, June 2013, survey of 2000 US and European Security Professionals


 Cyber Security & Privacy Innovation Awards 2015 – Public
 



## PACS Segments

### BY SECURITY TYPE




- Network
- Endpoint
- Application
- Content/Data
- Wireless
- Cloud
- etc....

### BY SOLUTION

- Identity And Access Management (IAM)
- Risk And Compliance Management
- Encryption
- Data Loss Protection (DLP)
- Unified Threat Management (UTM)
- Firewall
- Antivirus And Antimalware
- IDS/IPS
- Security And Vulnerability Management
- Disaster Recovery
- DDOS Mitigation
- Web Filtering
- Etc...

### BY SECURITY SERVICE

- Consulting
- Design and Integration
- Risk and Threat Assessment
- Managed Security Services
- Training and Education


 Cyber Security & Privacy Innovation Awards 2015 – Public
 



# European ICT Security Industry Fragmentation

... la filière qui compte près de 700 acteurs ...

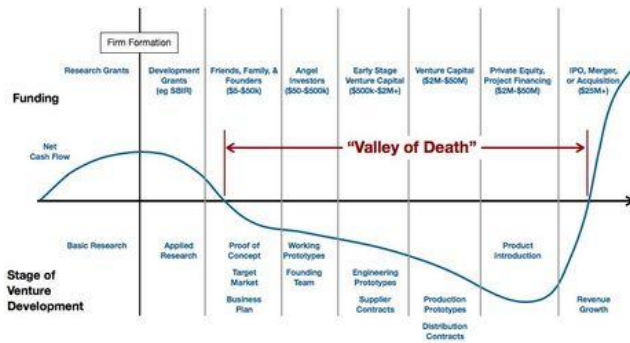


Source : <http://www.usine-digitale.fr/article/le-plan-pour-doper-l-industrie-tricolore-de-la-cybersecurite-N260867>

IPACSO Cyber Security & Privacy Innovation Awards 2015 – Public Private & Confidential, FIRE Project 17 17

## The Second Valley of Death

### Lifecycle of a venture



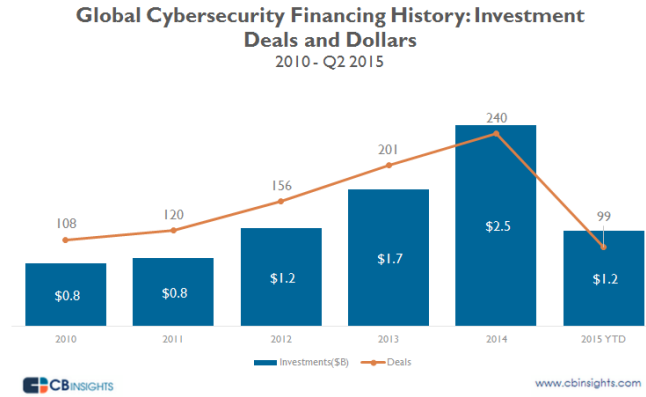
UCDAVIS CENTER FOR ENTREPRENEURSHIP




Graduate School of Management UCDAVIS

IPACSO Cyber Security & Privacy Innovation Awards 2015 – Public 18

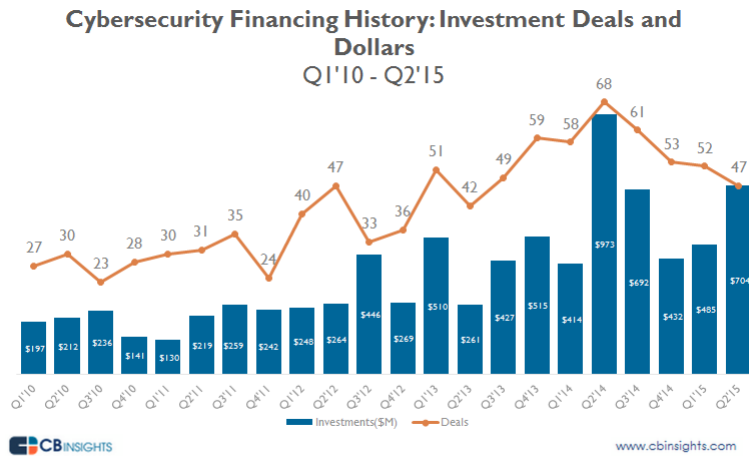
## Demand for Trustworthy ICT – Security Industry




- Investors put 4.6 Billion USD into cybersecurity startups in the last 2 years




 Cyber Security & Privacy Innovation Awards 2015 – Public
 



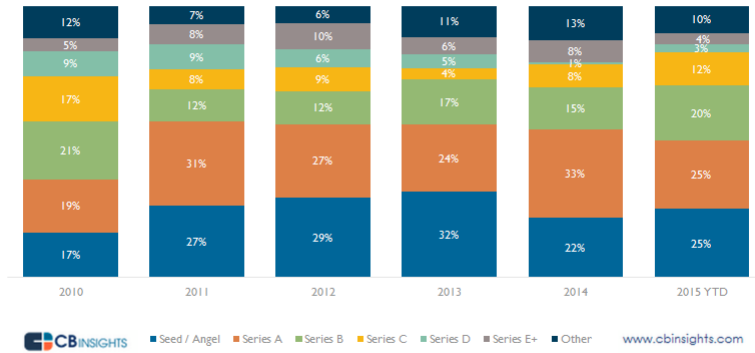
## Demand for Trustworthy ICT – Security Industry







 Cyber Security & Privacy Innovation Awards 2015 – Public
 



## Demand for Trustworthy ICT – Security Industry

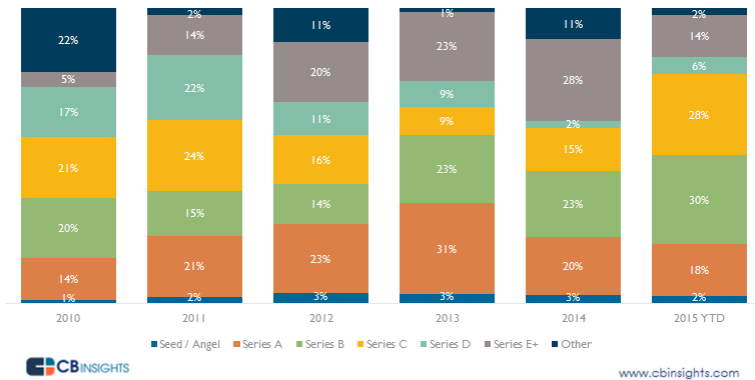
**Cybersecurity Financing Deal Share**  
By Stage, 2010 - Q2 2015







 Cyber Security & Privacy Innovation Awards 2015 – Public
 



## Demand for Trustworthy ICT – Security Industry

**Cybersecurity Financing Dollar Share**  
By Stage, 2010 - Q2 2015




 Cyber Security & Privacy Innovation Awards 2015 – Public
 



## Investment – typically Larger Funds

Most Active Cybersecurity Investors: 2010-Q2'15	
Rank	Investor
1	Intel Capital
2	Kleiner Perkins Caufield & Byers
2	Andreessen Horowitz
2	Accel Partners
3	Bessemer Venture Partners
4	Google Ventures
5	Norwest Venture Partners
5	New Enterprise Associates
5	Sequoia Capital
5	Lightspeed Venture Partners




Cyber Security & Privacy Innovation Awards 2015 – Public

23



## Early Stage Investors

Most Active Early Cybersecurity Investors: 2010-Q2'15	
Rank	Investor
1	Andreessen Horowitz
2	Google Ventures
2	Accel Partners
3	Kleiner Perkins Caufield & Byers
4	SV Angel
4	Norwest Venture Partners
4	Bessemer Venture Partners
5	Founder Collective
5	Data Collective
6	New Enterprise Associates




Cyber Security & Privacy Innovation Awards 2015 – Public

24





**IPACSO**  
CYBER SECURITY

Cyber Security & Privacy Challenges  
in 2015 & beyond


 Cyber Security & Privacy Innovation Awards 2015 – Public
 25





## A Deluge of Breaches

*3 macro level themes to disrupt the cycle*

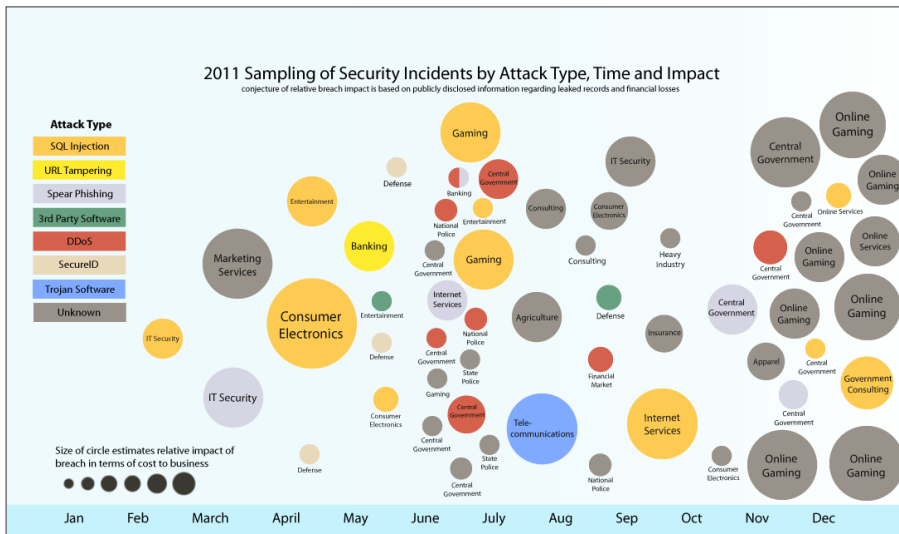
**Jason Kravitz**

IBM Security

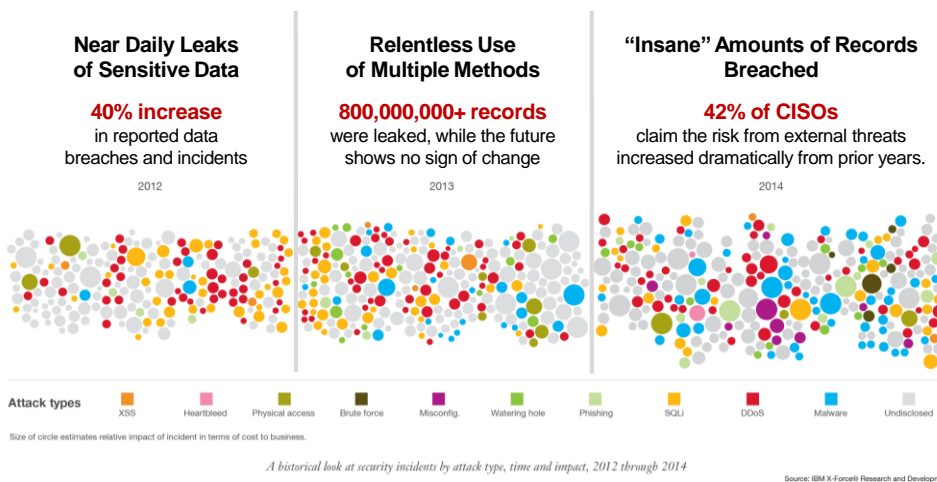
October 22, 2015



## 2011 – Year of the Breach (or was it?)



## 2012 – 2014: 83% of CISOs say that the challenge posed by external threats has increased in the last three years



Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015 and 2014 IBM Chief Information Security Officer Assessment

### Take-out Restaurant



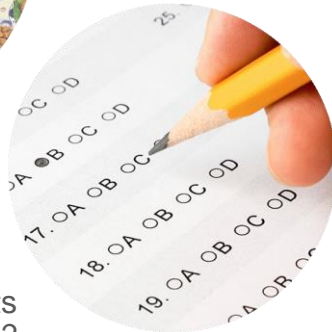
Source: Planet Takeout Flickr (not affiliated with actual incident)

### Bill the CFO



(not affiliated with actual incident)

### College Exams



Source: Alberto G Flickr (not affiliated with actual incident)

what are the biggest threats to your enterprise?

# Lack of Security Fundamentals



## Lack of Security Fundamentals: Social Engineering Still Works

### Bill the CFO



(not affiliated with actual incident)

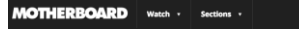
### 27 FBI: \$1.2B Lost to Business Email Scams

AUG 15

The FBI today warned about a significant spike in victims and dollar losses stemming from an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers. According to the FBI, *thieves stole nearly \$750 million in such scams from more than 7,000 victim companies in the U.S. between October 2013 and August 2015.*

In January 2015, the FBI released stats showing that between Oct. 1, 2013 and Dec. 1, 2014, some 1,198 companies lost a total of \$179 million in so-called **business e-mail compromise (BEC)** scams, also known as "CEO fraud." The latest figures show a marked 270 percent increase in identified victims and exposed losses. Taking into account international victims, the losses from BEC scams total more than \$1.2 billion, the FBI said. The scam has been reported in all 50 states and in 79 countries

<http://kebabsecurity.com/2015/08/fbi-1-2b-lost-to-business-email-scams/>



### How a Clever Hacker Tricked a Major Bitcoin Company Out of \$1.8 Million

September 17, 2015 // 12:15 PM EST

second step verification could have saved millions of \$\$\$



© 2015 IBM Corporation 31

## Lack of Security Fundamentals: Poor Passwords

<ul style="list-style-type: none"> <li>• POS Remote Support Login</li> </ul> <p><b>Default</b></p> <p>admin: admin</p>	<ul style="list-style-type: none"> <li>• Hash Cracking</li> <li>• Admin Servers</li> <li>• Cloud Accounts</li> </ul> <p><b>Weak</b></p> <p>abc123</p>	<ul style="list-style-type: none"> <li>• Loyalty Cards</li> <li>• Frequent Flyer</li> <li>• Webmail</li> </ul> <p><b>Reuse</b></p> <p>abc123 abc123 abc123</p>
--	---	--



weak passwords reused from other breaches = more breaches



© 2015 IBM Corporation 32

## Lack of Security Fundamentals: Insiders and Access Controls

### Who are the “bad guys”?



- Auditing users with access to sensitive data
- Improper provisioning of privileged accounts
- Shared admin passwords on servers impacts accountability
- Remote access tools installed and used by ex-employees

Source: [IBM 2015 Cyber Security Intelligence Report](#)

## Cracks in the Foundation



## Cracks in the Foundation: Malware at the Watering Hole

### Take-out Restaurant



Source: Planet Takeout Flickr (not affiliated with actual incident)

### *Hackers Lurking in Vents and Soda Machines*

By NICOLE PERLROTH APRIL 7, 2014

SAN FRANCISCO — They came in through the Chinese takeout menu.

Unable to breach the computer network at a big oil company, **hackers infected with malware the online menu of a Chinese restaurant** that was popular with employees. When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the business's vast computer network.

<http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html>

attackers take path of least resistance for **return on exploit**

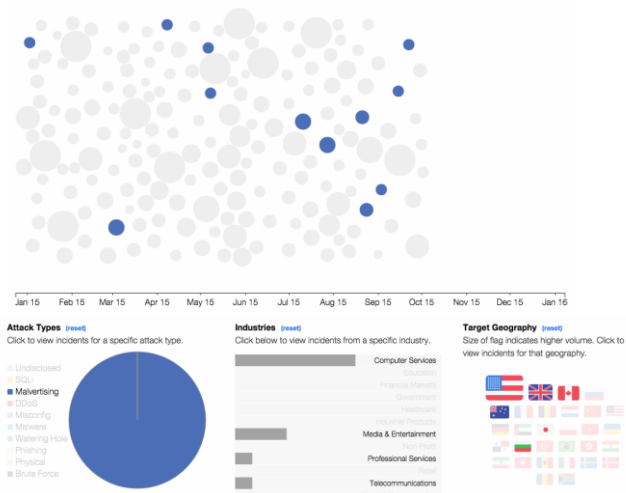
## Cracks in the Foundation: Vulnerable Core Platforms



millions of sites using a limited number of technology platforms can result in **widespread exploitation**

## Cracks in the Foundation: Malvertising on the Rise

### IBM X-Force Interactive Security Incidents

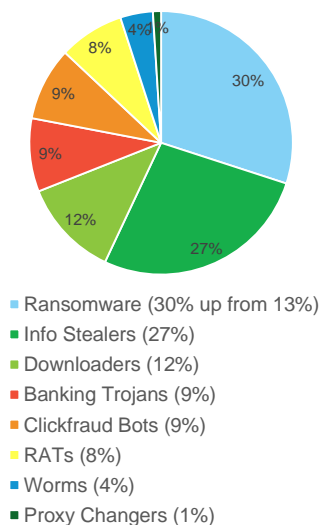


**infected ads**  
no click required

source: <http://IBM.com/security/xforce/xfisi>

## Cracks in the Foundation: Threat Roundup, Ransomware Rising

Malware Threat Roundup  
(Sep 2015 IBM Trusteer Apex Customer Endpoints)



**2010**

**WinLock non-encrypted premium-rate SMS unlock**

**2013**

**CryptoWall, CryptoLock, ZeroLocker**

ransom paid in anonymous crypto-currencies

**2014**

Ransomeb attacks target web applications through vulnerable web servers

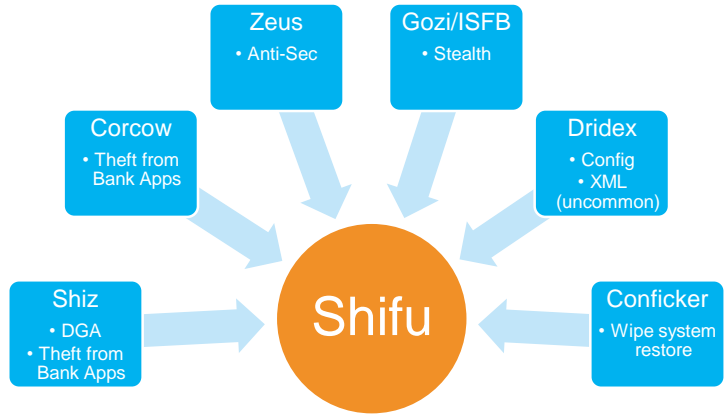
Encrypt data to database

**2015**

Tox "ransom-ware as a service" kit released in the wild

CryptoWall popular (18M + USD)

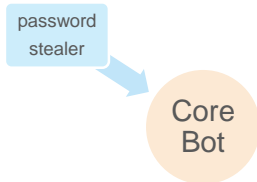
### Cracks in the Foundation: Shifu Malware has Best of Breed Features



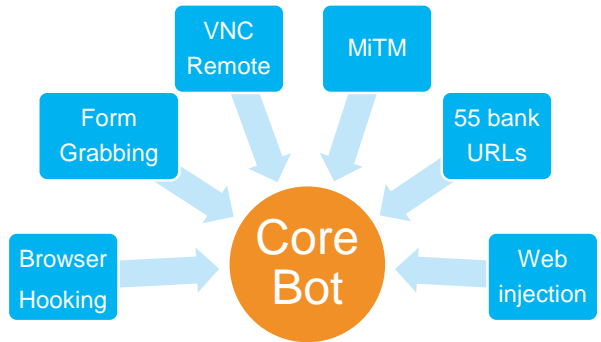
security hooks **prevent other malware** from getting installed

### Cracks in the Foundation: CoreBot, Modular Malware Agilely Adapted

First Version (late August 2015)



Next Version (a few days later)



in **a few days**, CoreBot went from password stealer to **fully featured banking trojan**

read more: <https://securityintelligence.com/an-overnight-sensation-corebot-returns-as-a-full-fledged-financial-malware/>

# Shrinking Privacy in Digital World



© 2015 IBM Corporation

## Shrinking Privacy: Who is Accountable for your Data?

### College Entry Exams



Source: Alberto G Flickr  
 (not affiliated with actual incident)

4/3/15

### Frequently Asked Questions

#### 1. What happened?

A: On March 2, 2015, The university became aware of a data security incident involving the inadvertent exposure of the personal information of some current, former, and prospective students, including applicants who never enrolled or attended the university. The University corrected this internal issue the day it was discovered and retained independent IT forensics experts to help identify the full extent of the data involved, as well as the individuals who may have been affected. While our investigation is ongoing, we have determined that files containing the personally identifiable information of certain current, former, and prospective students were inadvertently accessible through the Internet between September 2014 and March 2, 2015. Although we are unaware of any attempted or actual misuse of any personal information as a result of this incident, we have taken action to directly notify and provide support to all those whose information may have been exposed.




#### 2. What type of personal information was accessible?

A: The information varied depending on each individual, but was some combination of name, address, date of birth, Social Security number, email address, and academic information. No financial information, bank account or payment card information was involved.

marketing firm sells student data which ends up in breach



## These are the Challenges – Where can you Innovate?

<p><b>A lack of security fundamentals</b></p>	<ul style="list-style-type: none"> <li>• Social engineering &amp; phishing still effective</li> <li>• Weak, default, and reused passwords</li> <li>• Lack of policies and controls, insiders undetected</li> </ul> 
<p><b>Cracks in the foundation</b></p>	<ul style="list-style-type: none"> <li>• Widespread x-platform vulnerable browser plugins</li> <li>• Same OS, open-source libraries, and CMS software are foundation of many websites</li> <li>• Several of these systems and libraries had vulnerabilities disclosed in 2014</li> </ul> 
<p><b>Shrinking privacy in a digital world</b></p>	<ul style="list-style-type: none"> <li>• Lack of accountability for how data used and protected</li> <li>• Healthcare record leaks surged in 2015</li> <li>• Attackers leveraging personal / sensitive data</li> </ul> 

## Learn more about IBM X-Force and IBM Security



- TOP 3** enterprise security software vendor in total revenue
- 20** industry analyst reports rank IBM Security as a **LEADER**
- 133** countries where IBM delivers managed security services
- 10K** clients protected *including...*
- 24** of the top 33 banks in Japan, North America, and Australia

- 

 Visit our web page  
[IBM.com/security/xforce](http://IBM.com/security/xforce)
- 

 Interactive Security Incidents  
[IBM.com/security/xforce/xfisi](http://IBM.com/security/xforce/xfisi)
- 

 View upcoming webinars & blogs  
[SecurityIntelligence.com](http://SecurityIntelligence.com)
- 

 Follow us on Twitter  
[@ibmsecurity](https://twitter.com/ibmsecurity)

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

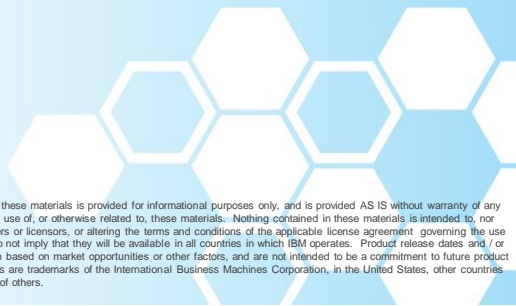
# THANK YOU

[www.ibm.com/security](http://www.ibm.com/security)



## IBM Security

Intelligence. Integration. Expertise.



© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties, or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.



# IPACSO

CYBER SECURITY

## Panel Debate : Innovation Development



Cyber Security & Privacy Innovation Awards 2015 – Public

49



## Panel

- Jason Kravitz, IBM – cyber expert
- Luc Doms, cyber entrepreneur – advisor
- Paul De Hert, Prof. dr. VUB – University Tilburg, privacy innovator
- Dr. Adrian Burden, co-founder UK-Cyber Security Forum



Cyber Security & Privacy Innovation Awards 2015 – Public

50



Cyber Security Innovations through IPACSO



Cyber Security & Privacy Innovation Awards 2015 – Public

51





# Espion

## Leveraging IPACSO Framework + Activities

October 2015

Corrig Court, Corrig Road, Sandyford Industrial Estate, Dublin 18, Ireland  
Phone: +353 1 210 1711 Email: info@espiongroup.com

For more information visit [www.espion.ie](http://www.espion.ie)

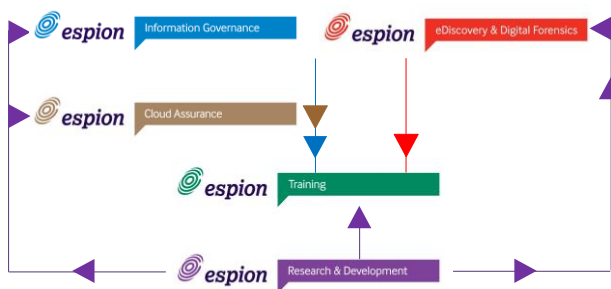
### Espion Snapshot



Irish SME

Founded 2001

~100 employees



(WP2 Lead)

[www.espiongroup.com](http://www.espiongroup.com)

Why IPACSO?



**Next Gen Growth:**  
Formalise R&D (2010)

New Product Development



**Two Key Objectives**

1. Identify + implement company- wide innovation framework
2. Streamlined process for customer engagement

(IPACSO: "PROCESS" THEME)



- "Consultative Selling"
- R&D Tech Roadmapping
- "New Product Development"

(IPACSO: "IDEAS" THEME)



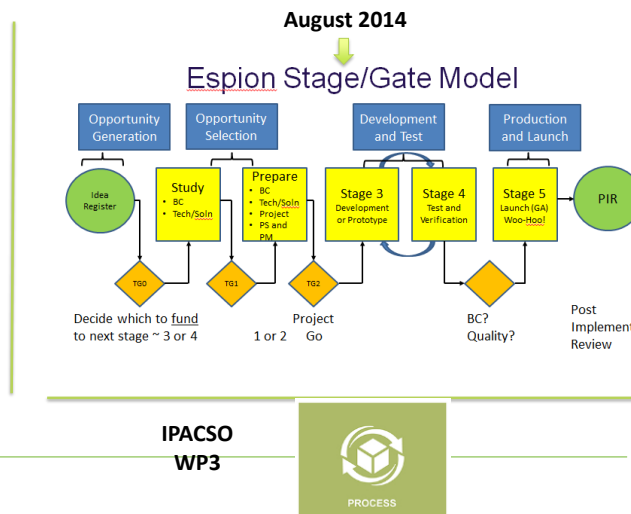
www.espiongroup.com

IPACSO CASE 1 – STAGE GATE INNOVATION FRAMEWORK

**ESPION GOAL:** Identify + implement company- wide innovation framework

**Challenges**

- Ideas not formally captured + prioritised
  - Strategic opportunities missed
- Raise employee understanding of innovation
  - Innovation NOT just R&D!
- Risk averse approach
  - R&D + Consultancy – cultural differences
  - Product ideas not adequately resourced or pursued

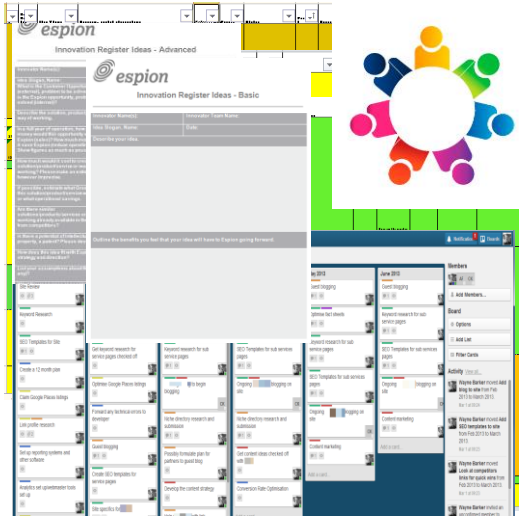


IPACSO WP3



IPACSO CASE 1 – STAGE GATE INNOVATION FRAMEWORK 

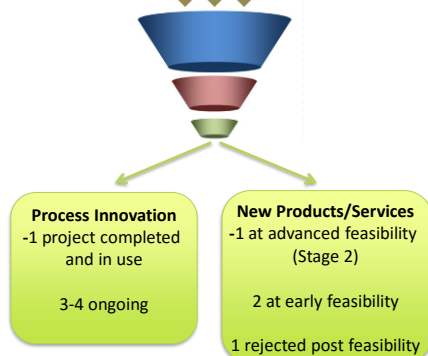
- Idea Forms
- Idea Board
- Idea Register
  - Excel to Trello planned
- Idea is categorised
  - New product/service
  - New process/WoW
  - Research Enquiry
- Idea is assessed
  - **ACTION**
  - **ICEBOX**
  - **HOLD/IMPLEMENT**
- **Ideal:** 3 to 4 new ideas being assessed/pursued at any given time



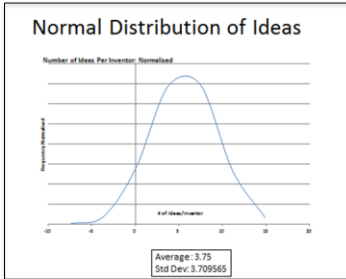
IPACSO CASE 1 – STAGE GATE INNOVATION FRAMEWORK 



75 ideas registered thus far



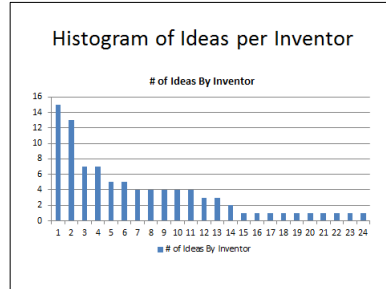
- Report Process Automation
- Privacy Mgt + Governance
- Test estimation and scoping
- SIEM "Lite" for OT-Based
- PCI Audit Optimisation
- Critical Infrastructures
- Enterprise Search
- Email Data Reconstruction + QC
- "CORTESE"



Avg. of 3-4 ideas per proposer

**24 individuals have submitted at least one idea**

(~1 in 4)



Small minority are prolific!

**7 in 10 ideas are based around new products and services – HIGH!**

**28% of ideas are in “ACTION” state – exceeds resource availability**

**POSITIVES?**



- **Focused + repeatable process**
- **Observable, Transparent, Measurable**
- Complementary teams get alot done quickly!

**NEGATIVES?**



- Engagement **beyond R&D** challenging at times
- **Syncing of resources** across divisions - bottlenecks common
- Finance + **Working Capital** lacking for largest ideas

**IMPROVEMENTS?**



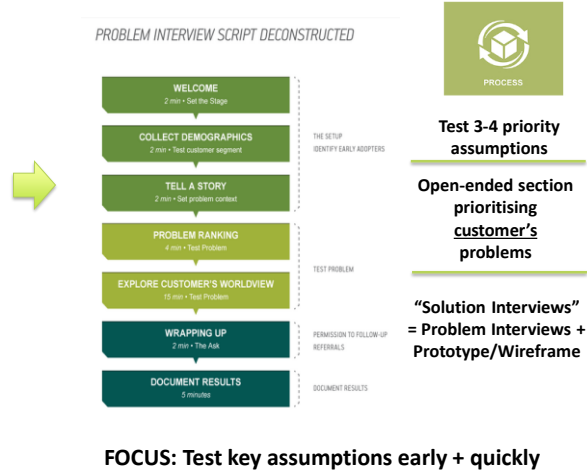
- Cross-functional workshops + synergies
- How to do more “Open Innovation”
- Decreasing the idea backlog – becoming more ruthless with ideas
- Incentives/Rewards!

## IPACSO CASE 2 – STRUCTURED CUSTOMER ENGAGEMENT

### Customer Engagement – Challenges/Concerns

- Sales-based bias in interviewing
  - Day-to-day trumps long term
- Ad-hoc, non-standardised approach among team
- Capturing maximum info in least time available (time pressed CISOS/C-Level people) – reduce waste
- Support multiple needs:
  - Consultative Selling
  - R&D Roadmap
  - Product Concept Validation

### Lean Problem Interviewing Approach



## IPACSO CASE 2 – STRUCTURED CUSTOMER ENGAGEMENT

### Key Advantages



- **Time efficient**
  - 30 mins max for problem interviews
  - 1 hr max ideal for solution interviews
- Script **focuses on key priority issues** being solved
  - Less is more (~3-4 max)
  - Reduce background noise from open-ended formats
- Engenders **openness** from customer – research discussion first, sales discussion second
  - Can be difficult for some to adapt – go off script easily

## IPACSO CASE 2 – STRUCTURED CUSTOMER ENGAGEMENT

### Streamlined Interview Approach - Used Multiple Ways To Date

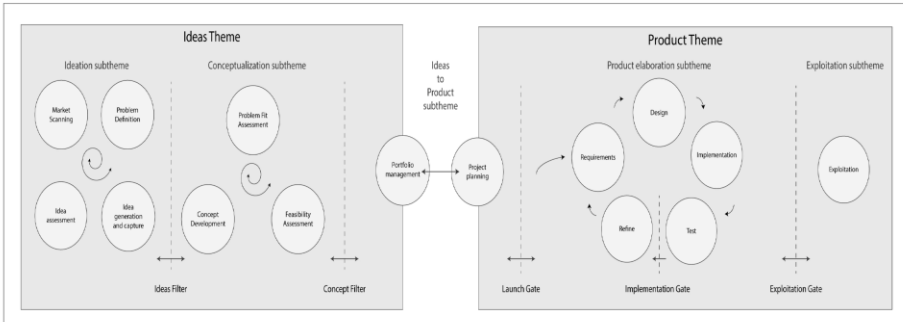
When	Project	Customer Audience	Interview Format	Status
Aug-Oct 2015	<b>Consultancy – Top 15 customers</b>	CISOs + IT Heads in each company	Problem Interview 1. Cyber security maturity + readiness 2. Strategic direction for cyber security 3. Key improvement projects 4. What kept them awake	11 of 15 interviews completed to date
June-July 2014	<b>Privacy Management Concept – Validation</b>	DPOs + Privacy Professionals	Problem interview – early concept validation  Prioritisation of problems + potential feature solutions	10 interviews Solution interviewing to occur post prototype
Nov-Dec 2014	<b>DocGenie - Product Validation</b>	Law Firms, Record Management players	Stage 1 problem interviews + Stage 2 prototype validation via solution interviews	15 interviews Concept failed at stage 2
Nov 2015 (TBC)	<b>SIEM “Lite” for CIs</b>	Critical Infrastructure Operators	Problem interview - early concept validation	Planned/TBC

## Background on VASCO

- International company
- Leading supplier of strong authentication and e-signature solutions
- Customer base of 10,000 companies in more than 100 countries, including more than 1,700 banks
- Prime markets: financial sector, enterprise security, e-commerce and e-government

# IPACSO Framework

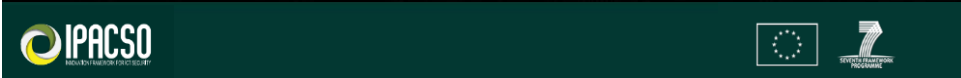
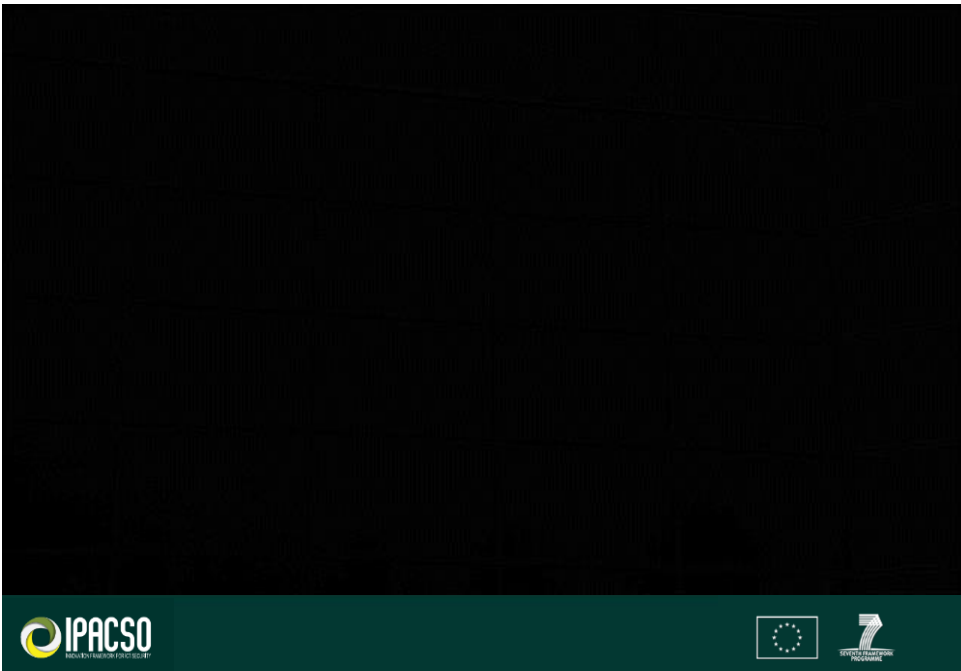
IPaCSO Core Innovation Process (*Doing Innovation*)



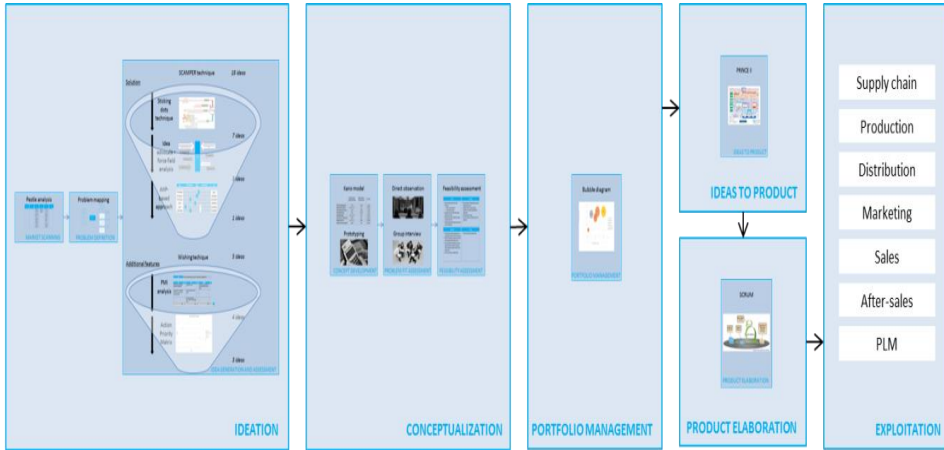
IPaCSO Supporting Innovation Themes



## The Case



# The Process



# Ideation – Market scanning

P Political	E Economic	S Sociological	T Technological	L Legal	E Environmental
		<ul style="list-style-type: none"> <li>The adoption of smartphones raised from 9% of the total world population in 2009 to 22% in 2013</li> <li>Shift towards using a mobile phone or tablet for banking (+45% of those people owning a smartphone)</li> <li>Banks are increasingly focusing on customer service and more specifically mobile services (more than 50% of US commercial banks are offering some form of mobile banking)</li> <li>Enhancement of governmental online services for which the online identity is required (eID)</li> </ul>	<ul style="list-style-type: none"> <li>Increasing security threats, which make that One-Time Passwords (OTP) might no longer be sufficient</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory use of electronic signatures</li> <li>Europe is asking for more cyber security</li> <li>Connected Reader is required for eID applications. However, Belgium is allowing use of offline eID in specific cases (strict rules)</li> <li>EU gives electronic signature the same legal value as a regular signature in ink (EIDAS)</li> <li>Make eID valid across borders (STORK)</li> <li>Adoption of EIDAS regulation (electronic identification and trust services for e-transactions)</li> </ul>	



## Ideation – Idea generation & capture 1

Assumption	180° assumptions
2-factor authentication is enabled by a combination of something 'you have' and something 'you know'	Replace one of the factors with something 'you are'
Authentication should use 2 factors	Use 1 or 3 factors
User types pin code	User says pin code or writes pin code
Pin is entered on a separate card reader	Enter pin on mobile device
Card is inserted in the reader	Card is hold against reader or mobile device
Separate card reader is used	Enter card in mobile device
The card reader and mobile device should be connected directly to each other	Use a pc or the user as intermediate



## Ideation – Idea generation & capture

### Proposed solution after the 180° Thinking session

- Authentication based on PIN code and face recognition
- Embedding reader in mobile device
- App/middleware connecting tablet to PC



## Ideation – Idea assessment

Criteria	Weight	Alternatives					
		Authentication based on PIN code and face recognition		Embedding reader in mobile device		App/middleware connecting tablet to PC	
		Score	Weighted score	Score	Weighted score	Score	Weighted score
User friendliness	4	4	16	5	20	1	4
User acceptance	3	3	9	1	3	1	3
Security in terms of authentication	4	5	20	5	20	5	20
Security in terms of signing	4	2	8	2	8	5	20
Possibility to integrate with mobile devices	5	5	25	1	5	4	20
<b>TOTAL SCORE</b>			<b>78</b>	<b>TOTAL SCORE</b>	<b>56</b>	<b>TOTAL SCORE</b>	<b>67</b>

→ None meet the expected qualities



## Ideation – Idea generation & capture 2

- Use SCAMPER technique
  - Start from existing solution that works on PC
- New idea after using SCAMPER is to replace the usb connection by one of the following:
  - Flashing patterns
  - WiFi
  - Bluetooth
  - Sound
  - Make use of the cable of charger
  - 3G/4G
  - NFC



## Ideation – Idea assessment 2

- Use of the techniques ‘Idea advocate’ and ‘Force field analysis’ allowed to eliminate the following:
  - 3G/4G
  - WiFi
  - Sound
  - Make use of the cable of charger
- Further assessment using the AHP-Based approach eliminated
  - Flashing patterns
  - NFC
- Remaining solution
  - Bluetooth



## Ideation – Idea assessment 3

Stage / characteristic	Failure	Consequence(s)	Severity of impact	Potential cause(s)	Likely of occurrence	Control(s)
Setup of the connection	The user has no mobile device that is Bluetooth enabled	The user cannot connect to the card reader	5	-	2 - The likelihood is rather low. Almost all mobile devices today are Bluetooth enabled	- Keep possibility to connect via USB-cable
Setup of the connection	The card reader loses power	The user cannot connect to the card reader	5	Earlier versions of Bluetooth are power consuming	3	- Charging through NFC technology - Use of rechargeable batteries
Setup of the connection	The user incorrectly pairs the devices (does not check the security code shown on the devices)	The assaulter can compromise the user's card reader/mobile device	5	- User is not paying enough attention - Lacking awareness - Security codes are difficult to compare (small, not visible)	2	- Increase awareness by stating alerts on the card reader - Alert the user by a sound - Display the code in different fonts
Transferring transaction data	An assaulter succeeds in intercepting the Bluetooth signal	Potential breach of privacy. However, even if the assaulter is able to intercept or even modify the message. The user still has to verify the transaction details on the card reader	3	Assaulter is within reach of the Bluetooth signal	2 - The likelihood is low. Bluetooth is protected with a strong security mechanism (WPA2)	
Transferring transaction data	Card reader is compromised	The assaulter can make the user believe he is signing the transaction he/she wants to sign while this is not the case	5	Assaulter gains access to the card reader	2 - The likelihood is low. The Bluetooth pairing process is found to be secure. Therefore the assaulter cannot compromise the card reader	-
Transferring transaction data	The user accepts the information shown on the device without checking it (account number and code)	The assaulter can successfully modify the transaction without the user noticing and correcting	5	- User is not paying enough attention - Lacking awareness - Transaction information is difficult to check (small, not visible)	2	- Increase awareness by stating alerts on the card reader - Extra control is new account number (that has not been used yet) or amount >100€





## Conceptualization- feature list

- Features that were brainstormed before:
  - Pairing by comparing codes on the two device to be connected;
  - Signing through fingerprint (one push);
  - Verifying account and amount on card reader (WYSIWYS);
  - 2-factor authentication (card and PIN code);
  - Rechargeable battery;
  - Device check when user verifies too fast.
- Potentially interesting functionalities resulting from the FMEA method:
  - Charging through NFC;
  - Possibility to connect through USB.



## Conceptualization – Concept development

Results the questionnaire using the Kano model

	Highest frequency dysfunctional answer	Highest frequency functional answer	Conclusion
<b>Pairing by comparing codes</b>	Dislike	Must be	Must be
<b>Signing through fingerprint</b>	Can live with it	Like it	Attractive
<b>Verifying account and amount</b>	Dislike	Must be	Must be
<b>2-factor authentication</b>	Dislike	Must be	Must be
<b>Rechargeable battery</b>	Can live with it	Like it	Attractive
<b>Check when user verifies too fast</b>	Neutral	Like it	Attractive
<b>Charging through NFC</b>	Can live with it	Neutral	Indifferent
<b>Possibility to connect through USB</b>	Neutral	Like it	Attractive



## Conceptualization- feature list 2

- Features retained after Keno:
  - Pairing by comparing codes on the two device to be connected;
  - Verifying account and amount on card reader (WYSIWYS);
  - 2-factor authentication (card and PIN code);
  - Signing through fingerprint (one push);
  - Device check when user verifies too fast.
- Extra feature to align with current product range:
  - Supporting multiple SC formats, including EMV, PKI or eID;
  - Supporting multiple mobile platforms, including iOS, Android, MAC OS X, and Windows;
  - Operable in bot connected (Bluetooth or USB) or unconnected modes (e.g. for one-time password);
  - Secured by means of encryption and passkey.



## Conceptualization – feasibility assessment

Market	Technology
<ul style="list-style-type: none"> <li>▪ Who is your target audience, and what characteristics do they possess?</li> <li>▪ How can you reach this target audience?</li> <li>▪ What part of this target audience is likely to buy your product?</li> <li>▪ At what price are they willing to buy this product?</li> </ul>	<ul style="list-style-type: none"> <li>▪ What technology is needed to turn this concept into a full marketable product?</li> <li>▪ What technological constraints are there?</li> <li>▪ Which technologies do not yet exist?</li> <li>▪ How easy are technologies that do exist to come by?</li> <li>▪ What is the cost of these new and existing technologies?</li> </ul>
Organization	Financial
<ul style="list-style-type: none"> <li>▪ Which organizational structure is needed to bring this concept to market?</li> <li>▪ Do we already have the right structures in place?</li> <li>▪ What is the cost of setting up these new structures?</li> <li>▪ Do we have the right corporate culture for bringing this concept to market?</li> <li>▪ Do we have the right people to transform this concept into a real product?</li> <li>▪ What is the cost of retraining existing staff, or the cost of hiring new staff with regards to this new product?</li> </ul>	<ul style="list-style-type: none"> <li>▪ NPV – Net Present Value</li> <li>▪ ROI – Return on Investment</li> <li>▪ IRR – Internal Rate of Return</li> </ul>

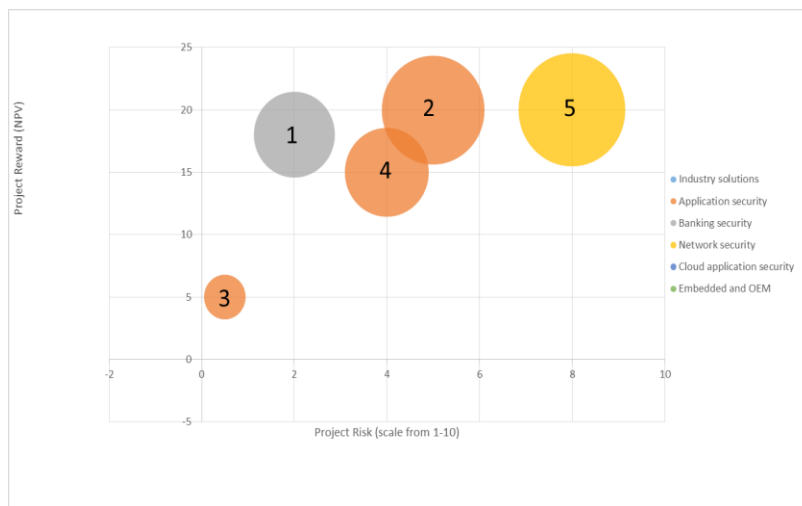


## Conceptualization – feasibility assessment

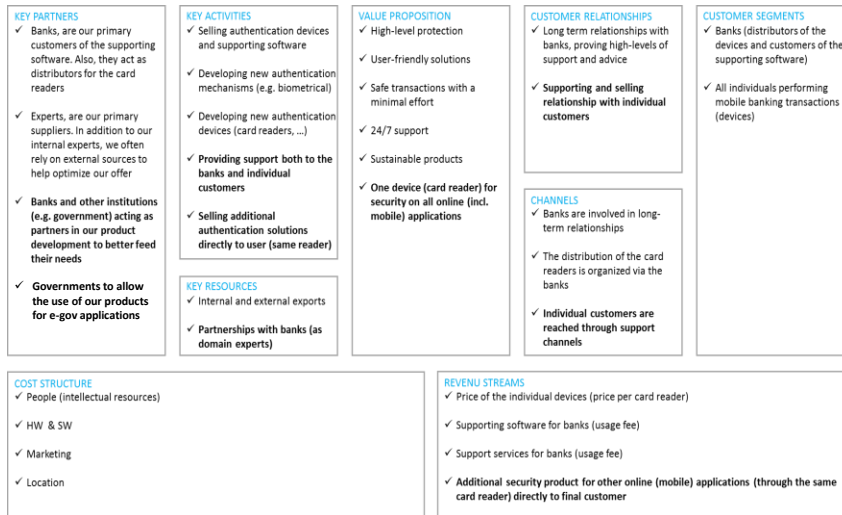
Market	Technology
<ul style="list-style-type: none"> <li>Banks who distribute the devices to their customers. Characteristics:               <ul style="list-style-type: none"> <li>Sensitive to security and ease-of-use;                   <ul style="list-style-type: none"> <li>To a lesser extent price sensitive;</li> </ul> </li> </ul> </li> <li>Target audience can be reach through existing connections (existing offer of card readers)</li> <li>All partners that currently buy our DIGIPASS 870 are probably interested in this offer as well</li> <li>Our potential customers are willing to pay the approx. the same price as for the DIGIPASS 870</li> </ul>	<ul style="list-style-type: none"> <li>Required technologies are the following: Bluetooth, fingerprint, rechargeable batteries, timer, etc.</li> <li>Technological constraints: to achieve the fingerprint authentication, the card reader should be provided with a stronger processor</li> <li>All technologies exist at this moment</li> <li>The main cost is related to the rechargeable batteries and the fingerprint scan</li> <li>...</li> </ul>
Organization	Financial
<ul style="list-style-type: none"> <li>We already produce and distribute comparable products. The same organizational structure can be used as for those products</li> <li>Within our entire organization we recognize the trend of mobile devices and transactions. Mobile is part of our culture</li> <li>As we are market leaders in user authentication, we have the right people to transform this concept into a real product. In addition, a Bluetooth security specialist is attached to provide support in this area</li> <li>The cost of this extra resource is estimated at € 8,000</li> </ul>	<ul style="list-style-type: none"> <li>The Net Present Value (NPV) was estimated to be high.</li> </ul>



## Portfolio Management



# Evaluate business model

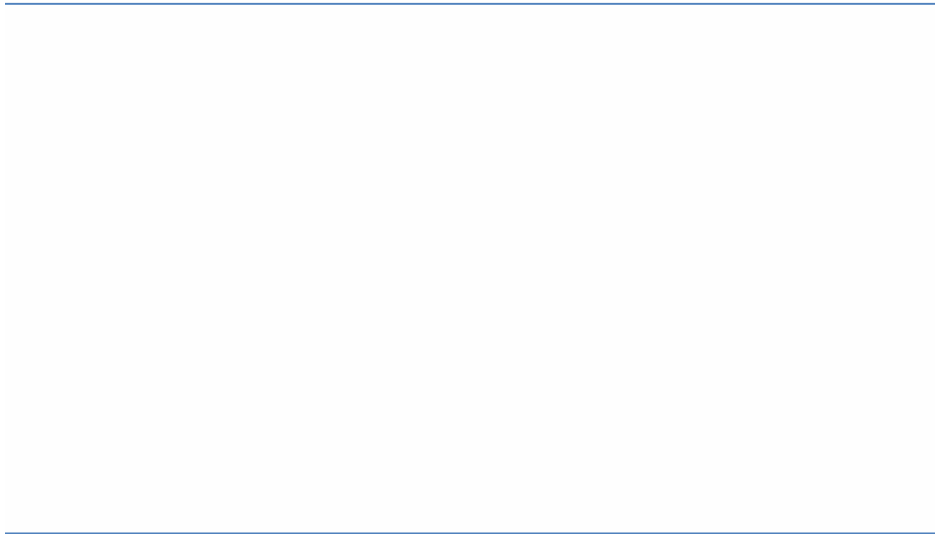


## Next steps ... (business as usual)

- Product gets a go, hand over to engineering
- Industrialization (get ready for mass production)
- Training
- Sales
- Marketing
- After-sales
- Product lifecycle Management



## Finally

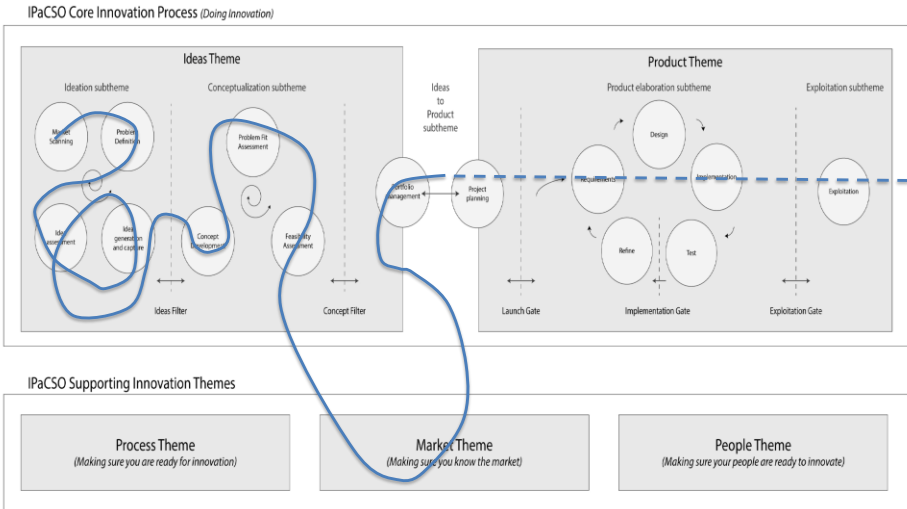


## Conclusion - Benefits for VASCO

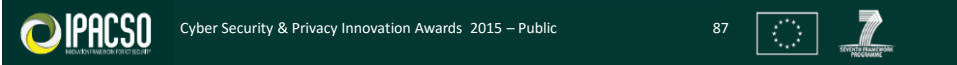
- IPACSO encouraged us to assess our innovation process which resulted in
  - Better documented process
  - Creation of an Innovation center within VASCO
- Documented techniques (the templates)
  - More efficient at collecting ideas by using a multitude of techniques
  - Better documented decisions



# IPACSO path for the 'Dp875'



## Some IPACSO Activities





## GuardSquare

The experts in mobile application protection



Our software makes mobile applications

Smaller

Faster

Secure against tampering



## Cybersecurity Analytics: Operationalizing Threat Intelligence



HiCrypt™ 2.0



10/22/2015



Peter Liebing, Head of Sales & Marketing



TANKER

Data encryption for  
SaaS & Cloud applications



Multi Dimensional Access Control

MDAC & MDAC  $\Phi$ ®

"BRIDGING THE GAP"

Elisabeth de Leeuw



n-Auth

Usable, secure and private authentication



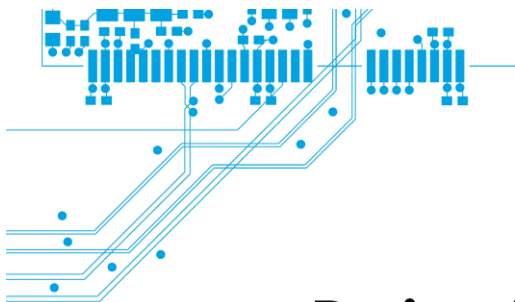


Cyber Security & Privacy Innovation Awards 2015 – Public

96



**Juan Luis Moreno,**  
Legal Manager  
[www.enigmediasecurity.com](http://www.enigmediasecurity.com)



# Project Turris

Research project helping to protect home networks

**Martin Strbačka** [martin.strbacka@nic.cz](mailto:martin.strbacka@nic.cz)

**cz.nic** | CZ DOMAIN  
REGISTRY

[www.turris.cz](http://www.turris.cz)

Decisionmaking  
while protecting  
privacy

[dan.bogdanov@cyber.ee](mailto:dan.bogdanov@cyber.ee)  
[baldur.kubo@cyber.ee](mailto:baldur.kubo@cyber.ee)  
<https://sharemind.cyber.ee>

 **CYBERNETICA**

 **sharemind**



# Access Governance for SAP environments

Multi-layer analysis

Automated role building

Reverse engineering

Comply privacy regulations



Innovation Leader  
Access Control / Governance  
for SAP environments  
July 2015



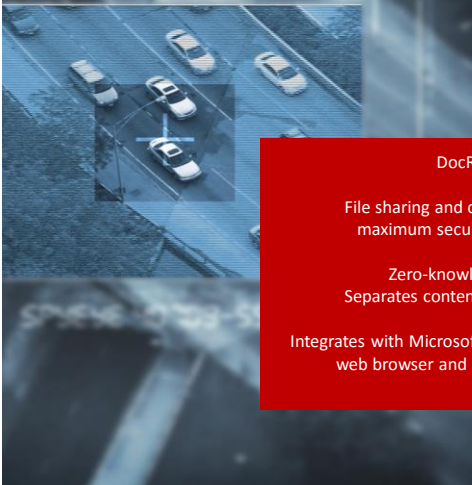
Product Leader  
Access Control / Governance  
for SAP environments  
July 2015

Johan Hermans  
CEO  
johan.hermans@csi-tools.com

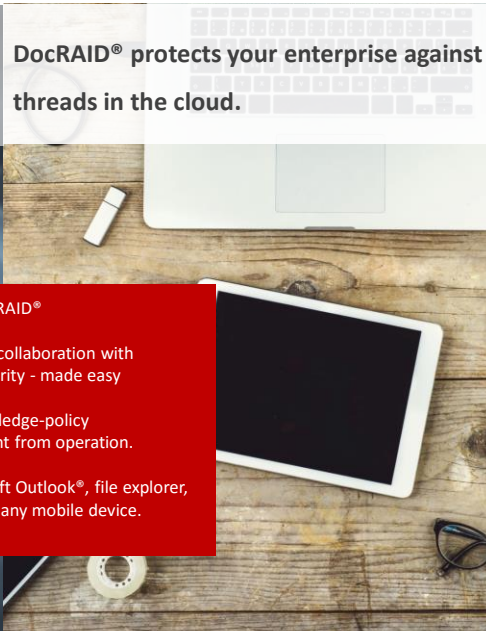
## DocRAID®

zero knowledge enterprise file sharing and email encryption

Security concerns limit the use of cloud services.



DocRAID® protects your enterprise against threads in the cloud.



DocRAID®

File sharing and collaboration with maximum security - made easy

Zero-knowledge-policy  
Separates content from operation.

Integrates with Microsoft Outlook®, file explorer, web browser and any mobile device.

# SecurIT

Marc Vanmaele  
CEO

Oct 2015



## TrustBuilder Identity Hub

Smart bridging of the identity cloud

© 2015 SecurIT

## UM Labs UC Security Platform

Peter Cox  
CEO and Inventor

October 2015



# CRYPHO

End-to-end-encrypted messaging and sharing  
for high-security environments.



Winner Startup World London '13



Winner Norwegian Young Technology Award



Winner: Tech Trailblazers Security Prize Europe

## About ThreadStone

- Founded in 2014
- Awarded with **first place** by HSD development fund
- Partnership with TNO and WorldStream
  - Quality approval current solution
  - Future innovation
- Part of the National campaign on [www.veiligzakelijkinternetten.nl](http://www.veiligzakelijkinternetten.nl) (safe internet for SME companies)
- Partner of [www.alertonline.nl](http://www.alertonline.nl) (national campaign for SME companies)
- Partner of KPN's MKB Veilig proposition

TNO innovation for life



veilig internetten  
wat je kan doen en laten

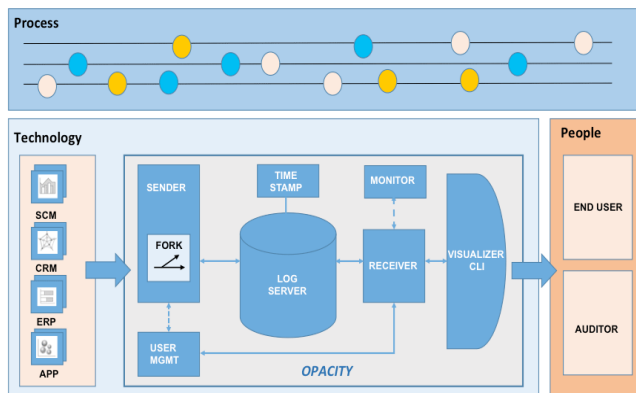
CCV Centraal Cyber Veiligheids Centrum PROFESSOR VAN ROOIJEN



mkb servicedesk TNO innovation for life



# Opacity



# ...continuumsecurity...

THE PROCESS OF SECURE SOFTWARE



**LIOPA DEVELOPS UNIQUE TECHNOLOGY THAT  
ACCURATELY IDENTIFIES A PERSON VIA ANALYSIS  
OF THEIR LIP MOVEMENTS DURING SPEECH**

The Liopa product will be sold into the mobile and security biometrics marketplace, estimated to be worth **\$25Bn by 2020**, to provide secure access to mobile and enterprise computing devices and applications (as an alternative to typing passwords, and for increased security)

Innovate UK Grant Number 102052



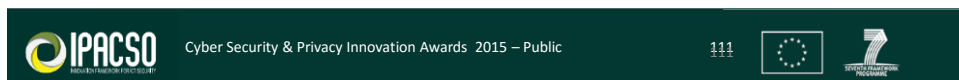
What is the alternative?

[WWW.STORRO.COM](http://WWW.STORRO.COM)



## IPACSO highlights events with stakeholders

- Innovation Awards
- Boot Camps (13)
  - Belgium : 4x cyber security, 1x privacy, tbd 1x investor
  - Netherlands: 1x cyber security, tbd 1x cyber security
  - Ireland : 3x cyber security
  - France : tbd 1x cyber security
  - UK: Oct 16<sup>th</sup>, Thames Valley Cyber Security Cluster
- Accelerator – Incubator partnerships
  - HSD : Netherlands
  - SmartFinCap – LSEC : Belgium
  - Euratechnologies : France
  - UK Cyber Security Forum, Cylon, Level39: UK
- Events, conferences, tradeshows, speaking opportunities, publications



MORE THAN 6000 visitors per month

with over 100 cyber security starters TRAINED

13 BOOTCAMPS

Over 300 European cyber security innovators registered for **Innovators Awards**

Digipass BT  
VASCO THE AUTHENTICATION COMPANY

96 TOOLS For starters




Innovations materialized using the innovation framework

## IPACSO at MobileWorld 2015

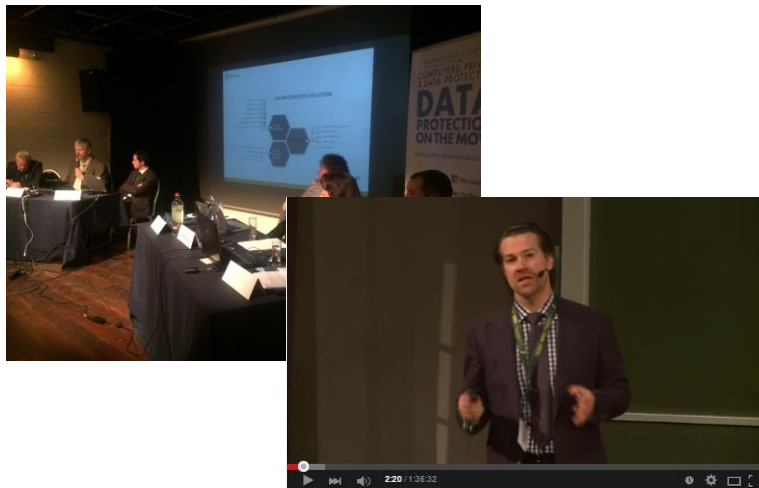





# Seminars, Conferences, Workshops



 Cyber Security & Privacy Innovation Awards 2015 – Public 114  

# Seminars, Conferences, Workshops




 Cyber Security & Privacy Innovation Awards 2015 – Public 115  

# Seminars, Conferences, Workshops




© Leaders in Security – LSEC, 2015, Private & Confidential, p 116  
Cyber Security & Privacy Innovation Awards 2015 – Public

116



116




# Promotion




INTERNATIONAL CONFERENCE • 21-23 JANUARY 2015 • BRUSSELS, BELGIUM  
**CPDP COMPUTERS, PRIVACY & DATA PROTECTION**  
**2015 DATA PROTECTION ON THE MOVE**

IPACSO Cyber Security & Privacy Innovation Awards 2015 – Public

117



117



# Seminars, Conferences, Workshops



© Leaders in Security – LSEC, 2015, Private & Confidential, p 118

Cyber Security & Privacy Innovation Awards 2015 – Public



118



# CSP Forum 2015

CYBERSECURITY & PRIVACY INNOVATION FORUM 2015

Day 1 - Tuesday 28th April.



08.00 - 09.00	<b>REGISTRATION.</b>	14.15 - 15.00	<b>Room AB:Track 5 "NCP Support in H2020"</b> Chair: Alessandro Barbagli, Head of ICT Committees & National Contact Points sector	<b>Room CD:Track 6 "Security Visualisation Make and Do"</b> Chair: Mrs Margaret Ford, Consult Hyperion	<b>Room EF:Track 7 "Incentivising Innovation in Cybersecurity &amp; Privacy Part 2"</b> Chair: Zeta Dooley, Waterloo Institute of Technology
09.00 - 10.00	<b>Room AB: Official Opening</b> <b>Keynote:</b> Zoran Stančič, Dep <b>2nd Keynote:</b> Giovanni But	15.00 - 15.30	<b>Panel:</b> "The Network of ICT National Contact Points" "Lesson learned from H2020 ICT Security Calls" "The H2020 SME survivor kit" "Sedici Innovations - H2020 SME Experience"	<b>Lizzie Coles-Kemp</b> , Royal Holloway University of London <b>Claude Heath</b> , Royal Holloway University of London <b>Jeroen Barends</b> , LUST	<b>"Economic Incentives for Cyber-security Innovation"</b> Dr Nicola Antonicelli, DMIW <b>"Cybersecurity commercialisation: one to large perspective"</b> Mark Carolan, ESPION
10.00 - 10.30	<b>Coffee Break/Networking</b>	15.30 - 16.15	<b>Coffee Break/Networking &amp; Exhibition Space</b>	<b>Room CD:Track 9 "Ubiquitous security for mobile users: SDN and NFV to the rescue"</b> Chair: Antonio Liroy, Politecnico di Torino	<b>Room EF:Track 10 "Security Awareness and Risk Assessment"</b> Chair: Luca Compagna, SAP
10.30 - 12.30	<b>Room AB:Track 1 "Introdu "Overview" Martin Muehleck</b> H2020 info topic 1 H2020 info topic 2 H2020 info topic 3 H2020 info topic 4 "The JRC approach to the ICT"	16.15 - 17.30	<b>Room AB:Track 8 "H2020 Supporting SMEs"</b> Chair: Viorica Peca, Head of Innovation Unit <b>"Introduction and H2020 SME Instruments"</b> Viorica Peca, Head of Innovation Unit <b>"The H2020 SME survivor kit"</b> "Sedici Innovations - H2020 SME Experience"	<b>"Security for all: network-based protection for personal devices"</b> Antonio Liroy, Politecnico di Torino <b>"Bootstrapping (software) infrastructure trust: from SDN towards NFV"</b> Lučović Jacquin, HP Labs <b>"A NFV-based architecture for security services"</b> Diego Lopez, Telefonica <b>"Specification and Enforcement of Privacy Policies"</b> Michela D'Ermo, EnCloud project, HP, UK <b>Claudio Carini</b> , Cooc Cloud project, HP, Italy	<b>"Business Situational Security Awareness"</b> Roland Rilke, SIF Fraunhofer <b>"Medusa - A Supply Chain Risk Assessment Methodology"</b> Assistant Professor Panagiotis Kotzianikolaou, University of Piraeus <b>"What's so Unique about Cybersecurity?"</b> Kerry Doyle, WIT-TSSG <b>Room EF:Track 13 "Trust, Security &amp; Privacy"</b> Chair: Fabio Massimo LUNINI
12.30 - 13.30	<b>Lunch Break/Networking</b>	18.00 - 20.00	<b>Room AB:Track 11 "Cybersecurity Standards"</b> Chair: Ulrich Seifried, LSEC <b>"ETS's role in Cyber Security"</b> Scott W Cadzow, Cadzow Communications Consulting Ltd <b>"ISO 27032 - 27001"</b> "An Innovative ETSI standard covering all security detection aspects (BSG ISG) Gerard Gaetan, D'CC"	<b>Room CD:Track 12 "Implementing Privacy Policies In the cloud"</b> Chair: Nick Wainwright HP Labs <b>"EU DP legal framework review and its impact on cloud architecture"</b> "Demotesthera Baromou, Head of Information Security & Data Protection Unit, ENSA <b>"Specification and Enforcement of Privacy Policies"</b> Michela D'Ermo, EnCloud project, HP, UK <b>Claudio Carini</b> , Cooc Cloud project, HP, Italy	<b>"ETSP on the Internet Privacy Engineering Network (IPEW)"</b> Massimo Atoneri, EDP5 <b>"Evidence-based Trustworthiness of Internet-based Services through Controlled Software Development"</b> Sachar Pappas, InCoStoLab Mannheim <b>"A Reputation Based Trust Management Model for Cyber Security Services"</b> "Hakan Kilinc, NETAS <b>"Security and Privacy in vehicular communications with IEEE 802.11p"</b> "Sam M. Rubin, University of Murcia
13.30 - 14.15	<b>Room AB:Track 2 "From PII to Privacy-By-Operation"</b> Chair: Antonio Kung'u, T1lab "The path towards privacy-by-design" Nicolas Notariis, ATOS "Creation of a privacy pattern" Frank Kargl, ULLM "Creation of an educational material" Claudia Rada, American UOW	<b>Evening Networking Event 18.00</b> (Exhibition Space at MCE Venue) <b>Keynote Speaker:</b> Paul Timmer, Director of the Sustainable & Secure Society Directorate, European Commission, DIG CONNECT IPACSO Innovation Award - Discovery of the European Cybersecurity Entrepreneurial Path (Intrinsik-ID, Sedici, KLAB)			



Cyber Security & Privacy Innovation Awards 2015 – Public

119



# IPACSO Exploitation



**CLUSTER 3**  
**EURATECHNOLOGIES**

**LANÇE LE 1<sup>ER</sup> PROGRAMME D'INCUBATION & D'ACCÉLÉRATION DEDIE A LA CYBERSECURITE & CONFIANCE NUMERIQUE**

**QUI EST EURATECH ?**  
Copropriétaire du Forum International de la Cybersecrité depuis 2012 et animateur de l'un des plus grands clusters technologiques en France, les Euratech (Euratechnologies, Institut pour l'Etat Numérique de la Libre et leur expertise unique en services des entreprises.

**POURQUOI POSTULER ?**  
Accélérer la création et le développement de la startup grâce à un programme d'accompagnement dédié et unique. Le programme dédié s'adresse à toutes les startups d'Euratechnologies soutenues par des partenaires métiers qualifiés.

**LE PROGRAMME**

- Des sessions thématiques interactives
- Des ateliers d'accompagnement
- Des mentors dédiés
- Des appels à candidatures

Un accompagnement pour accélérer votre implantation sur le marché de la cybersecrité et de la confiance numérique.

HOSTING NETWORKING FUNDING COACHING

Un accès privilégié à un réseau d'experts, de mentors et à un vivier de clients.

ADMINISTRATIONS PUBLIQUES

SANTÉ DÉFENSE FRANCE  
RETAIL TRANSPORTS SMART CULTURE

Postulez sur le site [www.euratechnologies.com](http://www.euratechnologies.com)



**UN PROGRAMME EUROPÉEN**  
**IPACSO** Accélérer votre développement en Europe grâce à un réseau d'experts et de mentors qualifiés, un accompagnement personnalisé et un accès privilégié.

**DES PARTENAIRES METIERS ET TECHNOLOGIQUES**  
IBM, EXEL, INFOS, TELECOM, BVA

**LILLE, CAPITALE DE LA CYBERSECURITE**

UN RESEAU DE PROFESSIONNELS DE LA CYBERSECURITE	6500 SALAIRES
UN ECOSYSTEME INNOVANT	110 ENTREPRISES
32 FORMATIONS	10 CENTRES DE RECHERCHE

Créé en 2005, l'Euratechnologies centre d'Innovation Numérique (EIN) est le premier incubateur européen dédié à la cybersecrité et à la confiance numérique en Europe et le 1<sup>er</sup> en France. En six années d'existence, l'Euratechnologies a réussi à s'imposer comme le hub de la confiance numérique française. L'Euratechnologies a été nommé meilleur incubateur de 2014 par le magazine Entrepreneur et a été nommé meilleur incubateur européen de 2014 par le magazine Entrepreneur.


Un réseau d'experts et de mentors dédiés à la cybersecrité et à la confiance numérique

- 100 experts européens
- 100 mentors internationaux
- 100 appels à candidatures
- 100 startups financées

Objectif pour 2015



- 100 startups
- 100 mentors
- 100 appels à candidatures

www.euratechnologies.com




Cyber Security & Privacy Innovation Awards 2015 – Public

120





## IPACSO Panel



Cyber Security & Privacy Innovation Awards 2015 – Public

121

# IPACSO Methodological Approach

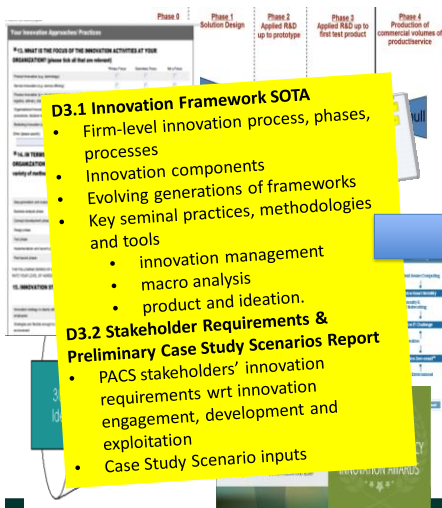


Cyber Security & Privacy Innovation Awards 2015 – Public

122



## Activities turning into Deliverables



### Transformed/ Utilised for

- NIS WG 3 Deliverable
- Presentations/  
Publications
- Framework Themes
  - templates
- Bootcamp material/delivery






Cyber Security & Privacy Innovation Awards 2015 – Public

123

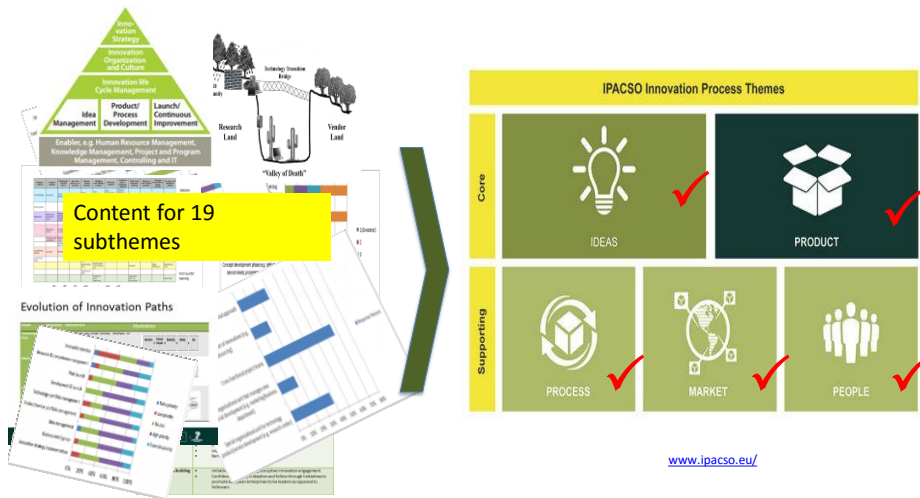


# Relevance to Stakeholders

	Start-Up	Innovator/ Entrepreneur	Researcher	Policy
<b>Innovation SOTA</b>	Knowledge repository	Benchmarking	Knowledge repository	Knowledge
<b>Innovation Requirements</b>	Knowledge	Benchmarking	Knowledge	Data
<b>Publications</b>	Knowledge, Insights, Recommendations	Knowledge, Insights, Recommendations	Knowledge, Insights, Recommendations	Practice/knowledge
<b>Innovation Exemplars</b>	Best practice	Best practice	Best practice	Best practice
<b>Framework Themes &amp; Templates</b>	Guidance and methodologies	Guidance and methodologies	Guidance and methodologies	Guidance and methodologies
Ideas	Generating, screening, feasibility			✓
Product	Elaboration and exploitation			
Market	Macro and Micro analyses techniques			
Process	Considerations for (re)designing, benchmarking, improving			
People	Selecting, managing, motivating, rewarding, partnering			







 Cyber Security & Privacy Innovation Awards 2015 – Public
 
 124
 


# The IPACSO Framework Themes






**Content for 19 subthemes**

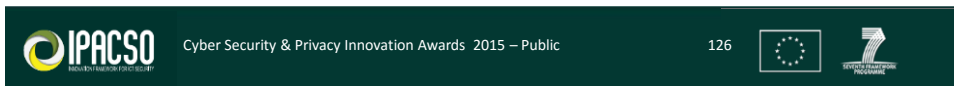
**IPACSO Innovation Process Themes**

<b>Core</b>	 IDEAS ✓	 PRODUCT ✓	
<b>Supporting</b>	 PROCESS ✓	 MARKET ✓	 PEOPLE ✓

[www.ipacso.eu/](http://www.ipacso.eu/)


 Cyber Security & Privacy Innovation Awards 2015 – Public
 
 125
 


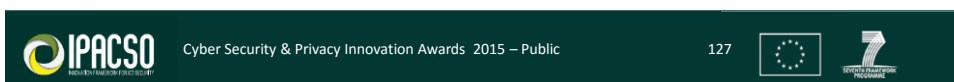
# IPACSO Framework

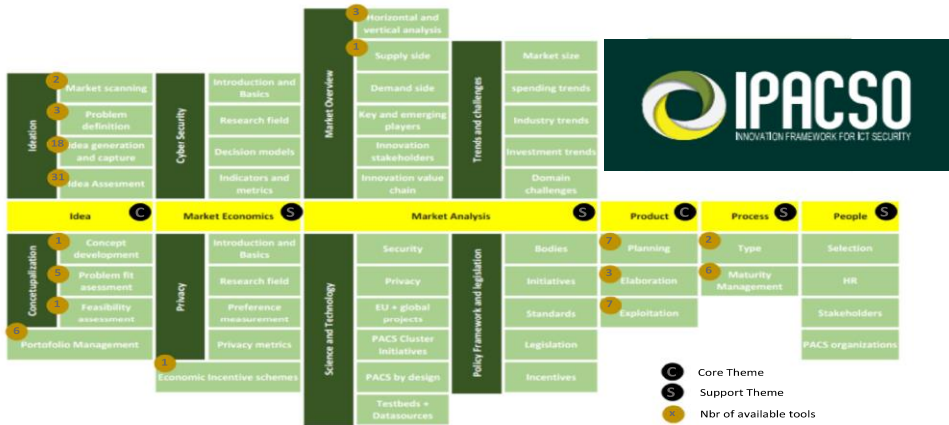


## Framework Templates

<http://ipacso.eu/innovation-framework-under-development/innovation-framework-templates.html>

Ideas	Product	Process	Market	People
Market Scanning	Concept Development	Project Planning	Macro/micro analysis	HR for Innovation (selection, managing, rewarding)
Problem Definition	Problem Fit Assessment	Development processes	Economic assessment/ impact	
Idea Generation & Capture	Feasibility Assessment	Maturity assessment		
Idea Assessment	Portfolio Management			





## Irish bootcamps roadtrip in June 2015

- Waterford
- Dublin
- Belfast



# IPACSO NIS Contribution

- SRA (NIS WG3) Secure ICT Research and Innovation emerging research priorities:
  - Fostering assurance
  - Focussing on data
  - Enabling secure execution
  - Preserving privacy
  - Increasing trust
  - Managing cyber risks
  - Protecting ICT infrastructures
  - Achieving user-centricity



Cyber Security & Privacy Innovation Awards 2015 – Public

130



## IPACSO Community *highlights*

- IPACSO Award winners – cybersecurity /privacy products & services
- Linking with **other EU funded research** – building EU market capacity
- Developed comprehensive IPACSO innovation framework
  - Knowledge base, case studies, stakeholder engagement, policy recommendations
- Toolkit of templates, examples and mechanisms to drive ideas into cybersecurity marketplace
- Hosted bootcamps for innovators across Europe
- Published papers
- NIS platform and EU Strategic Research Agenda contribution
- Holistic view of cybersecurity

NIS Platform WG3 meeting  
EU Industry Innovation and Competitiveness  
March 2nd, 2015  
European Commission, Brussels



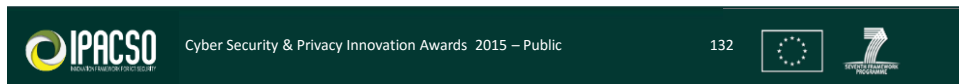
Cyber Security & Privacy Innovation Awards 2015 – Public

131

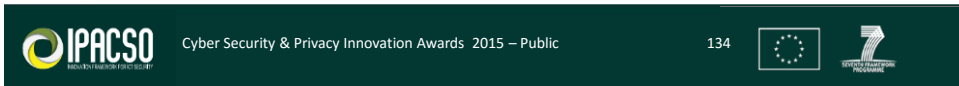


## Available resources

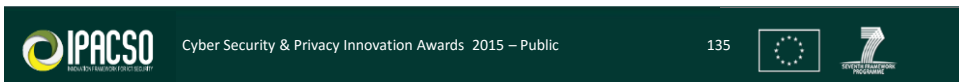
- IPACSO deliverables, white papers, reference documents, templates and examples
  - NIS WG3
    - Secure ICT Landscape
    - Business cases and innovation paths
    - Snapshot of Education & Training landscape for workforce development
- SRA NIS WG3



The image features a central graphic of a globe with a network of glowing lines representing connections. Overlaid on this is the text 'IPACSO' in large white letters, with 'CYBER SECURITY' in smaller white letters below it. At the bottom of the graphic, there is a dark green banner with the text 'EC - DG CONNECT - Head Unit Trust &amp; Security' and 'Mr. Jakub Boratynsky' in white. The bottom of the slide features a dark green footer with the IPACSO logo, the text 'Cyber Security &amp; Privacy Innovation Awards 2015 - Public', the number '133', the European Union flag, and the 7th Framework Programme logo.



## Innovative Cyber Security Product



# GuardSquare

The experts in mobile application protection



Our software makes mobile applications

Smaller

Faster

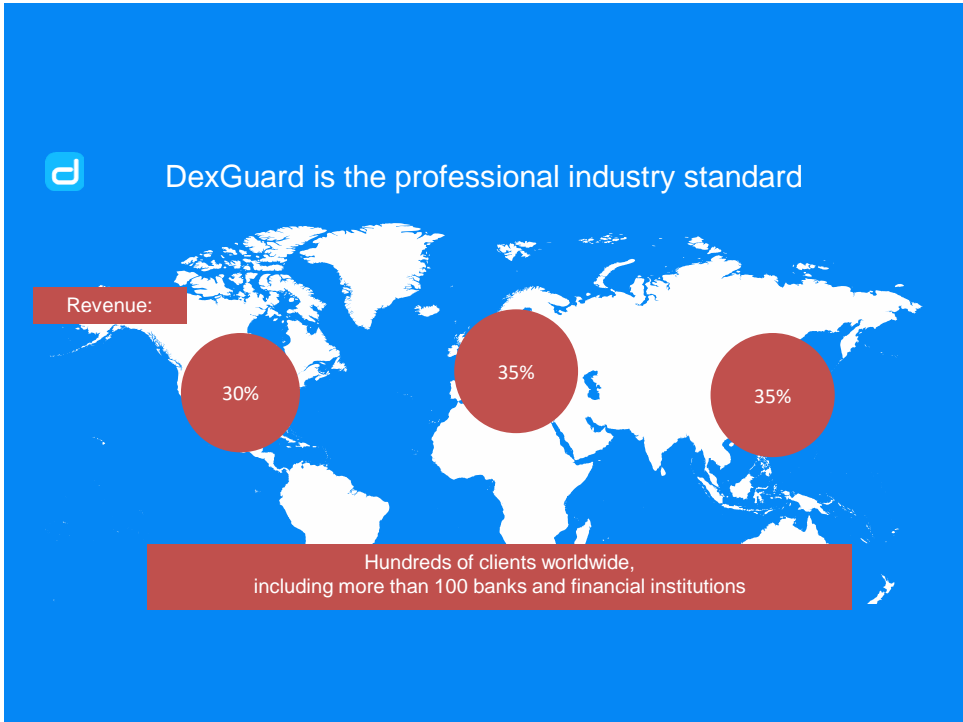
Secure against tampering






## ProGuard is the open source industry standard

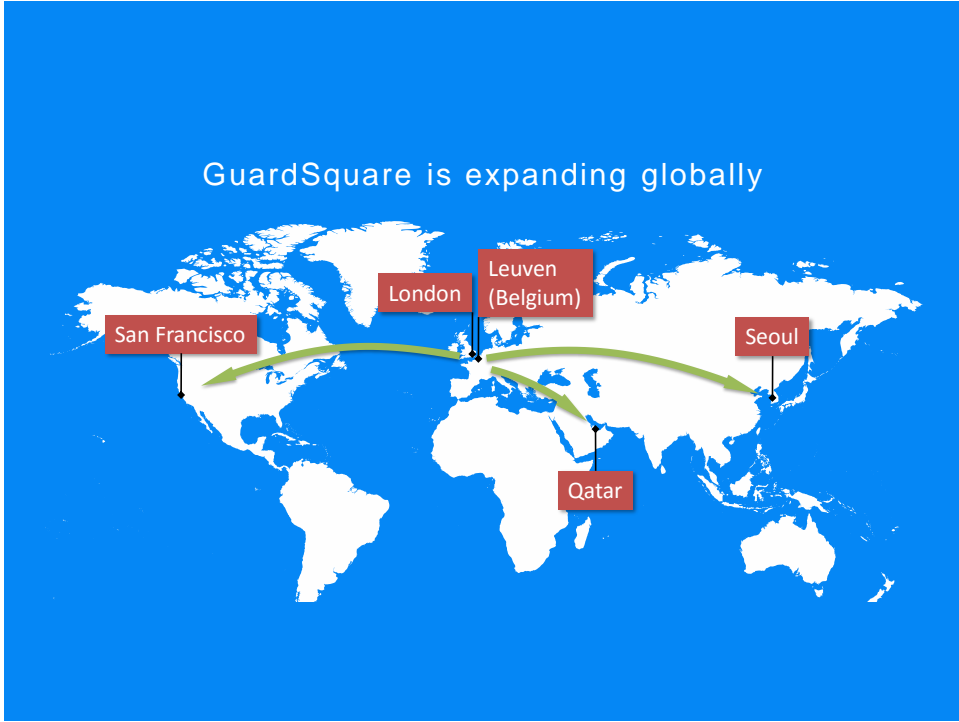


Thousands of companies, more than 1 million developers, more than 1 billion devices



### DexGuard makes apps smaller, faster, and secure

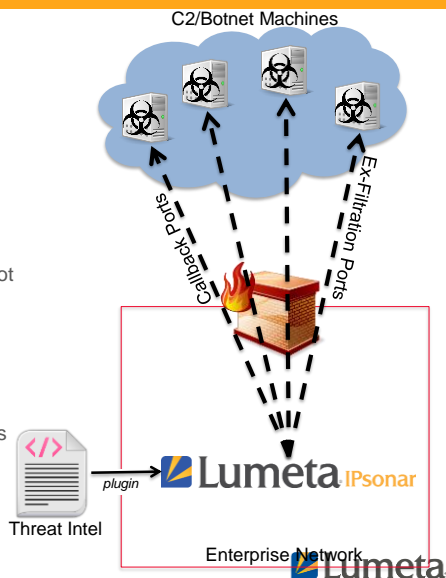
- Smaller**  
  
by shrinking the code and resources
- Faster**  
  
by optimizing the code and resources
- Secure**  
  
by obfuscating and encrypting the code and resources



Cybersecurity Analytics:  
Operationalizing Threat Intelligence

## Validate No Access to Known Malware C2 Servers

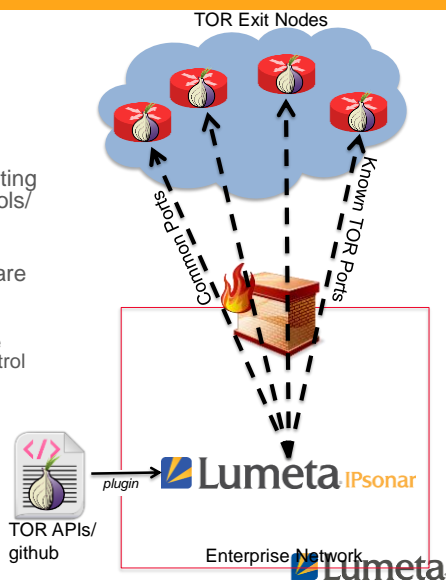
- ▣ Determine whether or not active security controls prevent call back to known botnet/command and control networks and servers
- ▣ Findings
  - Firewall rules are not effective at limiting outbound sessions over risky protocols
  - Firewalls/NGFW/IPS/DLP solutions are not effective at limiting or blocking access to known bad networks or servers
    - Also validates that threat intelligence used in test is available to these control points
  - Security architecture is not uniform across the enterprise
    - Multiple egress points where one or more did not let traffic out



## Validate No Access to Known TOR Exit Nodes

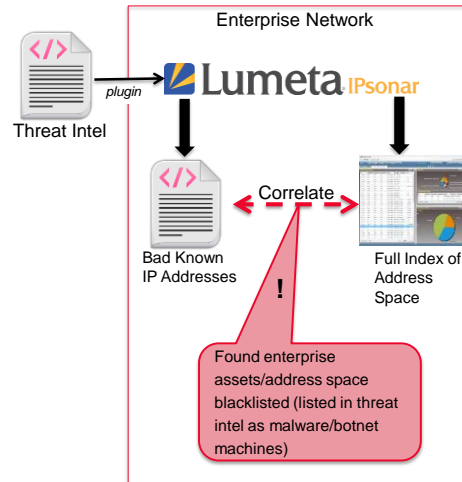
TOR – The Onion Router/Dark Web Infrastructure

- ▣ Determine whether or not active security controls prevent call back to TOR exit nodes
- ▣ Findings
  - Firewall rules are not effective at limiting outbound sessions over risky protocols/ports
  - Firewalls/NGFW/IPS/DLP solutions are not effective at limiting or blocking access to TOR
    - Also validates that threat intelligence used in test is available to these control points
  - Security architecture is not uniform across the enterprise
    - Multiple egress points where one or more did not let traffic out



## Zombie Hunting

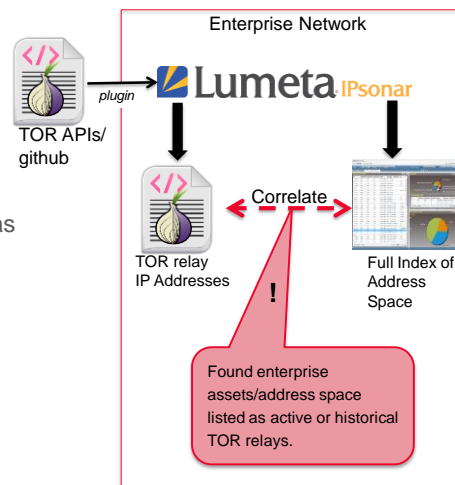
- Determine whether or not any trusted/enterprise assets are malware infrastructure or part of blacklists/dropnets/Shadowserver/attacker lists
  
- Findings
  - Identified machines have active malware on them
  
  - The reputation service (if subscribed) is not...
    - Functioning as expected
    - Implemented effectively



 Lumeta

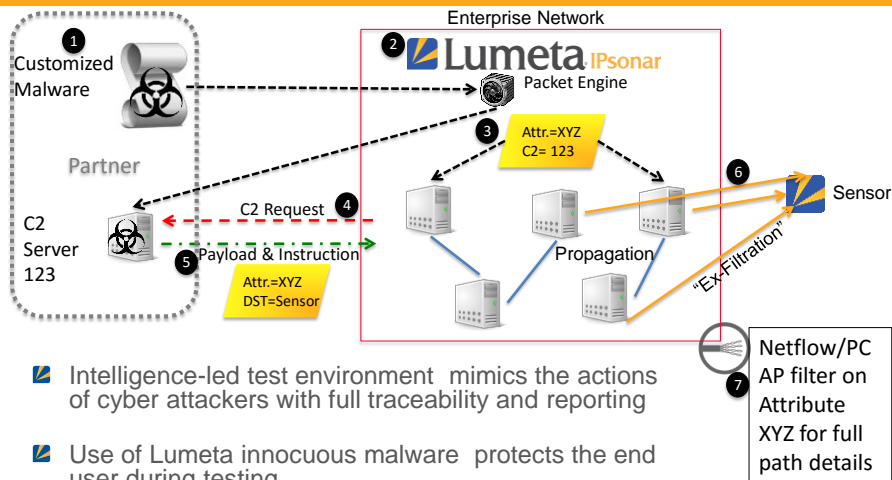
## Internal TOR Relays/Bridges

- Determine whether or not any trusted/enterprise assets are/were acting as TOR relays/bridges
  
- Findings
  - Identified machines are acting as TOR nodes, potentially for nefarious purposes
    - Botnet/zombie
    - Malware
  
  - Endpoint controls and network-based security solutions are misconfigured or not operating effectively



 Lumeta

# Network Attack Emulation Solution



- Intelligence-led test environment mimics the actions of cyber attackers with full traceability and reporting
- Use of Lumeta innocuous malware protects the end user during testing
- We are partnering with the Security testing teams

Netflow/PC AP filter on Attribute XYZ for full path details



# sentryo

Cyber Security for the Industrial Internet

Situational Awareness + Anomaly Detection + Security Management

Sentryo HQ | 66 Bd Niels Bohr CS 52132 69603 Lyon-Villeurbanne - France  
+33 970 469 694 | [contact@sentryo.net](mailto:contact@sentryo.net) | [www.sentryo.net](http://www.sentryo.net)

**Laurent Hausermann - Founder**

[laurent.hausermann@sentryo.net](mailto:laurent.hausermann@sentryo.net)  
+33 (0)6 17 10 94 33

**Thierry Rouquet - Founder**

[thierry.rouquet@sentryo.net](mailto:thierry.rouquet@sentryo.net)  
+33 (0)6 32 67 48 35

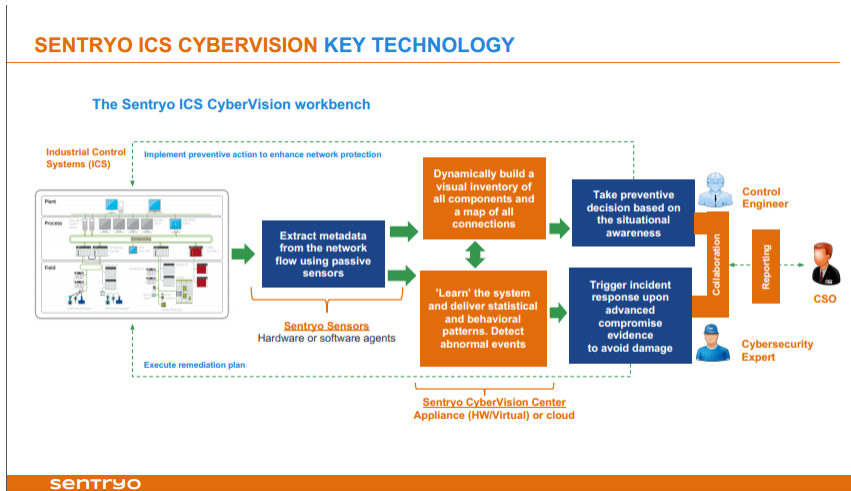


Cyber Security & Privacy Innovation Awards 2015 – Public

147



## SENTRYO ICS CYBERVISION KEY TECHNOLOGY



Cyber Security & Privacy Innovation Awards 2015 – Public

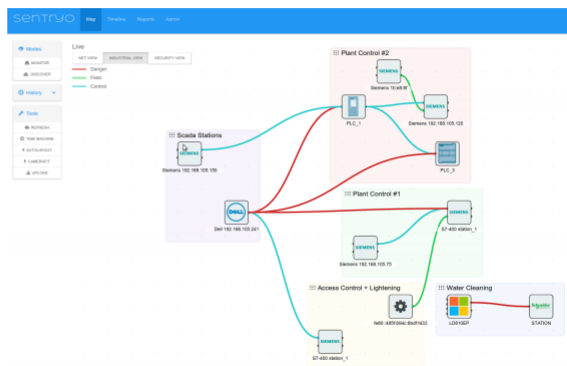
148



## SENTRYO ICS CYBERVISION SITUATIONAL AWARENESS

To secure your ICS you need an inventory and a map

- **complete** with all the running assets (PLC, Switches, IO Module),
- **intuitive** with an easy to use UI,
- **interactive** to dive into your ICS network and annotate it,
- **automatic** that will learn everything from the network,



sentryo

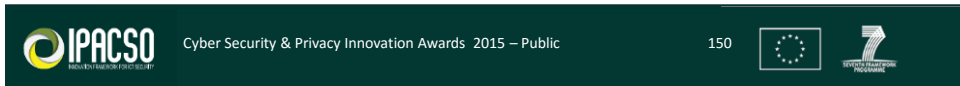


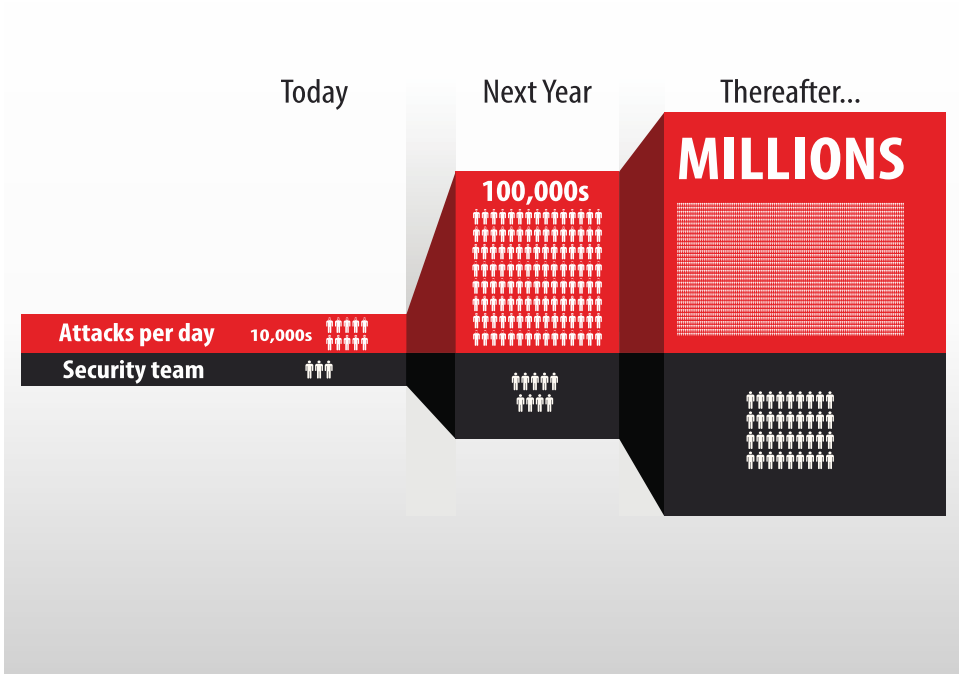
Cyber Security & Privacy Innovation Awards 2015 – Public

149



# Innovative Cyber Security Product





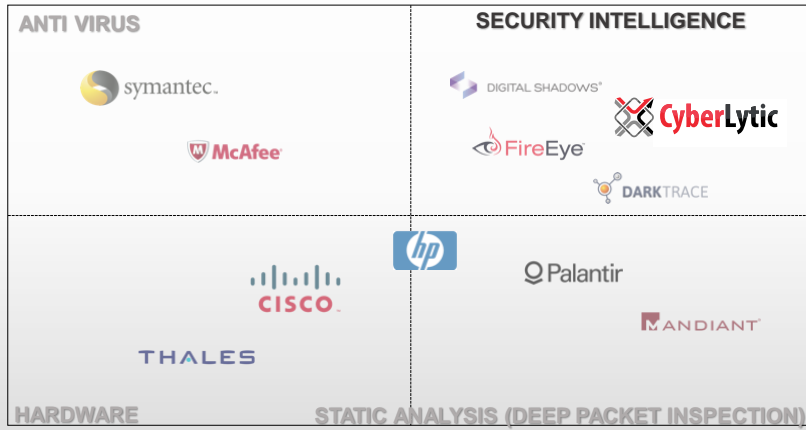
 **Cyber Threat Profiler**



**Triage Cyber Attack**

- Sophistication**
- Capability**
- Effectiveness**

### Cyber Security £47Bn Global Market



Founded October 2013

Experienced Team

Grant funded development

CSIT, Queen's University


Patent Pending

Product Trials underway


Recruiting NOW

Clear Technology Roadmap


**Cyber Threat Profiler**



**Automated Cyber Defence**



**Cyber Risk Trends & Prediction**



Threat Module (SQUAD)

Module (YSS)

Module (SRF)

Module (SRF)

Module (SRF)

Module (SRF)

Module (SRF)

Enable security teams to be more efficient

Triage security alerts;  
Reduce response times to seconds

**Complete EIS round**

**Build research & development  
team**

**Conclude trials and product  
sales**

**Develop strategic partnerships**

**Innovative Cyber Security Service**



## The main dilemma of SME Cybercrime:



- Average time before detection after breach : 205 days
- % of hacks that would have been easy to prevent : 85%
- % of breached sites, a patch was already more than 1 year (!) available : 71%

### WHY???

The 'average' SME's...

- IT is outsourced
- don't know technically about cybercrime
- think their IT supplier acts and take care on cybercrime

**HE DOES NOT ACT!!**

The 'average' IT supplier...

- do know about cybercrime
- do know how to technically solve problems

**HE DOES NOT ACT** because he can't invoice the hours needed to solve overdue maintenance to his customers!!





## About ThreadStone

- Founded in 2014
- Awarded with **first place** by HSD development fund
- Partnership with TNO and WorldStream
  - Quality approval current solution
  - Future innovation
- Part of the National campaign on [www.veiligzakelijkinternetten.nl](http://www.veiligzakelijkinternetten.nl) (safe internet for SME companies)
- Partner of [www.alertonline.nl](http://www.alertonline.nl) (national campaign for SME companies)
- Partner of KPN's MKB Veilig proposition



## Innovative Cyber Security Service





We help achieve **Applied Intelligence**

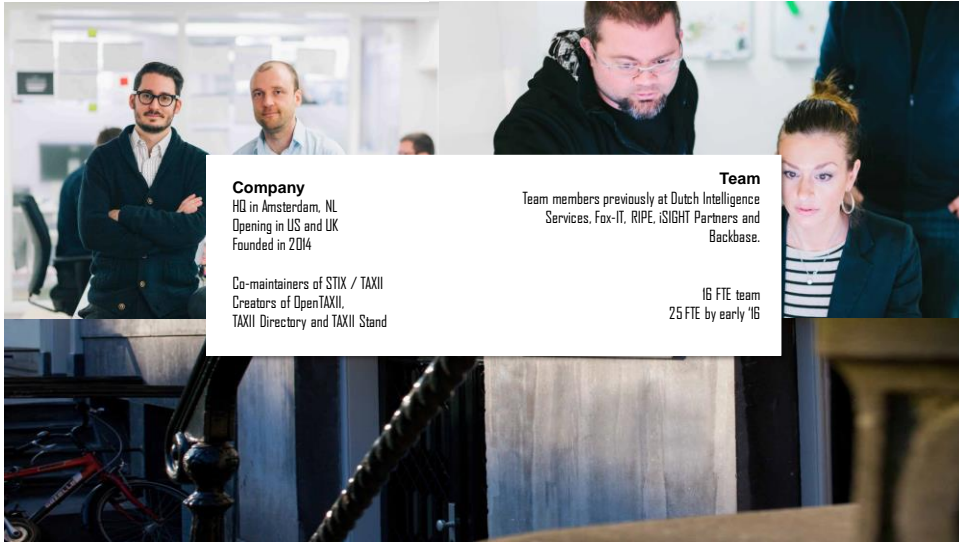
*Operationalize security Information Exchange*

*Empower Analyst Workflow and Collaborative Analysis*

*Facilitate technical Integration*

*Manage Intelligence Content procurement*

ISAC ISAO CERT SOC  
FUSION CENTER INTEL PRACTICE



**Company**

HQ in Amsterdam, NL  
Opening in US and UK  
Founded in 2014

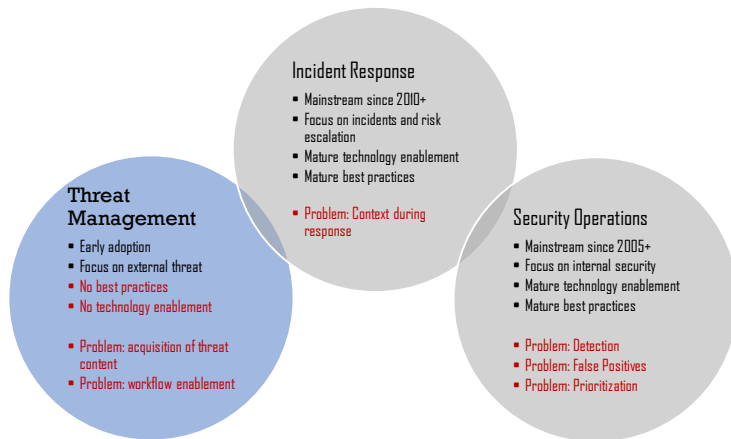
Co-maintainers of STIX / TAXII  
Creators of OpenTAXII,  
TAXII Directory and TAXII Stand

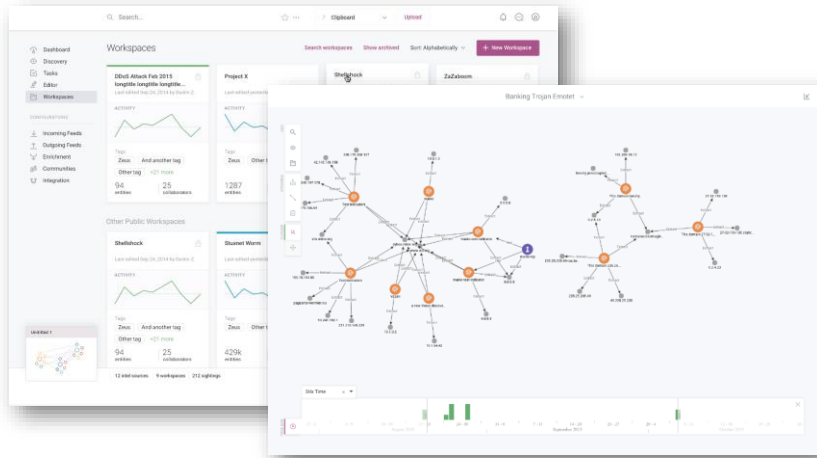
**Team**

Team members previously at Dutch Intelligence  
Services, Fox-IT, RIPE, iSIGHT Partners and  
Backbase.

16 FTE team  
25 FTE by early '16

Security practices in the large enterprise





# Innovative Cyber Security Company



**SPEAR-PHISHING PROTECTION SERVICE**

**VOTIRO**  
SECURED.

**Spear Phishing**

**SECURE YOUR DATA WITH  
VOTIRO SPEAR-PHISHING PROTECTION**

170

## Innovative Cyber Security Company

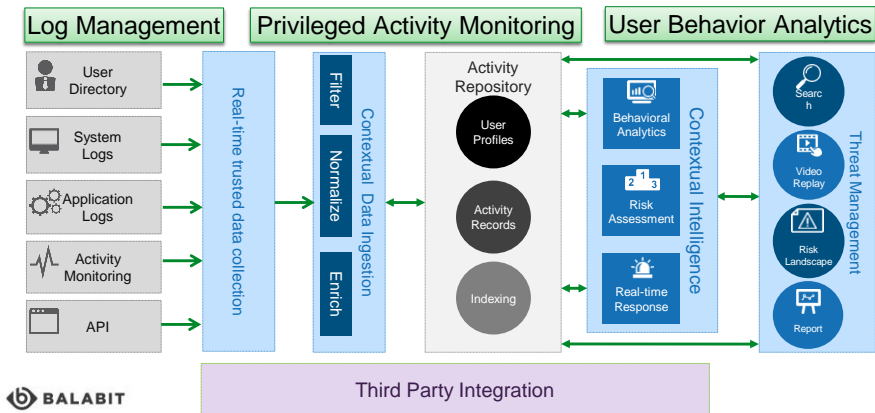
**IPACSO AWARDS**  
INNOVATION FRAMEWORK FOR ICT SECURITY

**WINNER OF THE 2015 EDITION**

171

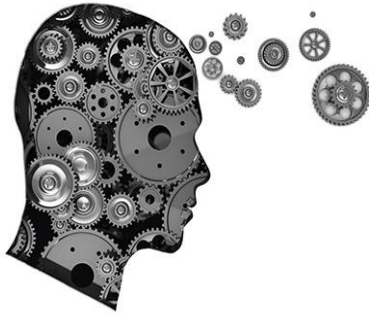


### The Contextual Security Intelligence Platform POWERED BY BALABIT



# Blindspotter for User Behavior Analytics

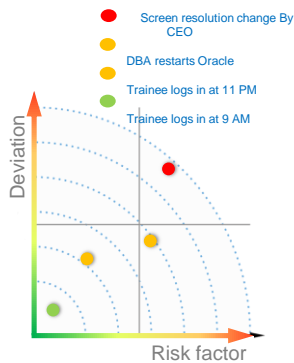
algorithms on top of all collected data



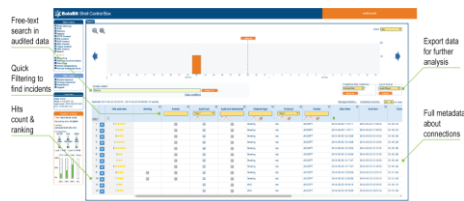
- Syslog-ng and SCB provide **visibility**, Blindspotter offers **understanding**
- Gather users' **digital footprints**
- Build a baseline for „normal” behavior
- Identify **unusual activities** in real-time
- Act immediately to **prevent data breaches**
- It is based on **machine learning and monitoring**



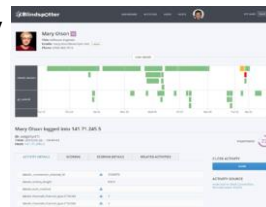
## Risk-score activities



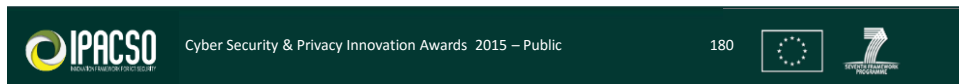
## Drill into threats



## Video replay



# Innovative Privacy Company



**LIOPA DEVELOPS UNIQUE TECHNOLOGY THAT ACCURATELY IDENTIFIES A PERSON VIA ANALYSIS OF THEIR LIP MOVEMENTS DURING SPEECH**

The Liopa product will be sold into the mobile and security biometrics marketplace, estimated to be worth **\$25Bn by 2020**, to provide secure access to mobile and enterprise computing devices and applications (as an alternative to typing passwords, and for increased security)

Innovate UK Grant Number 102052

## Who Are Liopa?



- New spin-out from Queen's University Belfast and CSIT (Centre for Secure IT)
- Leveraging 8 years of research into
  - Speech and Image processing
  - Fusion of speech and lip movements for robust speech&speaker recognition
- Management Team
  - Proven track record in founding and developing hi-tech s/ware start-ups
  - Expertise in image processing, facial, phoneme and viseme analytics
  - Expertise in software architectural design techniques and development methodologies for highly resilient and scalable systems

182

## The Solution



### Analyses Speaker Lip Movement

- Verifies speaker identity
- Verifies spoken phrase (**to prevent spoofing/replay attacks**)

### Process

- User enrolls by speaking and Liopa 'learns' their lip movement profile
- User subsequently authenticate by speaking random challenge phrase
- Algorithmic comparison performed to validate user identity

### Implementation

- Will work on any device with a standard camera (**no additional h/w needed**)
- Will run in the cloud, on-premis or on-device
- SDK for embedding verification into 3<sup>rd</sup> party application, device or service
- Deployed as sole authentication technique or in "multi-modal" solution

### Timeline

- Downloadable beta App & SDK November 2015
- 1<sup>st</sup> Commercial release Q2 2016

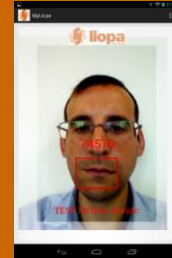
183

## Use Cases



### User Authentication

- Mobile Device Access
- Mobile App Access (e.g. banking app)
- Remote or personal device (BYOD) access to Enterprise assets
- Online retail transactions (on behalf of payment providers)
- Online access to eGov/Healthcare services
- Physical Access Control, Time & Attendance monitoring



### Visual Phrase recognition

- Supporting technology for speech recognition platforms especially in mobile or noisy office environment
  - Voice-based intelligent assistants – cortana, siri
  - Dictation systems

184

## Competition



Viseme based technique is unique to Liopa and offers distinct advantages over popular biometric authentication techniques

	Fingerprint	Voice	Iris	Behavioural	Face	Lip
Ease of Use	●●	●	●	●	●	●
Accuracy	●	●	●●	●	●	●
“Liveness” Detection	●	●	●	●	●	●●
Additional Cost (H/W)	●	●●	●●	●●	●●	●●
Current Market Share	40%	15%	15%	5%	15%	0%

Liopa’s unique IP is based on 10+ years of research at Queen’s  
Patent process has commenced Q3 2015



185



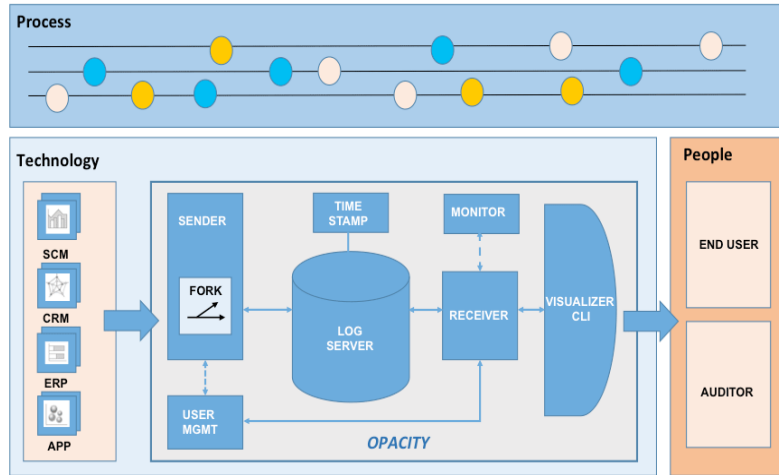
# OPACITY

Enhance your enterprise's  
reputation by being transparent

## Privacy Protection in EU Law

<p><b>Lawfulness</b></p> <p>(a) given consent, or processing is necessary (b) for the performance of a contract, (c) for compliance with a legal obligation, (d) to protect vital interests of the data subject, (e) for a task carried out in the public interest, or (f) for the purposes of legitimate interests pursued by the data processing entities if such interests are not overridden by the fundamental rights and freedoms of the data subject.</p>	<p><b>Consent</b></p> 	<p><b>Purpose Binding</b></p> <ul style="list-style-type: none"> <li>- Compatible with the one consented to</li> <li>- Principle is mostly unknown outside EU</li> <li>- It is inhibiting Big Data applications</li> </ul>	<p><b>Data Minimisation</b></p> <ul style="list-style-type: none"> <li>- Anonymized</li> <li>- Erased after use</li> </ul>
<p><b>Transparency</b></p> 	<p><b>Rights of the Individual</b></p> <ul style="list-style-type: none"> <li>- Access</li> <li>- Block</li> <li>- Erase</li> <li>- Withdraw</li> </ul>	<p><b>Data Protection and Security</b></p> <p><b>CIA</b></p>	<p><b>Accountability</b></p> <ul style="list-style-type: none"> <li>- Audit</li> <li>- Responsibilities</li> <li>- DPO</li> <li>- Cooperation with DPA</li> </ul>





## Innovative Privacy Company





# CRYPHO

End-to-end-encrypted messaging and sharing for high-security environments.



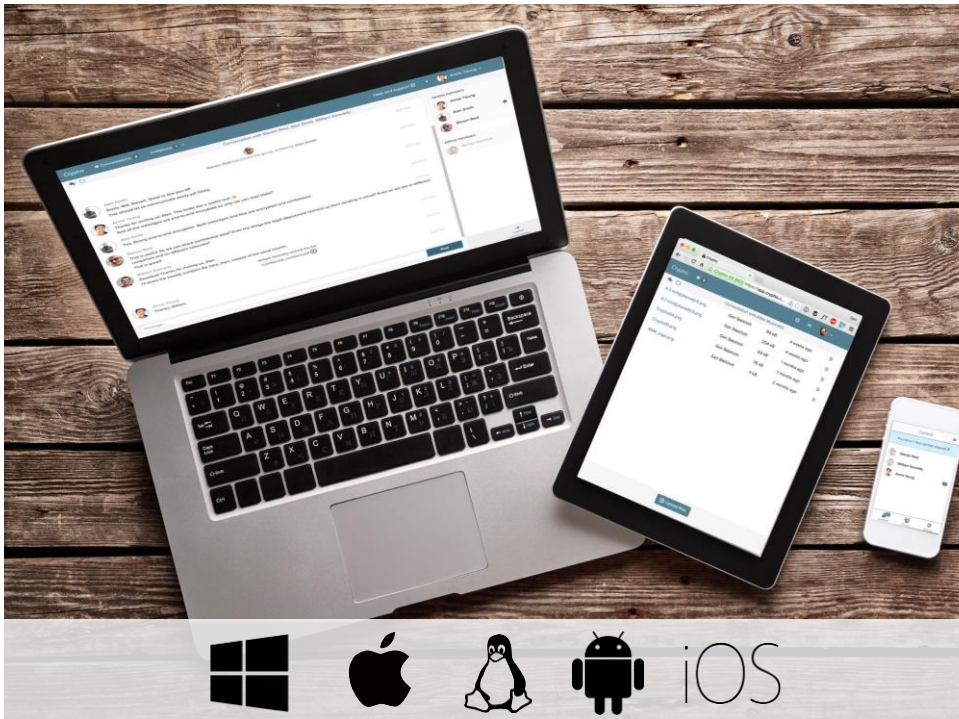
Winner Startup World London '13

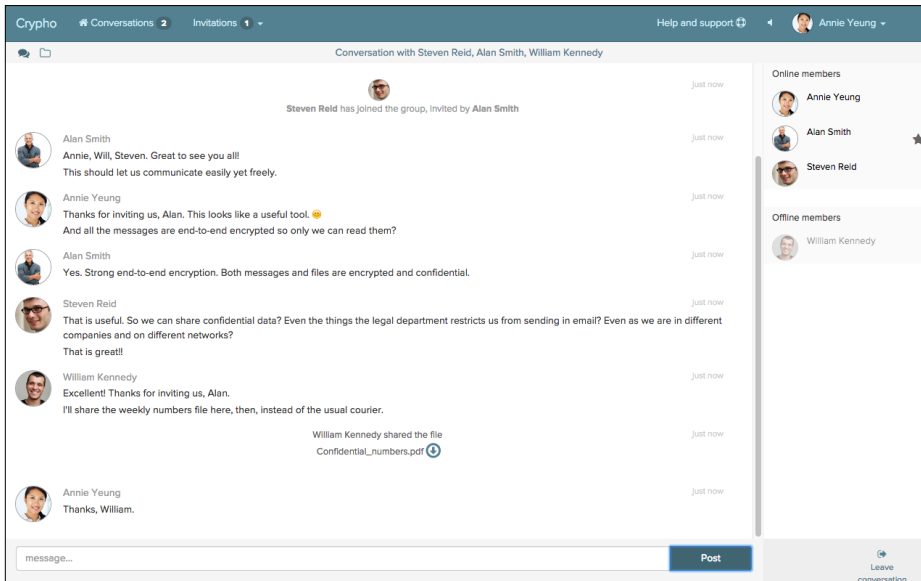


Winner Norwegian Young Technology Award



Winner: Tech Trailblazers Security Prize Europe





## End-to-end-encryption

All messages and files are encrypted before they transferred over the network. They can only be decrypted when they reach their intended recipient.

Only you hold your encryption keys, not even Crypho staff has access.



2-factor-authentication



No data stored unencrypted



Hosted in Europe under European Law

All information transferred or stored is encrypted with AES with random 265-bit keys on your phone or computer before being transferred over the Internet. Crypho's staff never handles or has access to your keys. Key exchange happens through elliptic curve cryptography (El Gamal ECC). Additionally, all communication runs through TLS to safeguard against potential man-in-the-middle attacks.

# CRYPTHO

Geir Bækholt

[baekholt@crypho.com](mailto:baekholt@crypho.com)



Winner Startup World London '13



Winner Norwegian Young Technology Award



Winner: Tech Trailblazers Security Prize Europe



## ICT Security Innovation





# HiCrypt™ 2.0



10/22/2015



Peter Liebing, Head of Sales & Marketing

## How you should **encrypt** your data:

	May 2015	May 2014	Abw. % YoY
Ertragssteu	210.441	173.059	21,1%
Warenwertsteu	0	0	0,0%
Umsatzsteuer	144.610	146.300	-1,1%
Steuerg. Betriebliche Krise	25	0	0,0%
Betriebslicher Aufwands	114.620	99.791	14,7%
Umsatzsteuer	80.819	80.800	0,0%
Umsatzsteuer	33.801	18.991	78,0%
Abgabenwegen	1.020	1.001	1,8%
Steuerg. Betriebliche Krise	0	0	0,0%
Betriebslicher Aufwands	48.270	41.204	17,2%
Zuschüsse	0	0	0,0%
Zuschüsse	0	100	100,0%
Steuerg. Betriebliche Krise	240	0	0,0%
Umsatzsteuer	46.441	21.654	114,5%

Managing Director

```

sik238fjnlkALO3LÖmxN35mÖL6ckemr38K
MMP5ö6e4p5mckB5e9r39mioo35mmMl0i
4io5jmcÖÄspden4594NjdouV49mclaiod
pocimcödiepo30kiköaiomLjhrfnwaoal
wu3nck291ö6nnl0NBAmateI3nmlösidije
45iöÜzpmxmAkLDmdmrbIUlSik238fjnlk
LO3LÖmxN35mÖL6ckemr38K MMP5ö6e4
p5mckB5e9r39mioo35mmMl0i4io5jmcÖ
Äspden4594NjdouV49mclaiodpocimcöit
joweiewerj38dfnl23Utdj04n6skpidocmrö
sakjsakwj389dnlLanLaöDnr95nsöcfnaü34
    
```

Administrator/Provider

## With HiCrypt™ 2.0

10/22/2015

## Function of our encryption software



What is the alternative?

[WWW.STORRO.COM](http://WWW.STORRO.COM)



STORRO




Secure sharing  
and storing

You have full  
control




No additional IT  
support

Just you and your contacts have the keys...  
and *no* one else.

[WWW.STORRO.COM](http://WWW.STORRO.COM)



STORRO



Technology to  
compartmentalize

Technology to  
encrypt

Technology to  
decentralize

Your files are *not* located at 3<sup>rd</sup> parties...  
nor can they be accessed by any.

[WWW.STORRO.COM](http://WWW.STORRO.COM)



Automatic  
back-up



Endless revision  
control



Permanent audit  
trail.

Your files *only* come in the hands of those  
for who they are intended.

[WWW.STORRO.COM](http://WWW.STORRO.COM)



STORRO

*You* are in control!

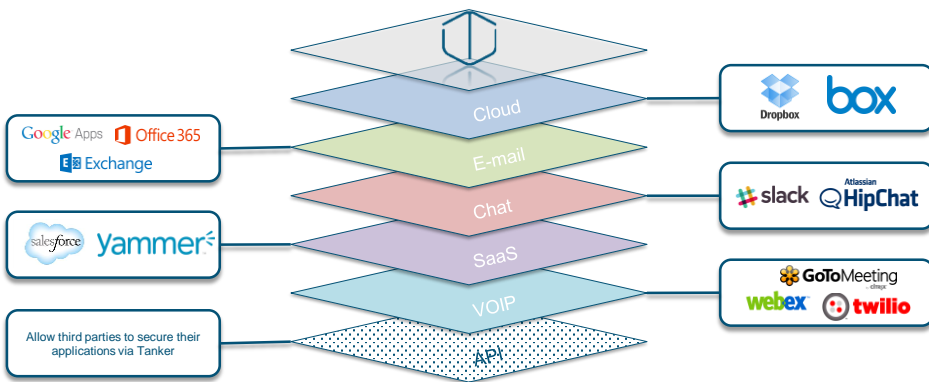
To be launched beginning of 2016. Stay up-to-date via [storro.com](http://storro.com)

**Coblu**  
e  
cybersecurity



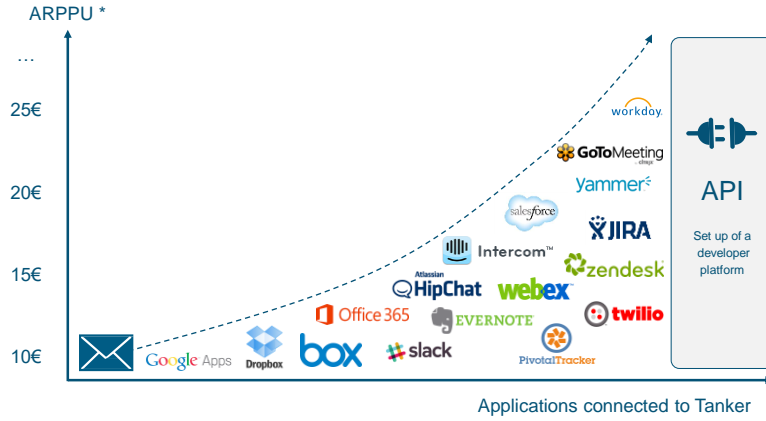
## Value Proposition

Tanker is an APP that encrypts all the data of your cloud apps directly on your device



# Growth

Our "Pay As You Go" model allows companies to gradually secure their business applications

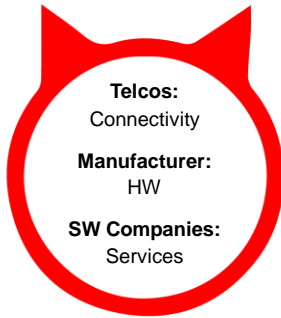


\* Average Revenue Per Paying User (per month)

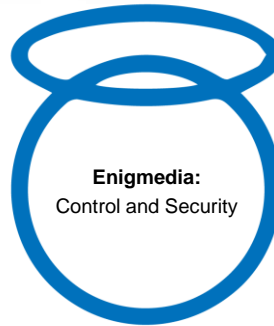


**Juan Luis Moreno,**  
Legal Manager  
[www.enigmediasecurity.com](http://www.enigmediasecurity.com)

## Each User fully control his network



They compete to get control over user's to build a platform.

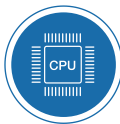


We provide users' full ownership and we let them grant secure access only to those services & devices they wish.

## How we do it?



We have discovered, implemented and patented a new method of encryption, **that is 160 times faster & more efficient than current Standards,** ready for market adoption.



**PERFORMANCE**  
95% less CPU consumption than standards



**PORTABILITY**  
No specific hardware required




**SECURITY**  
252 bits of seed – customizable




**CERTIFIED**  
Laboratories, Researchers, Universities, CC certified

Platform B2B




We are working in this vertical: First Product Brand -Easy approach -Revenue


Internet of Things




Most value for our tech: IoT - Critical Infrastructure - Satellites




## B2B Platform (audio – video – IM)




- ✓ Stand Alone Solution
- ✓ Customers do not need to trust us as a Security Provider
- ✓ Allows engage new users to the system even when they are outside the Company
- ✓ Performance






50% BW Savings




Adaptative audio



Secure IM



Open Network



Ownership



# Access Governance for SAP environments

Multi-layer analysis

Automated role building

Reverse engineering

Comply privacy regulations



Innovation Leader  
Access Control / Governance  
for SAP environments  
July 2015



Product Leader  
Access Control / Governance  
for SAP environments  
July 2015

Johan Hermans  
CEO  
johan.hermans@csi-tools.com



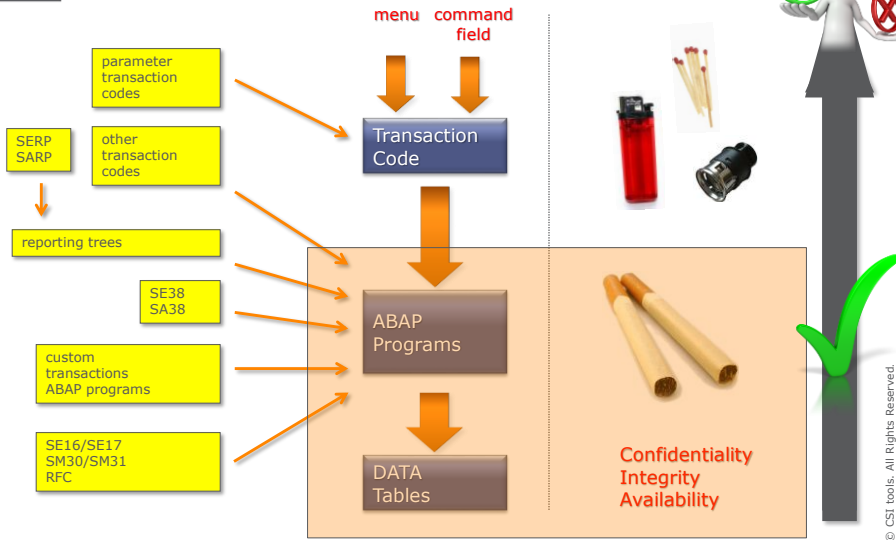
## Introduction Two Core Elements in SAP Application Security

Key questions:	Transaction codes	Authorization Objects
How many ... exist in an SAP ECC 6.0 system?		
Purpose?		
	Transaction codes	Authorization Objects
Typical reply by security administrators	20.000	A multiple of 20k
Purpose?	To manage access rights	To restrict on organizational levels
	Transaction codes	Authorization Objects
Reality	+ 150.000	1.000 for "R/3" functionality
Purpose!	Only first line of defense	To manage access rights

© CSI tools. All Rights Reserved.



# Demystification – SAP Security



# In depth analysis of the causing: our multi-layer security approach

accumulation of access rights

Profile (causing)	Role (causing)	E	Last used	A	T	V	Role (assigned)	c	E	Last use	Valid from	Valid until	e
FXXXXAPPRA	S99FXXXXAPPRA	<input checked="" type="checkbox"/>	03/2012	2/3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	S992-XXXX-AR_CLERK	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	03/2012	26/11/2012	31/12/9999	<input type="checkbox"/>
SXXXXBASEA	S99SXXXXBASEA	<input checked="" type="checkbox"/>	03/2012	1/3	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>
FXXXXAPPRA	S99FXXXXAPPRA		F110	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
FXXXXAPPRA	S99FXXXXAPPRA		FB20	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
FXXXXAPPRA	S99FXXXXAPPRA		FB25	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
FXXXXAPPRA	S99FXXXXAPPRA		FDTA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
FXXXXAPPRA	S99FXXXXAPPRA		F_RE_BUK	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	XXXXAPPRA01	<input type="checkbox"/>	<input type="checkbox"/>				
FXXXXAPPRA	S99FXXXXAPPRA		F_RE_KOA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	XXXXAPPRA01	<input type="checkbox"/>	<input type="checkbox"/>				
SXXXXBASEA	S99SXXXXBASEA		S_DA_GET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SXXXXBASEA01	<input type="checkbox"/>	<input type="checkbox"/>				

causing the access

used: when & frequency

assigned through

composite role used

Print    Export Excel    Export PDF    Export XML

Reset layout    Cancel

© CSI tools. All Rights Reserved.



## Access Governance: Automate Role Maintenance: **who – what – where !**

- Organizational perspective
  - Define Requirements on data level
  - Define Requirements on process level
- System perspective
  - Codify the WHAT requirements
  - Codify the WHERE requirements
  - Build all SAP roles fully automated
- Assign roles using business language



**WHAT**



**WHERE**

Workbooks - Domain workbook

Drag a column header here to group by that column.

General				Authorization restrictions							
Modu	Field	Description	Objects	M	T	A	Master XXXX	Belgium B10X	Netherlands N10X	USA L10X	New 11 UN10
F	KT0PL	Chart of Accounts	*	*	*	*	*	EURO	EURO	EURO	EURC
F	BUKRS	Company Code	*	*	*	*	*	3200	3100	0100, 0101	EURC
F	BFGRU	Authorization group	F_LFAT_BK	*	*	*	*	TBD	NET	NET	NEW
K	KONRS	Controlling Area	*	*	*	*	*	EURO	EURO	EURO	EURC
M	MELRCL	Plant	*	*	*	*	*	3200	3100	0100, 0101	EURC
M	EXOR0	Purchasing Organization	*	*	*	*	*	3200	3100	0100	0100

218

© CSI tools. All Rights Reserved.

# SecurIT

Marc Vanmaele  
CEO




Oct 2015

## TrustBuilder Identity Hub

Smart bridging of the identity cloud

© 2015 SecurIT

## SecurIT Company Overview

- Created in 1999 and privately held
- Offices:
  -  Gent
  -  Amsterdam
  -  New York
- Partner Eco system



### Product activity

- Software Editor
- VC funding
- TrustBuilder® Identity Hub



### Project activity

- Focus on IAM solutions
- +40 consultants on IAM
- +50 successful Projects at Large Enterprise Customers

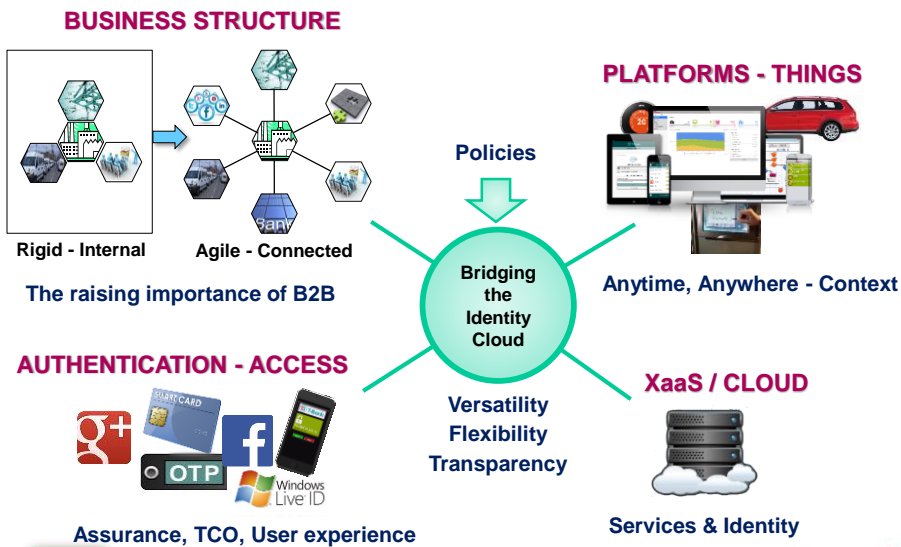


220

© 2015 SecurIT

**SecurIT**

## Challenges of a rapidly changing environment

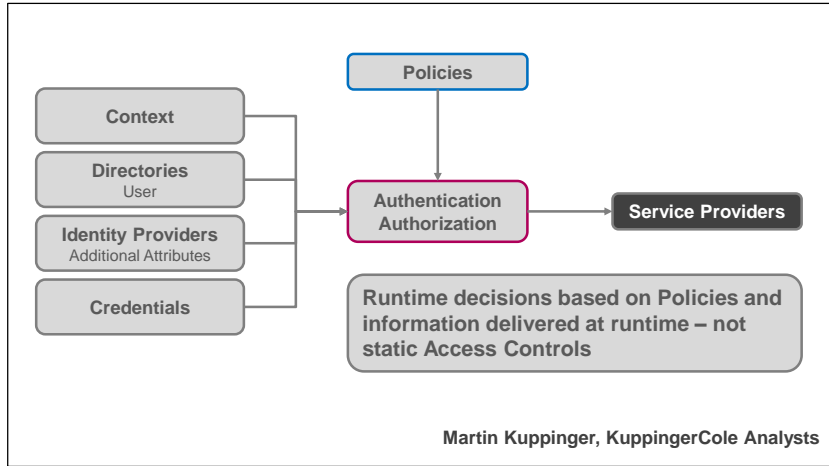


221

© 2015 SecurIT

**SecurIT**

### The Future of Authentication & Authorization

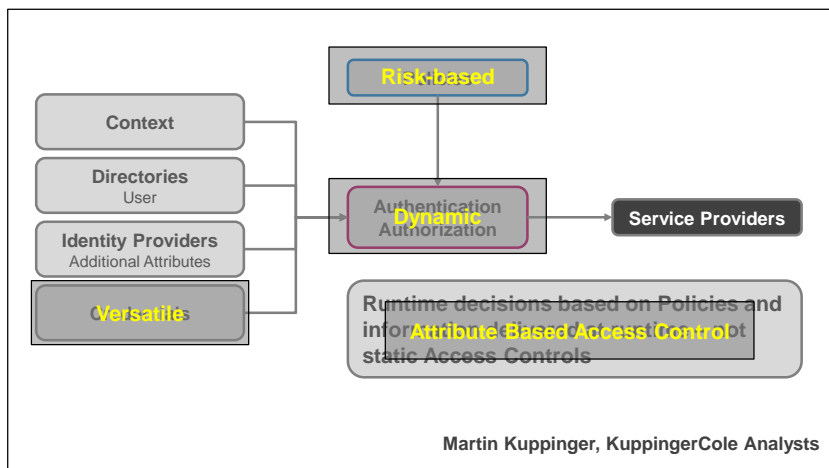


222

© 2015 SecurIT

SecurIT

### The Future of Authentication & Authorization

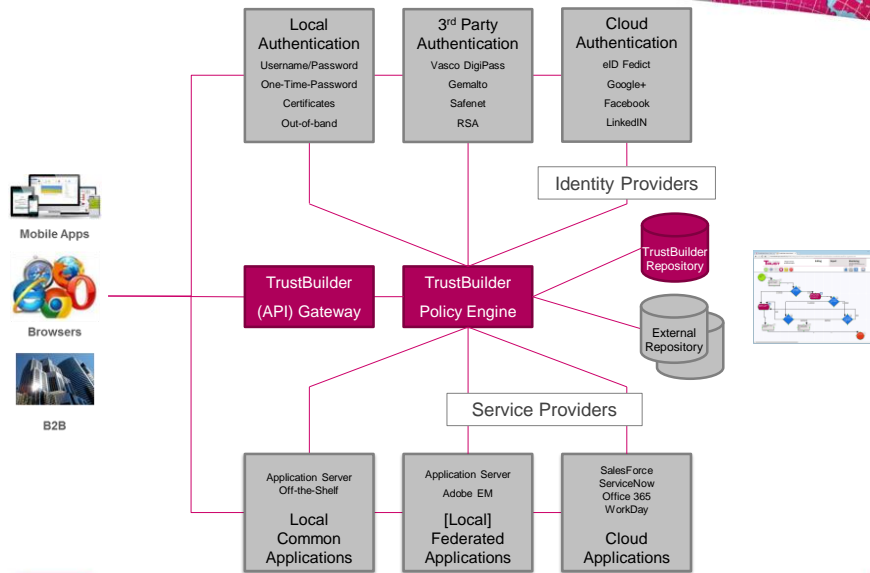


223

© 2015 SecurIT

SecurIT

## TrustBuilder Identity Hub: the big picture



224

© 2015 SecurIT

SecurIT

## Some SecurIT Customers






225

© 2015 SecurIT

SecurIT



## Access Security Solutions for IoT use cases


 Cyber Security & Privacy Innovation Awards 2015 – Public
 
 226
 


### IoT use cases



**Someone** requests an operation to an IoT Cloud or Gateway....

Online



From an App federated with the IoT



From a connected 'thing' (e.g. a car head unit)



If this operation is sensitive (safety, privacy...) or requires explicit user consent, the IoT Cloud or Gateway triggers a step-up authentication request to the credential server

The **legitimate user** is notified and prompted to give – or deny - his consent (via a seamless strong authentication) on the appropriate interface, such as



A web browser






The IoT Cloud provider App



A 'thing'



A wearable...


 Cyber Security & Privacy Innovation Awards 2015 – Public
 
 227
 


# UM Labs UC Security Platform

Peter Cox  
CEO and Inventor

October 2015

## Why UC Security Innovation is needed

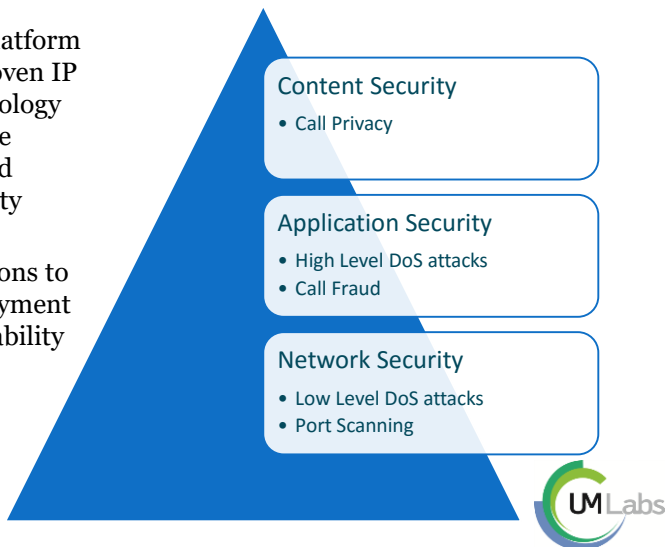
- VoIP and UC Services are growing
- All services run on IP networks
- Little or no awareness of the security threat
- Existing IP security technologies are a barrier to deployment
- Telco technology (SBCs) designed for peering, not security
- VoIP and UC Services specifically covered by EU compliance regulations

MarketsandMarkets expects the global mobile Unified Communications and Collaboration market to grow from **\$5.15 billion** in 2014 to \$17.38 billion by 2019, at a Compound Annual Growth Rate (CAGR) of **27.5%** during the forecast period 2014 – 2019.

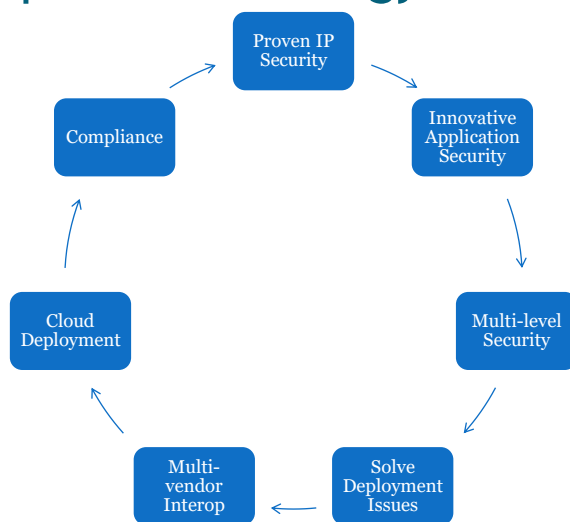


## The UM Labs Innovation

- UC Security Platform combining proven IP Security technology with innovative application and content Security
- Specific functions to simplify deployment and interoperability



## Disruptive Technology



## Commercial Proof Points

- European National Telco, UC Security as a service
- Bull France, back-end service for encrypted mobile devices
- nfon AG/nfon UK, integration with Microsoft Lync
- Many legal and financial institutions



...continuumsecurity...

THE PROCESS OF SECURE SOFTWARE

Countermeasure progress can be tracked through IriusRisk itself, or an issue can be created on a defect tracker.

Countermeasure Details    Test

Name\* Use prepared statements for all database queries

Rejected	Cost	Reference*	Defect ID
<input checked="" type="checkbox"/> Recommended	Low	CWE-89-PREPARED	
<input type="checkbox"/> Required			
<input type="checkbox"/> Implemented			

Description

including queries through an Object-Relational mapper should always be made  
 Creating queries by concatenating strings using untrusted data may result in **vulnerable code**, fo

```
String query = "SELECT user FROM users WHERE name = '"
+ request.getParameter("customerName")+'";
```

Standards

- OWASP-ASVS-Level-2-5.10
- OWASP-ASVS-Level-3-5.10
- OWASP-ASVS-Level-1-5.10

[Add standard](#)



Cyber Security & Privacy Innovation Awards 2015 – Public

234



## ICT Security Innovation



Cyber Security & Privacy Innovation Awards 2015 – Public

235

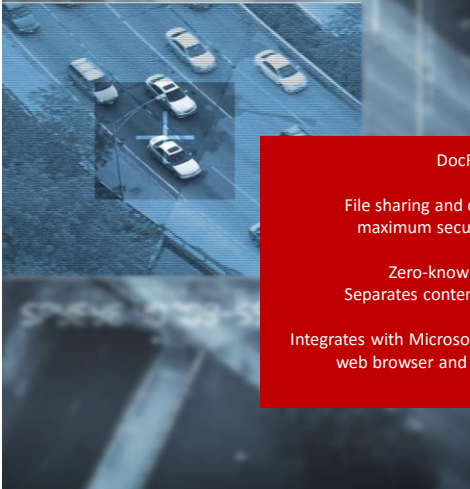




zero knowledge enterprise file sharing and email encryption

Security concerns limit the use of cloud services.

DocRAID® protects your enterprise against threads in the cloud.



DocRAID®

File sharing and collaboration with maximum security - made easy

Zero-knowledge-policy  
Separates content from operation.

Integrates with Microsoft Outlook®, file explorer, web browser and any mobile device.



zero knowledge enterprise file sharing and email encryption

Industrial espionage  
Information security  
Compliance  
IT Security  
Legal frameworks

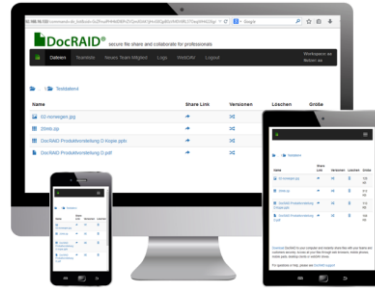
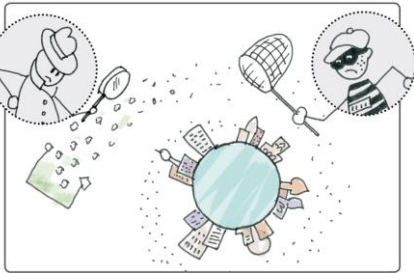
Share information, documents:  
teams, customers, clients,  
suppliers, contractors, ...  
Any device, anywhere  
Integration



Requirements from multiple stakeholders

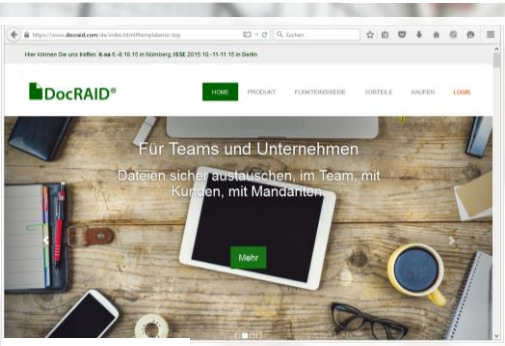
**DocRAID®** zero knowledge enterprise file sharing and email encryption

Information protection by design - IT security and compliance for all devices, all the time, everywhere



Multi award winning security features – fragmentation, encryption and redundant distribution

**DocRAID®** zero knowledge enterprise file sharing and email encryption



**Company server:**

**from 10€ per user/month**  
concurrent licenses / on-premise / off-premise

**Private account:**

**from 10€ per month**

Join DocRAID now at [www.docraid.com](http://www.docraid.com)



**Thank you!**

**DocRAID®**  
**ContentPro AG**  
 Wilhelm-Kabus-Str. 25-31  
 10829 Berlin  
 Germany  
 Tel. +49-30-60 9898 062

**Meet us here:**

**startupcon**  
 by Business of the Future

Köln, 22. Oktober 2015

**Contact:**

**Dr. Günther Hoffmann**  
 hoffmann@docraid.com

**2015 ISSE**

Berlin, 10. - 11. November 2015

## Privacy or Cyber Security Innovator

**IPACSO AWARDS**  
 INNOVATION FRAMEWORK FOR ICT SECURITY

**FINALIST OF THE 2015 EDITION**

Logos of partner organizations: L&SEC, EUROPEAN UNION, BERLIN, FINN, MANNOCO, explon, TSGG



**Pim Cornelissen**

Founder  
Chief Strategic Officer

**William van Collenburg**

Solution Architect

**CYBER  
ATTACKS  
AHEAD**



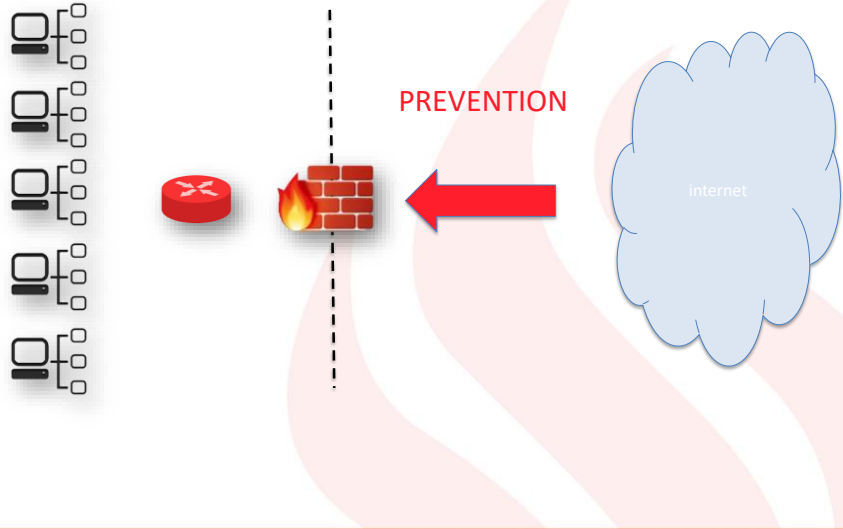
RedSocks is a Dutch IT security company specialized in detection and fighting of malware.

With a focus on flow-based monitoring of outbound data traffic.

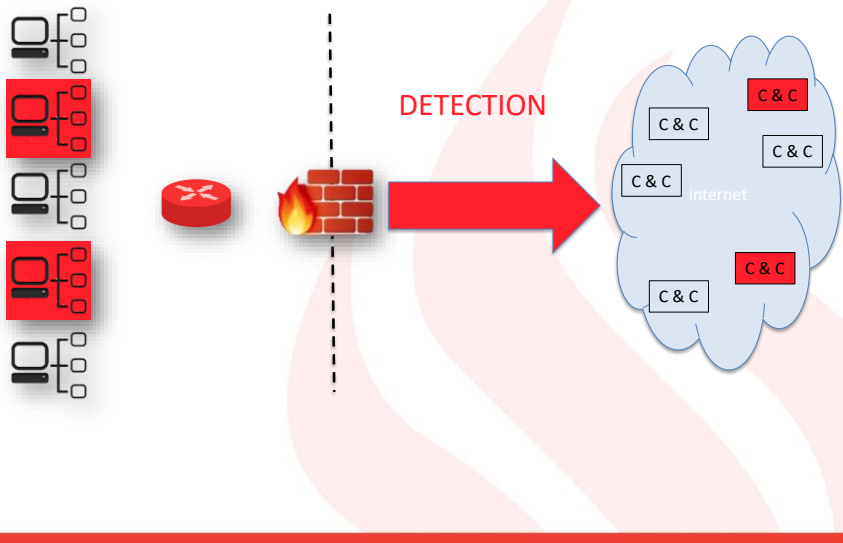
The critical information is compiled by the **RedSocks Malware Intelligence Team**. The team consists of specialists whose job it is to identify new threats on the Internet and translate them into state-of-the-art malware detection capabilities.



Most security measures focus on preventing infections

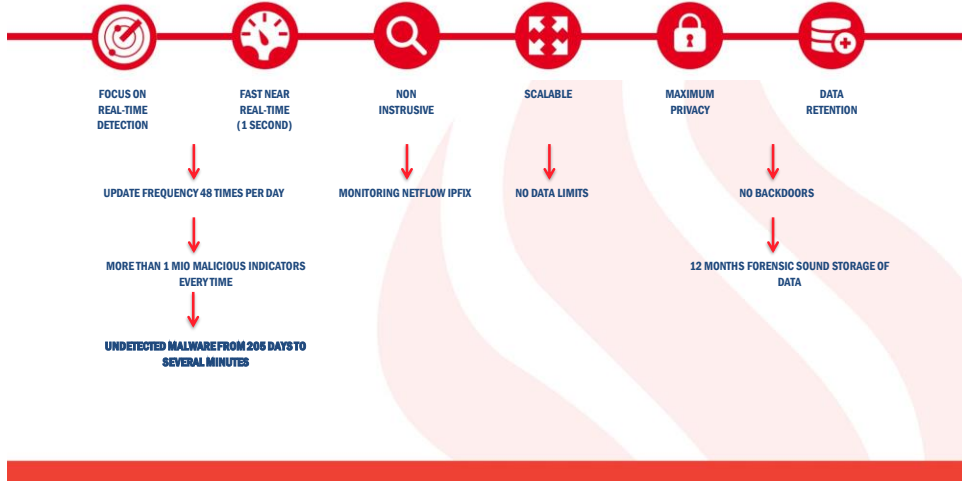


RedSocks: your network is already infected, so focus on detection!

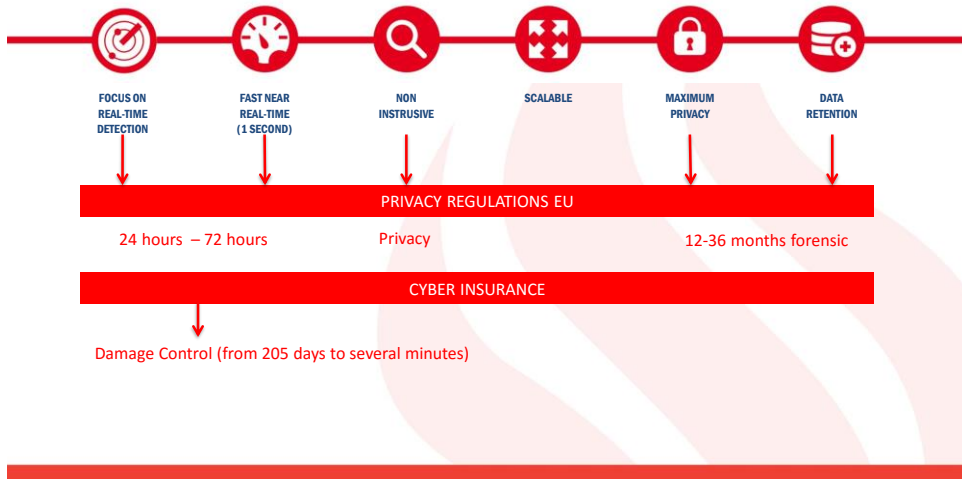




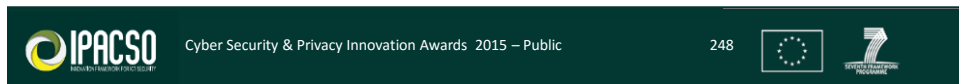
### RedSocks Malware Threat Detection unique Solution



### RedSocks as a Compliance & Insurance solution



## Privacy or Cyber Security Innovator



Decisionmaking  
while protecting  
privacy

dan.bogdanov@cyber.ee  
baldur.kubo@cyber.ee  
<https://sharemind.cyber.ee>

 CYBERNETICA

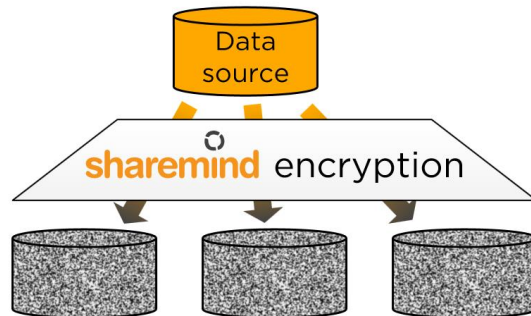
 sharemind

# Technology of Sharemind

- Cybernetica's in-house R&D team has worked on security technologies for 20 years.
- Sharemind is based on our breakthroughs in *secret sharing* and *secure multi-party computing*.
- Secret sharing provides cryptographically private, distributed storage encryption.
- Secure multi-party computation allows Sharemind to process encrypted data.

sharemind

## Sharemind protects data at the source



Separate hosts – no central control or key

sharemind

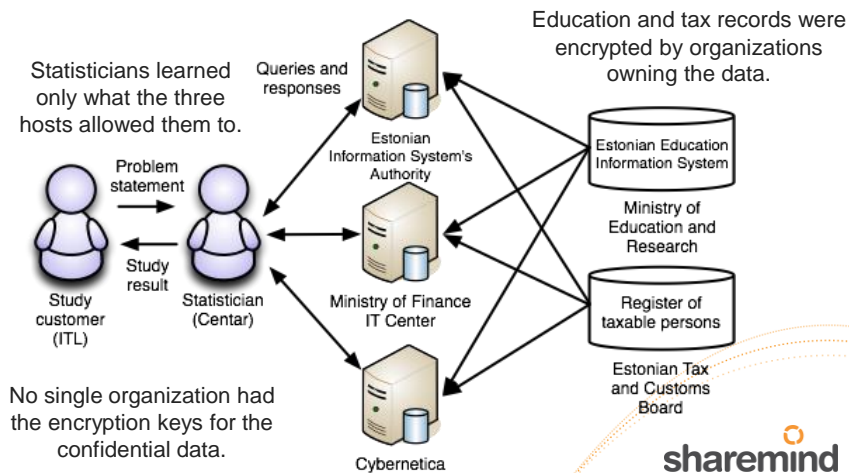
# Sharemind protects data in the analysis



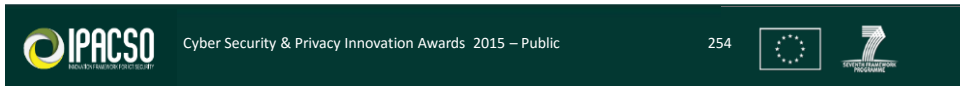
Decryption possible only with host consensus




# PRIST: Privacy-Preserving Statistical Study on Linked Databases



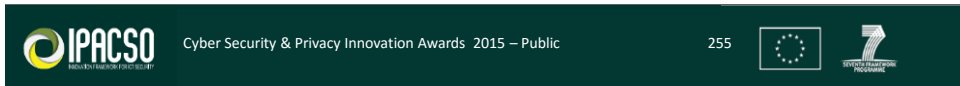
# Innovative Privacy or Cyber Security Research





**n-Auth**

Usable, secure and private authentication



## Business risks by the use of mobile devices: A decision support system of best practices for policy, roles, responsibilities & instructions to mitigate cyber risks

Trijntje van Dijk MA MLD MSc: Saxion  
t.vandijk@saxion.nl



Kom verder. Saxion.



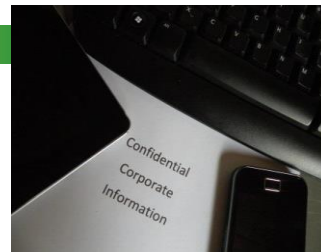
Csec: Promotor Prof.dr.ir. Jan van den Berg: DUT, LU  
Csaf: Promotor Prof. dr. W. Ph. Stol: OU, PA  
RM: Lector Wilbert Rodenhuis, Saxion



Kom verder. Saxion.

### Search, phasing, deliverables

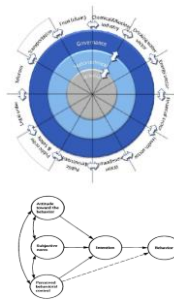
Main search:  
What factors make employees adapt to  
policy,  
responsibility and  
protective behaviour?



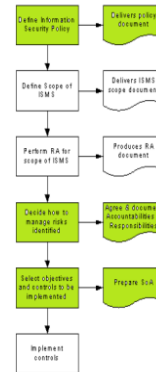
Year	Phases	Deliverables
2015-16	1-2 Problem identification, define objectives of a solution	Problems in policy, roles, responsibilities, instructions; Factors affecting users' behaviour. From Drinking Water, Water Defence, Food Chain, Banking (3), Education.
2017	3 Artefact	A set of best practices supporting decision making
2018	4-5 Demonstrate, evaluate	Testing in six contexts, mainly from the critical infrastructure; Data and evaluation report.
2019	6 Communicate	Publication*



# Theory and framing



- 1 Cybersecurity: NATO & Delft conceptualization socio-technical layer with critical infra domains (VandenBerg)
- 2 Quality: ISO 27001: policy, roles, responsibilities, instructions
- 3 System: System design science & phasing & products (Hevner, Peffer)
- 4 Risk communication: protective behavior, information seeking (Aizen, Griffin)



SAX_A4Factsheet_Staand_HR2					
1	2	3	4	5	6
<b>IDENTIFY PROBLEM &amp; MOTIVATE</b>	<b>DEFINE OBJECTIVES OF A SOLUTION</b>	<b>DESIGN &amp; DEVELOPMENT</b>	<b>DEMONSTRATION</b>	<b>EVALUATION</b>	<b>COMMUNICATION</b>
Define problem Show importance <i>Inference</i>	What would a better artefact accomplish? <i>Theory</i>	Artefact <i>How to knowledge</i>	Find suitable context Use artefact to solve problem <i>Metrics, Analysis knowledge</i>	Observe how effective Option iterate back to design <i>Disciplinary knowledge</i>	Scholarly publications Professional publications



# Key differentiators

Urgency: business problems, NIAS, NCSRAll, science knowledge gap

Product requirements

- A *behavioural* decision support model
- A *tailored* need & supply risk communication
- A *business-employees* setting
- A *cyber* setting

Critical Infrastructure as source and test context  
Drinking water, water defence, food chain, banking

Trans disciplinary

Technical business security & Human behaviour

International network recognition



Kom verder. Saxion.

## Network

André Richier



**European Commission**  
 DG for Internal Market, Industry, Entrepreneurship and SMEs  
 Unit for Key Enabling Technologies, Digital Manufacturing and Interoperability



European Committee for Standardization  
 Comité Européen de Normalisation  
 Europäisches Komitee für Normung



**General (ret.) Dick Berlijn**  
 Senior Board Advisor  
 Deloitte Executive Office

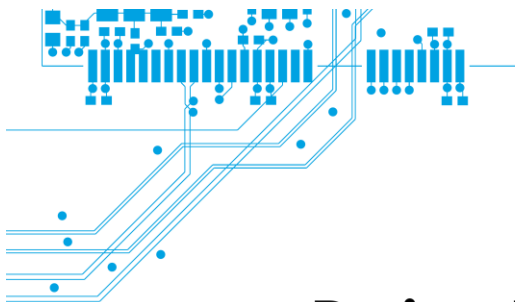


Twente Safety & Security



## Privacy or Cyber Security Innovator





# Project Turrís

Research project helping to protect home networks

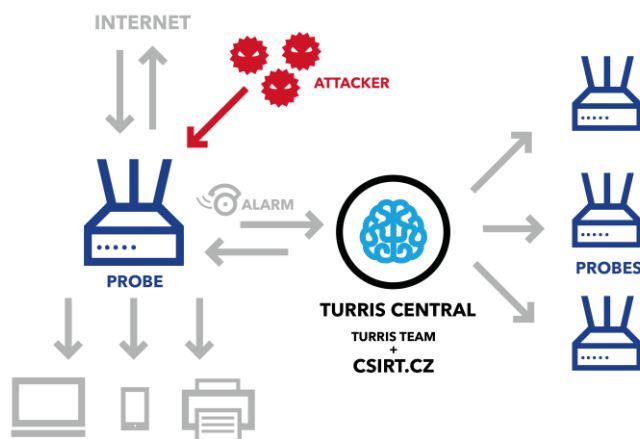
**Martin Strbačka** [martin.strbacka@nic.cz](mailto:martin.strbacka@nic.cz)

**cz.nic** | CZ DOMAIN  
REGISTRY

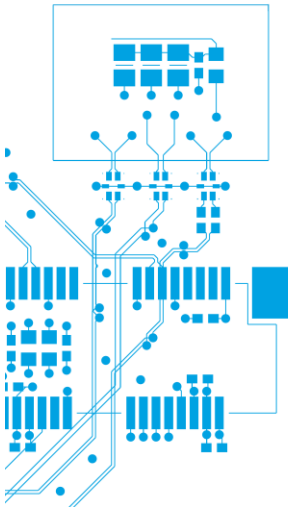
[www.turris.cz](http://www.turris.cz)

## How the Project Turrís works?

Complex secure ecosystem consisting of 2000 pcs secure-by-design routers (probes) and Turrís Central



## Project Turrís outcome



- We found:
  - 2 botnets consisting of SOHO routers
  - computers connected to Zeus botnet
  - malware in 2% of home networks
  - ISPs breaking net neutrality
- Cooperation with Synology on analysis of Synolocker malware
- Statistics, IP Address Greylist, Open data

### And also...

## ...we have learned how to make hardware

Turrís router main features:



### Open source

Open hardware running free operating system based on OpenWrt



### Performance

Most powerful SOHO router by the time of its release



### Security

Secure default configuration, easy setup and automatic updates

Not intended for market. We wondered how to satisfy demand on it...



# More than just a router

Spin-off of Project Turris

Coming soon to Indiegogo  
For now visit [omnia.turris.cz](http://omnia.turris.cz)



Cyber Security & Privacy Innovation Awards 2015 – Public

267

