ISA Italy Section

Cyber security - why and how

Frankfurt, 14 June 2018 - ACHEMA

Cyber security,
application software and data control:
do not fear the unknown,
face reality!

Premier Business Partner IBM

UNI EN ISO 9001:2015
UNI CEI ISO/IEC 27001:2014
CERTIQUALITY
SISTEMI DI GESTIONE CERTIFICATI

Marco Passerini

BAGGI®

RES IT®

All names and products mentioned in this document are registered trademarks of their respective holders.

The whole content of this document is property of RES IT srl

This edition applies to version 5, release 1, modification level 0, of **RES Suite** and to all subsequent releases and modifications, until otherwise indicated in new editions.

www.res-it.com/en

RES IT srl

A complete value proposition based on:

Skill – a Suite of solutions – Services

Skill

RES IT: two primary areas of the Enterprise IT Management:

- Process Engineering
- System Governance

Extensive experience, over 30 years of experience, an international presence, besides a deep knowledge of all platforms makes RES IT a point of reference for governance and optimization of software, development processes and for management of application components.

Res Suite

Res Suite provides a wide range of products, independent and synergistic with each other, based on a comprehensive and efficient "Database of Knowledge".

Services

As part of its technological offering, RES IT provides a full range of Professional Services:

- Consulting,
- Project Management,
- Service Management,
- Help Desk,
- Maintenance,
- Training.

Cybersecurity
definitions found on internet

Wikipedia:
[…] is the **protection** of computer systems **from the theft and damage**
to their **hardware**, **software** or **information** […], includes controlling physical access to the hardware,
as well as protecting against harm that may come via network access, data and code injection […]

Oxford Dictionaries:
The state of **being protected** against the **criminal** or **unauthorized** use of electronic data,
or the measures taken to achieve this

Gartner:
[…] a broad range of **practices**, **tools** and **concepts** related closely to those of information and
operational technology security.
Cybersecurity is distinctive in its inclusion of the offensive use of information technology
to attack adversaries […]

Cisco:
[…] is the practice of protecting **systems**, **networks**, and **programs** from **digital attacks**, usually aimed
at accessing, changing, or destroying sensitive information; extorting money from users;
or interrupting normal business processes […]

Cybersecurity
& Cyberspace

Cyberspace is the most complex thing that man has ever built:

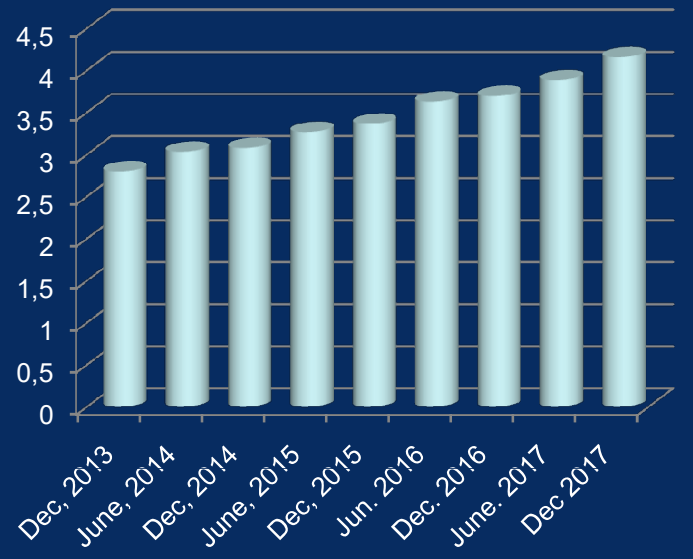
- thousands of interconnecting networks and components (HW – SW)
- stratification of software programs and protocols developed over decades
- complexity generates vulnerabilities (software errors, incorrect configurations and weaknesses in protocols)
- cyber criminals leverage on complexity and bugs to steal data and damage business

Cybersecurity

Internet, state of the art

Internet, million users - last 4 years growth:

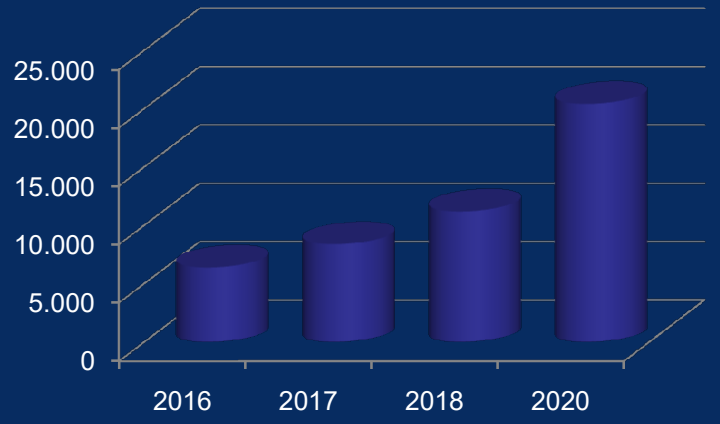
(Internet World Stats font)



Million users of IoT units installed base:

(***Gartner font***)

	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
	6,381.8	**8,380.6**	**11,196.6**	**20,415.4**

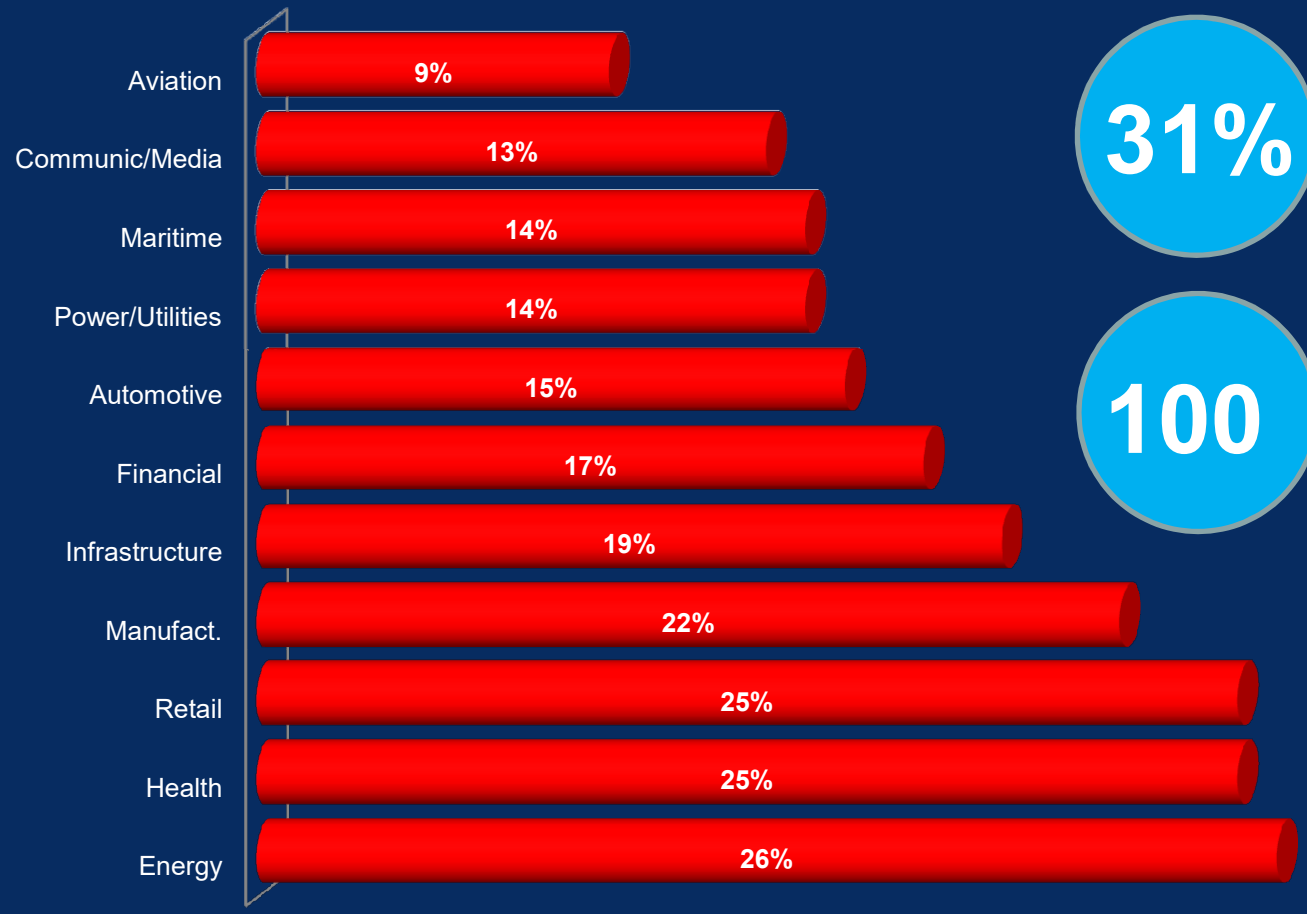


Cybersecurity

Cyber attacks, the reality

2017 - World wide ranking of the industries most commonly impacted by cyber attacks

(the Statistics Portal source)



31% of security professionals say their organizations have experienced attacks

(Cisco source)

100 Days, on average, to detect a breach

(Gartner source)

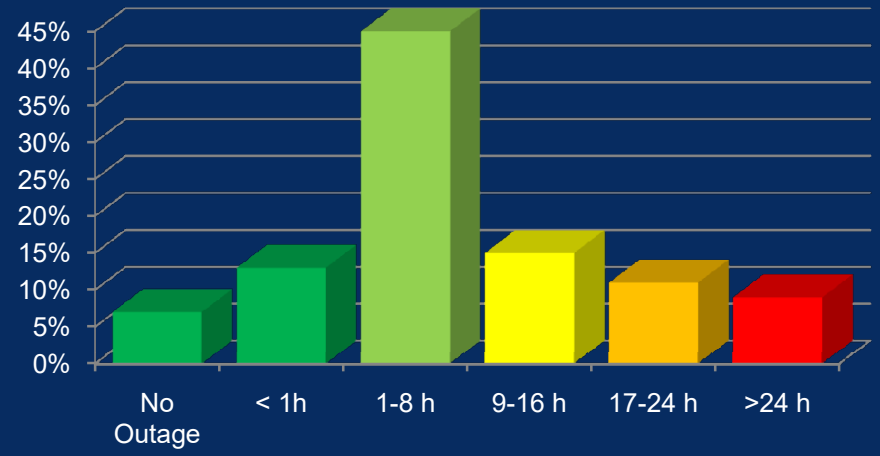
Cybersecurity

Cyber attacks, the reality

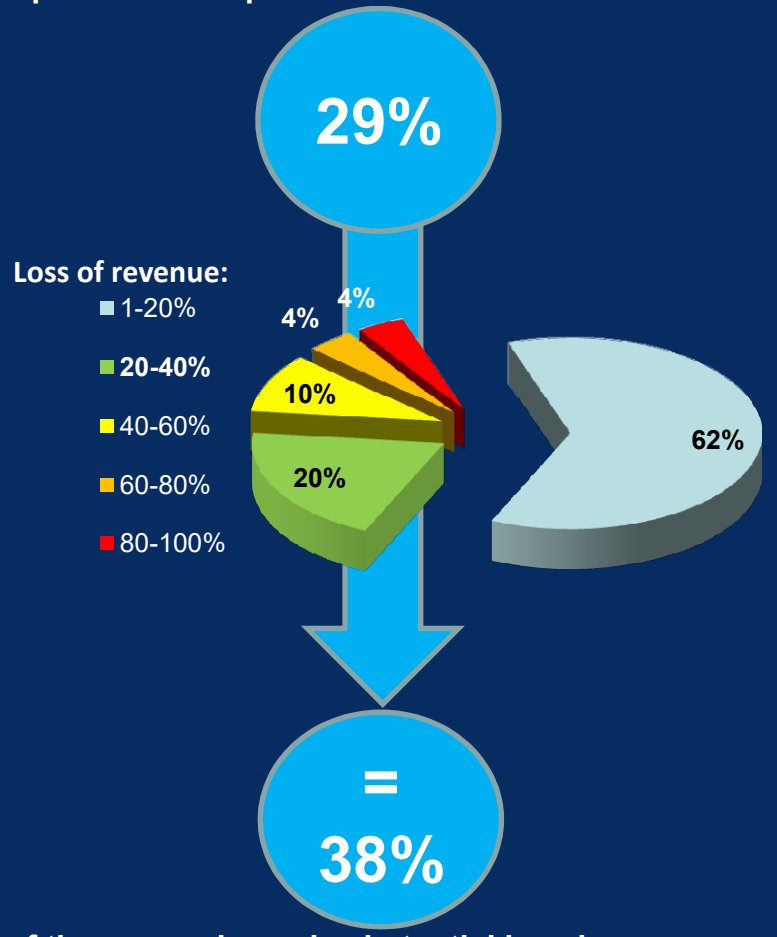
Biggest known data breaches (last 3 years):

Year	who	million users affected
2016	Yahoo	3.000
2016	Adult Friend Finder	412
2018	Twitter (risk of breach)	330
2014	Ebay	145
2017	Equifax	143
2015	Anthem	79
2014	JP Morgan Chase	76
2016	Uber	57

Outage = business down (hours)



Companies that experienced a loss of revenue in 2017



of them experienced substantial loss in revenue

(Cisco 2017 annual Cybersecurity report)

Cybersecurity
are we ready?

What's up in the SMB:

(Small Business use just Antivirus and Antispam)

44% **of Medium Business use "advanced" security systems for Intrusion Detection and Id/Access Mgmt**

30% **of Small Business do not use any protection system**

50% **SMB say they do not know what the GDPR is**

(***PoliMi source***)

Cybersecurity and GDPR

(General Data Protection Regulation - 2018/05)

also GDPR (UE 2016/679) **is part of the Cybersecurity context**

GDPR applies to companies that:

- Are established in the EU
- Offer goods or services to EU residents
- Monitor the behavior of EU residents that takes place within the EU

GDPR, among the rest, requires that the SW is checked to be breach-risk free:

- Programs developed in-house
- Third-party SW components (included, OEM, called, …)

Cybersecurity and CIS RAM

(Center for Internet Security® Risk Assessment Method, V7)

CIS RAM

a risk assessment method that helps organizations implement and assess their security

- **Basic Controls**
  1. Inventory and Control of Hardware Assets
  2. Inventory and Control of Software Assets
  3. Continuous Vulnerability Management
  4. Controlled Use of Administrative Privileges
  5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
  6. Maintenance, Monitoring and Analysis of Audit Logs

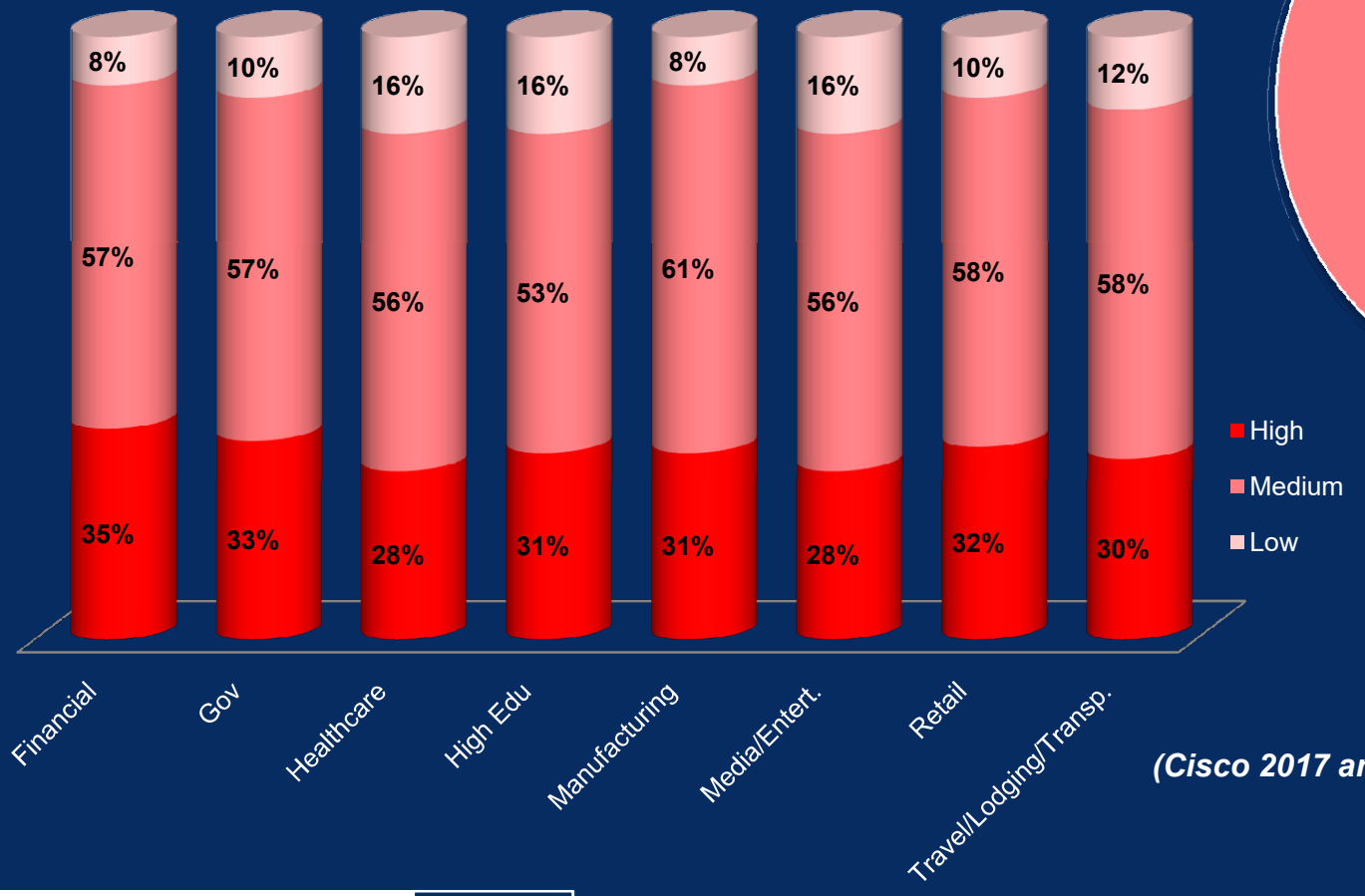
- **Foundational Controls**
  7. Email and Web Browser Protections
  8. Malware Defenses
  9. Limitation and Control of Network Ports, Protocols, and Services
  10. Data Recovery Capabilities
  11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
  12. Boundary Defense
  13. Data Protection
  14. Controlled Access Based on the Need to Know
  15. Wireless Access Control
  16. Account Monitoring and Control

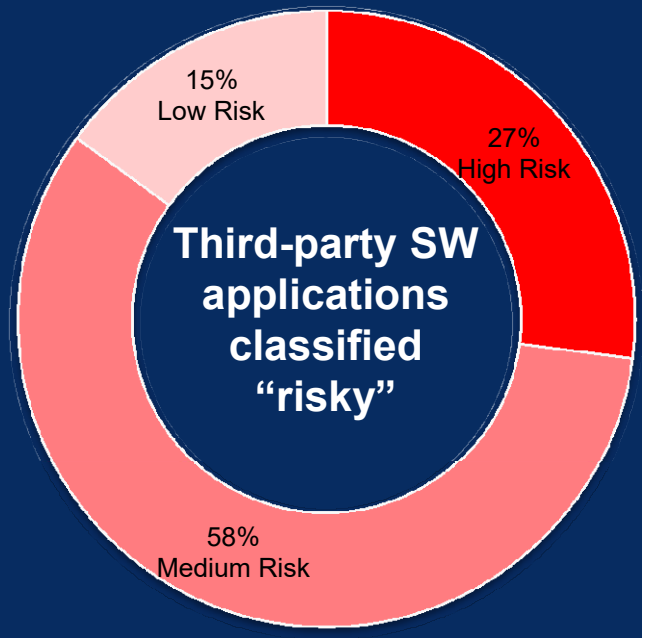
- **Organizational Controls**
  17. Implement a Security Awareness and Training Program
  18. Application Software Security
  19. Incident Response and Management
  20. Penetration Tests and Red Team Exercises

Cybersecurity

The risk hidden in third-party applications

Third-party applications classified to be "risky", by industry





(Cisco 2017 annual Cybersecurity report)

Cybersecurity

The risk hidden in the application layer (enterprise and SMB)

81% **of Fortune 500 reported breaches in the last 3Y**
(IBM source)

84% **of attacks target SW application layer**
(Gartner source)

- ***disproportionate spending on securing perimeter vs SW applications***
- ***a holistic approach to more secure SW is required***

Cybersecurity

Many tech solutions, but … is that enough?

Perimeter securing:

Intrusion Prevention Service (IPS)

Spam Blocker

Web Blocker

Application Control

Reputation Enabled Defense Service (RED)

Gateway Antivirus (GAV)

APT Blocker

Threat Detection & Response

Host Ransomware Prevention (HRP)

Data Loss Prevention (DLP)

Network Discovery

SW Applications and Data securing:

- Docet/EV

:

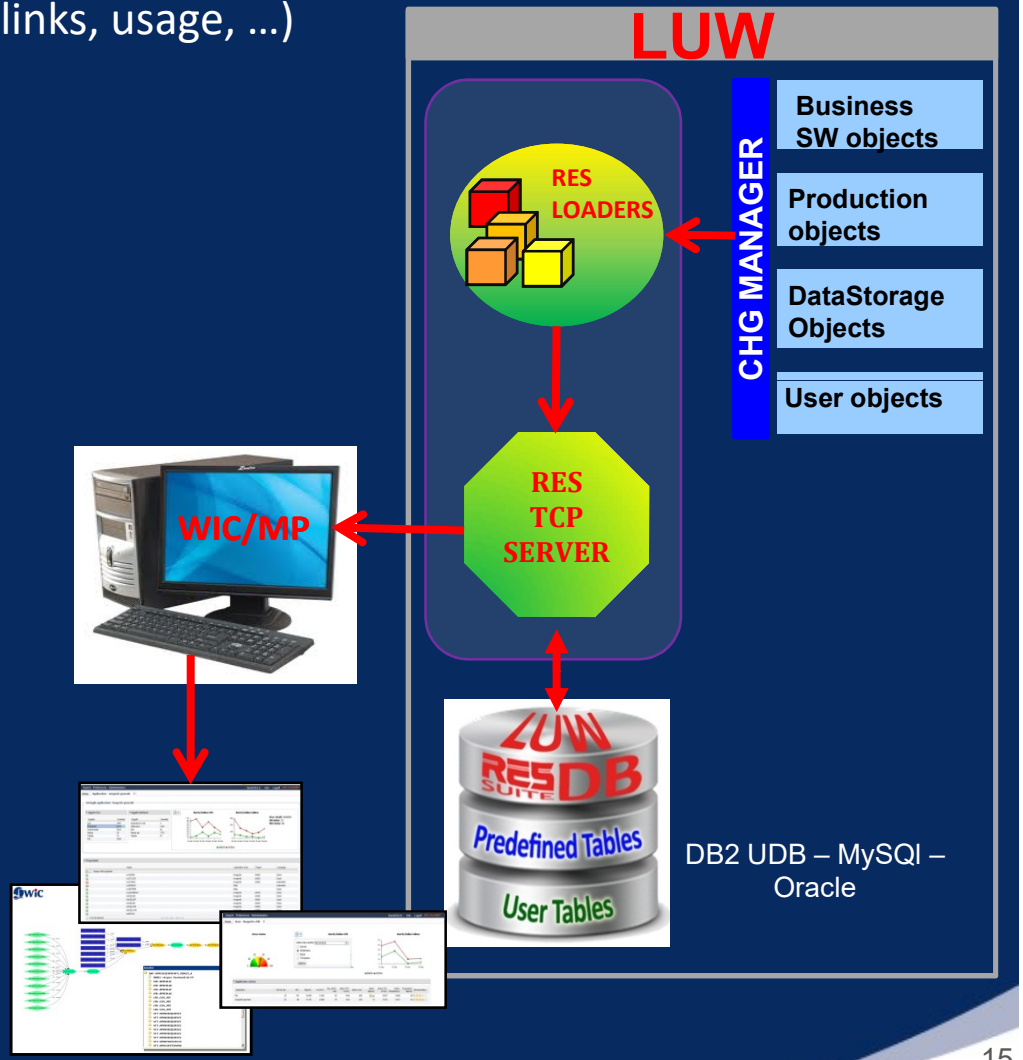
- RES DMD - Data Meaning Discovery

Docet/EV, the RES Suite solution for the SW cartography

an important "brick in the wall"

Docet/EV

- **Detailed SW documentation** (isolation, links, usage, …)
- **topography**
- **third-party vulnerability check**
- **data usage**
- **impact analysis**
- **metrics and quality assurance**



Main features of **RES IT Docet/EV**

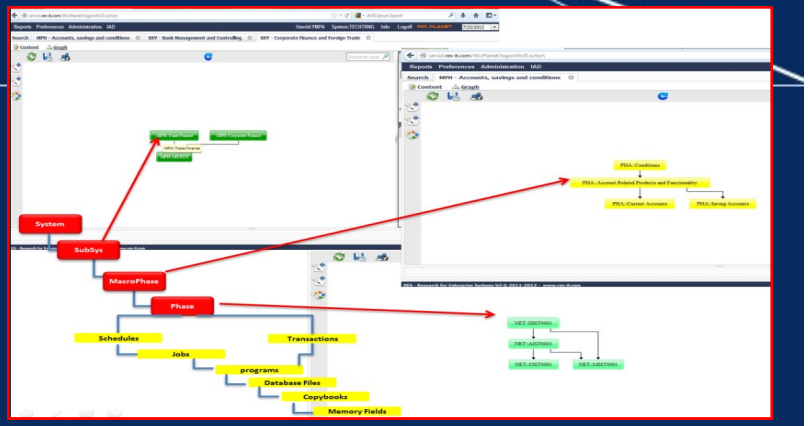
- **Describes in detail** (enterprise level):
  - Batch **Schedules**
  - **JOBs/scripts** (content and source)
  - **Files** and **Data Base** usage by JOBs / Programs
  - **Programs/Classes** invoked by JOBs
  - **Links** between all kind of objects
- Provides **impact analysis** starting from any SW resource
- Identify third-party SW components that expose to **risk of breach**, **vulnerability**
- **Connection** with **change-management systems** and **versioning systems**
- **Aggregates** applications through a "**business**" or "**functional**" view
- **Identifies obsolete** SW components
- **SW Metrics:** all standard Metrics + Open Metrics – for OpenSystems (LUW) and Mainframe
- **SW Quality:**
  - deprecated statements
  - Internal standards fulfilling
  - relational Data Base performance
- **100% automatic** SW **discovery** and **analysis**

Docet/EV, the RES Suite solution for the SW cartography

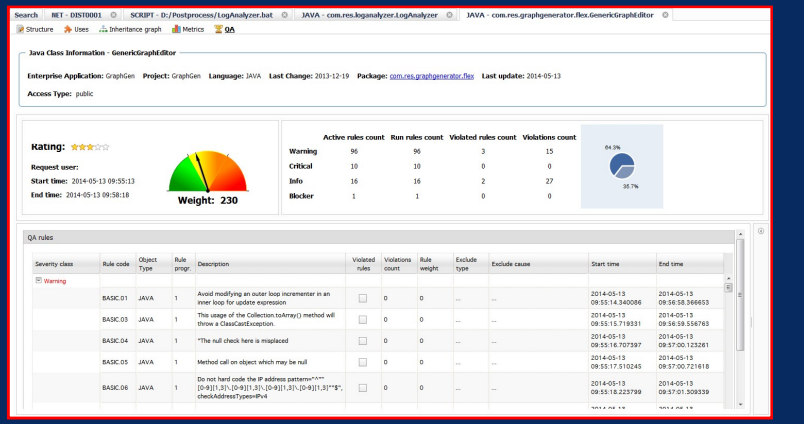
an important “brick in the wall”

Multiple purposes – One dashboard

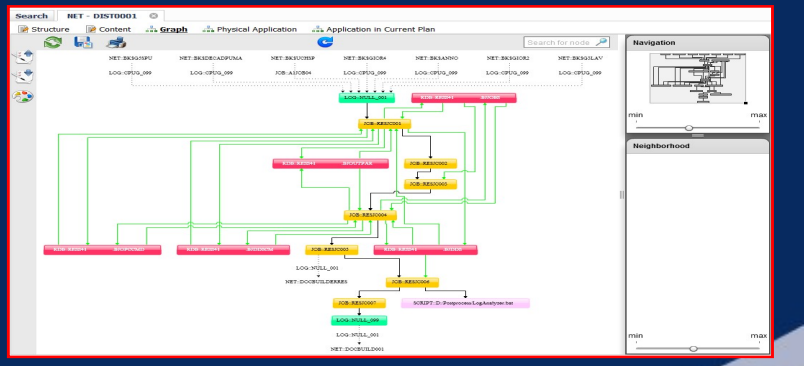
- LOB (Organizational) view of business applications



- SW Quality evaluation (SW Metrics, Vulnerability, …)
  - Compliance with regulations / standards



- SW applications topography, links between SW components

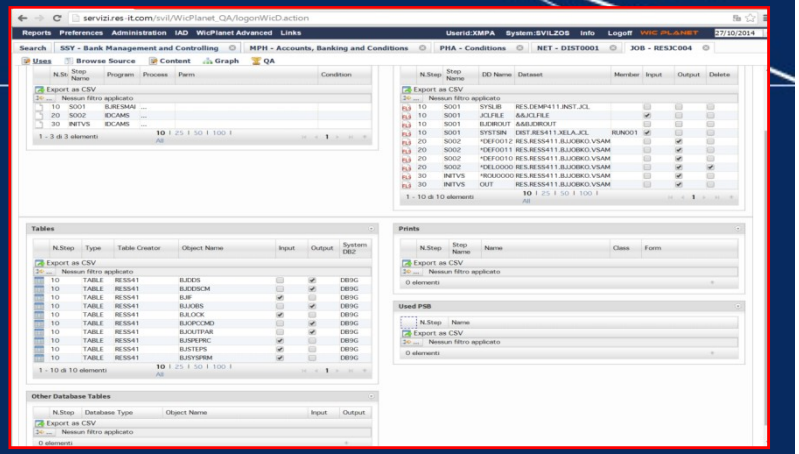


Docet/EV, the RES Suite solution for the SW cartography

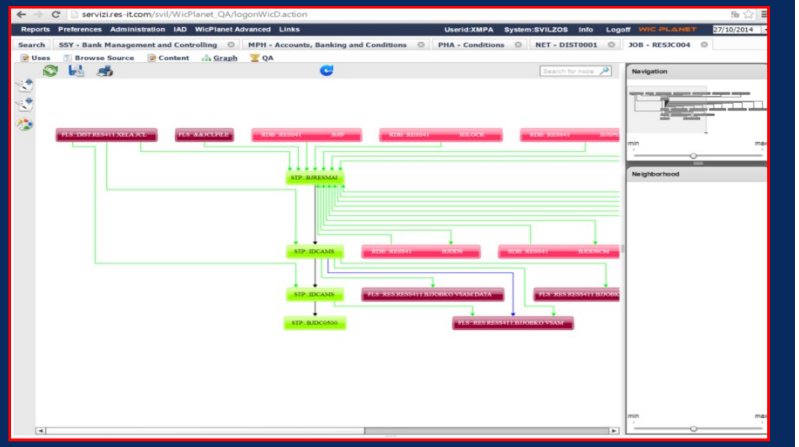
an important “brick in the wall”

Multiple purposes – One dashboard

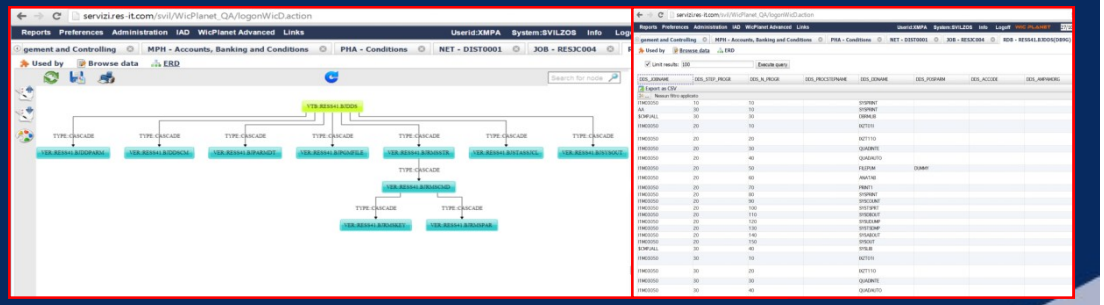
- Impact Analysis who-use-what, what-if, …



- Analysis of Data Usage by jobs, programs, …



- Data Base Structure analysis, referential integrity



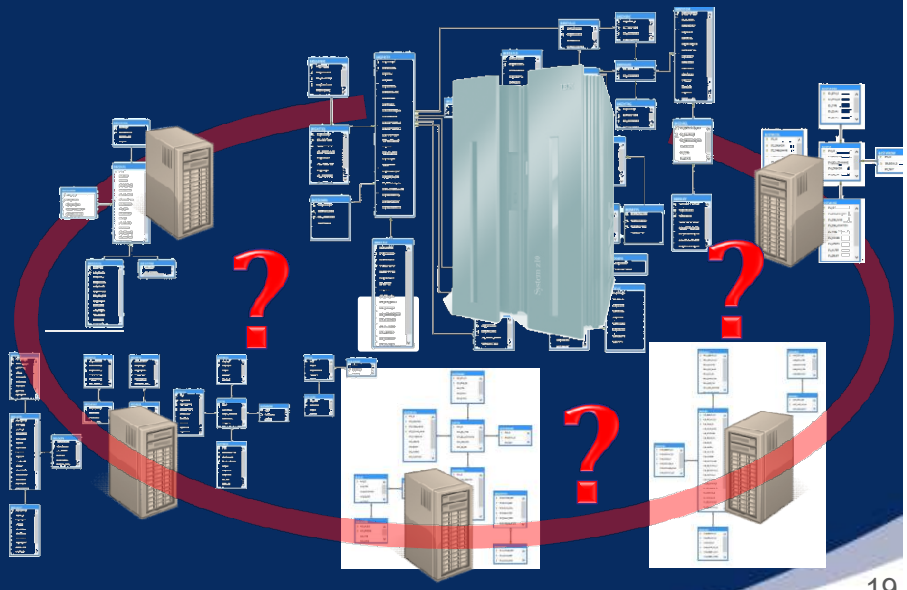
GDPR DMD, the RES Suite discovery of sensitive data

an important "brick in the wall"

GDPR DMD (Data Meaning Discovery)

- Automatic recognition of the meaning of data
- Provides info to support DBA, Data Administrator, SW developers, anyone who need to use data files
- Essential for projects like:
  - GDPR compliance ● Data Masking ● Impact Analysis ● Data Archival ● Data Quality Assurance ● ...
- Essential to understand where a piece of information is located

  (e.g. when a delete is required)
- Works on Data Files, CSV and DBMS like:
  - Oracle ● SQLServer ● DB2 z/Os ● DB2 UDB ● MySql ● ...



GDPR DMD, the RES Suite discovery of sensitive data

an important "brick in the wall"

GDPR DMD (Data Meaning Discovery)

Recognition through:

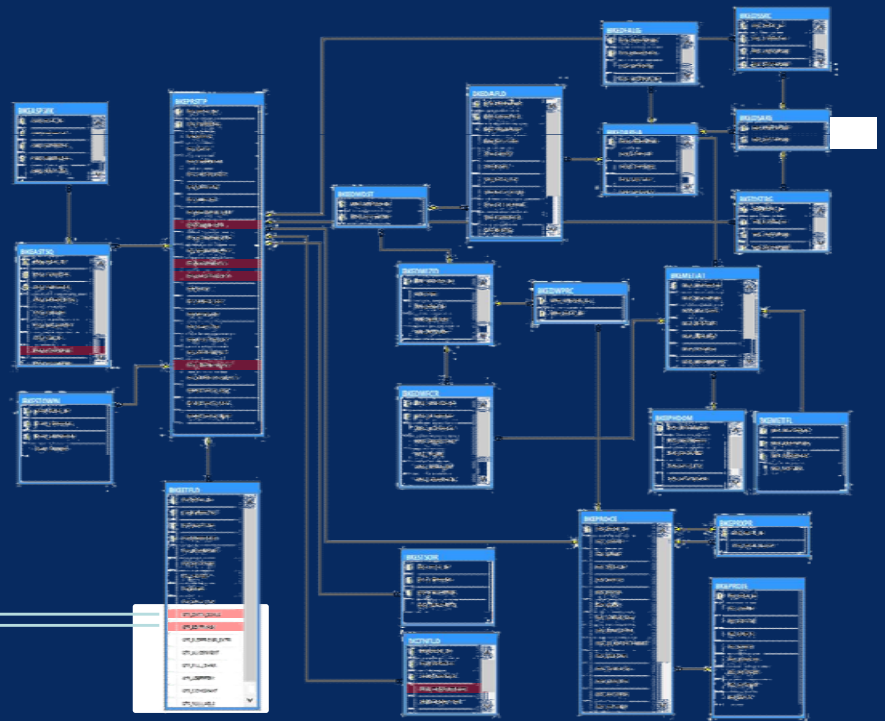
- Statistic Lookup Tables (surname, city, company, ...)
- Domain Tables (branch office, province, ...)
- Algoriths (Tax id num, ...)

Value	Frequency
MÜLLER	0,57332%
SCHMIDT	0,48326%
SCHNEIDER	0,39198%
FISCHER	0,33814%
MEYER	0,29965%
WEBER	0,25768%
…	
...	

Surnames

Names

Value	Frequency
MARK	2,8024%
FRANK	2,2165%
KARL	2,0547%
PETER	1,8756%
BRIGIT	1,7432%
KRISTEN	1,6745%
…	…



GDPR DMD, the RES Suite discovery of sensitive data

an important “brick in the wall”

GDPR DMD (Data Meaning Discovery)

Example of report (1 of 2):

FLD002	FLD003	FLD005	FLD008	FLD009	FLD010	FLD011	FLD013	FLD014
	ZYRTHM72P54F205Q	ZOEY THOMAS	LOS ANGELES	3332767084			AO7764625	
	RLDMLLI68R20Z330X	ORLANDO MILLER	PHILADELPHIA					ORLANDO
52334927741	GNVDNC40L03C145H	GINEVRA DUNCAN	MOAB					GINEVRA
	MRCCLR9R30E511E	MARCUS CLARK	NEW YORK CITY	332745553				
	ELSLEE75R66G062E	ELISABETH LEE	SACRAMENTO	3406659507				
91434921242	JSNJHNA60E02L682T	JASON JOHNSON	ORLANDO	3470334192				
	GRGSMTL43S51L219U	PAUL SMITH	SAINT GEORGE	0118993265	P_SMITH@GMAILCOM			
	ANNRBN71A62F839S	ANN ROBINSON	LOS ANGELES					
	WSHMLN66C04F704X	WASHINGTON MILANI	BETHESDA	3398547300			AJ7184387	WASHINGTON
	THMBRB64T08E734G	THOMAS BARBER	BOSTON					
	JSPLYN63B14Z216G	JOSEPHINE LYON	SANTA FE					
	JNTLAR81B10L682U	JONATHAN LEAR	SANTA ANA	3338392845				
	PTTGRB59A28I725M	PATTY GRUBER	WASHINGTON	3474349427				
	JKSSNS73S23I073W	JACKSON SANSOVINO	LOS ANGELES	3396832236			AO598289	JACKSON
	EGNNDRB26D869Q	EUGENE ANDERSSON	EUGENE	331776170				EUGENE
	GLNSPK57D30E014K	GLENDA SPIKE	NAXOS					
	DNLPRD75B57C665L	DANIEL PARODI	WASHINGTON D.C.	3381816774				
90002285711	AGAAGRC71L49G337Q	AUGUSTA GARCIA	AUGUSTA	0521772662		0521754362		AUGUSTA
	RCELON66A17L736U	ERIC LEON	LOS ANGELES	41000634660	ERIC96.LEON@GMAIL.COM		AK9438147	

GDPR DMD, the RES Suite discovery of sensitive data

an important "brick in the wall"

GDPR DMD (Data Meaning Discovery)

Example of report (2 of 2):

COLNAME	COLTYPE	LENGTH	SCALE
FLD001	DECIMAL	9	0
FLD002	CHAR	11	0
FLD003	CHAR	16	0
FLD004	CHAR	1	0
FLD005	CHAR	50	0
FLD006	DATE	4	0
FLD007	CHAR	2	0
FLD008	CHAR	30	0
FLD009	CHAR	20	0
FLD010	CHAR	50	0
FLD011	CHAR	20	0
FLD012	CHAR	3	0
FLD013	CHAR	16	0
FLD014	CHAR	30	0

Field Name	DataClass	SDtClass Observations frequency	SDtClass Observations number
FLD002	VAT NUM	88%	14
FLD003	TAX ID NUM	98%	926

Field Name	DataClass	Affinity Index	Affinity Index Confidence
FLD005	NAME AND SURNAME	18	50
FLD007	PROVINCE	70	27
FLD008	CITY	19	44
FLD014	CITY	3	93
FLD014	NAME	3	93

Affinity Index: affinity of belonging of data to a specific data-class

Affinity Index Confidence: reliability of the affinity index

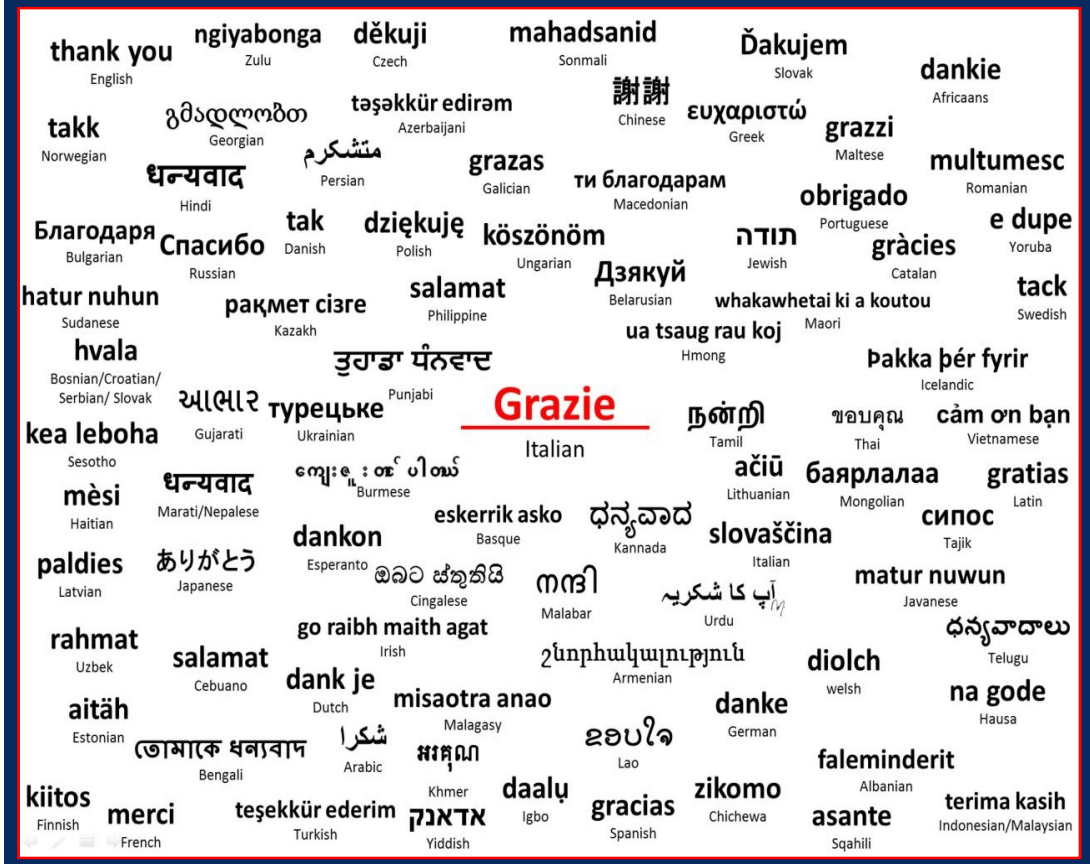
Some clients

who already took advantage from the **RES Suite** services

- Agos Ducato
- Axa Tech
- Banca CARIGE
- Banca d'Italia
- Banca delle Marche
- Banca Intesa San Paolo
- Banca Monte dei Paschi di Siena
- Banca Popolare di Milano
- Banca Popolare di Sondrio
- Bankadati – Creval SS
- BBVA Spain
- BCBS of Kansas
- Banque et Caisse d'Epargne de l'Etat Luxembourg
- BNL - BNP Paribas
- BPER Services
- Canadian Railway
- Cariparma – Silca - Crédit Agricole
- Cedacri
- Cembra Money Bank
- Caixa Geral de Depósitos
- Cofactor
- Deutsche Bank AG
- DTCC Depository Trust Company
- DWP Bank
- EQUENS
- Esselunga
- Federated Cooperative Ltd.
- Fondiaria SAI
- Global Value (Fiat)
- Grupo Mutua Madrilena
- Grupo Mutua Madrilena
- Gruppo UnipolSAI
- Guardian Life Insurance
- HP-EDS
- IBM Italy
- IBM Spain
- IBM Portugal
- IBM USA
- ISIDE - BCC Sistemi Informatici
- Jiangsu Rural Credit Commercial Bank
- Kmart SEARS
- Millennium BCP
- MIS (Mediobanca Innovation Services)
- Natixis Banque
- NiSource
- Novo Banco
- Poste Italiane
- Raiffeisen Bank
- Reale ITES
- SEC Servizi
- SGSS (Société générale Securities Services)
- SGS Banco Popolare
- State Auto Mutual
- Tampa Electric Company
- Telefonica - VIVO do Brazil
- Thomson Reuters
- T-System Brazil
- UBISS
- UBS
- UNICREDIT Global Information Services
- University of Wisconsin - Madison

Thank you for your attention

stay tuned, visit **www.res-it.com/en**



Marco Passerini - RES IT srl

VP MKT & International Operations

marco.passerini@res-it.com
www.res-it.com/en
@MarcoPasseriniR

T - +39 02 84907 125 M - +39 335 7474394
US: +1 646 480 0274