OBJECT MANAGEMENT GROUP

OMG IIoT Standards at Work

An Overview

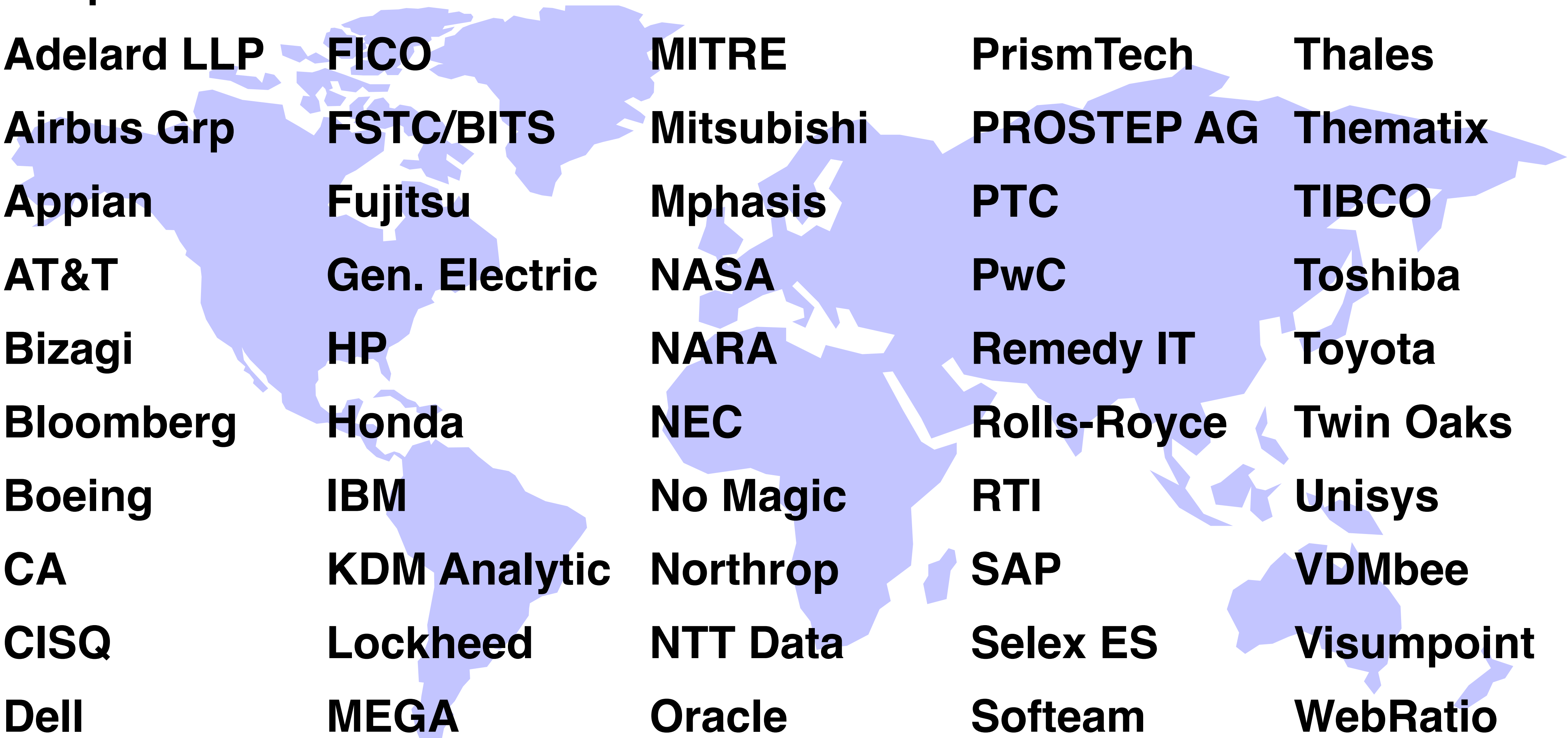
Andrew Watson
OMG Technical Director

Introducing OMG

- One of the most successful forums for creating open integration standards in the computer industry
  - Middleware platforms (DDS, CORBA & related specs)
  - Modelling platforms (UML, BPMN, SysML & related work)
  - Systems Assurance (SACM, DAF for SSCD ...)
  - Vertical domain specifications (C4I, Robotics, Healthcare ...)
- Member-controlled industrial consortium
  - Both vendors and users
  - Not-for-profit
- Interfaces freely available to all
  - Visit http://www.omg.org

OBJECT MANAGEMENT GROUP

Worldwide Membership



ACORD
Adaptive
Adelard LLP
Airbus Grp
Appian
AT&T
Bizagi
Bloomberg
Boeing
CA
CISQ
Dell
Eclipse Fndn.

EDM Council
EMC
FICO
FSTC/BITS
Fujitsu
Gen. Electric
HP
Honda
IBM
KDM Analytic
Lockheed
MEGA
Microsoft

Micro Focus
MID GmbH
MITRE
Mitsubishi
Mphasis
NASA
NARA
NEC
No Magic
Northrop
NTT Data
Oracle
Orbus

OSD
Penn Nat'l
PrismTech
PROSTEP AG
PTC
PwC
Remedy IT
Rolls-Royce
RTI
SAP
Selex ES
Softeam
Software AG

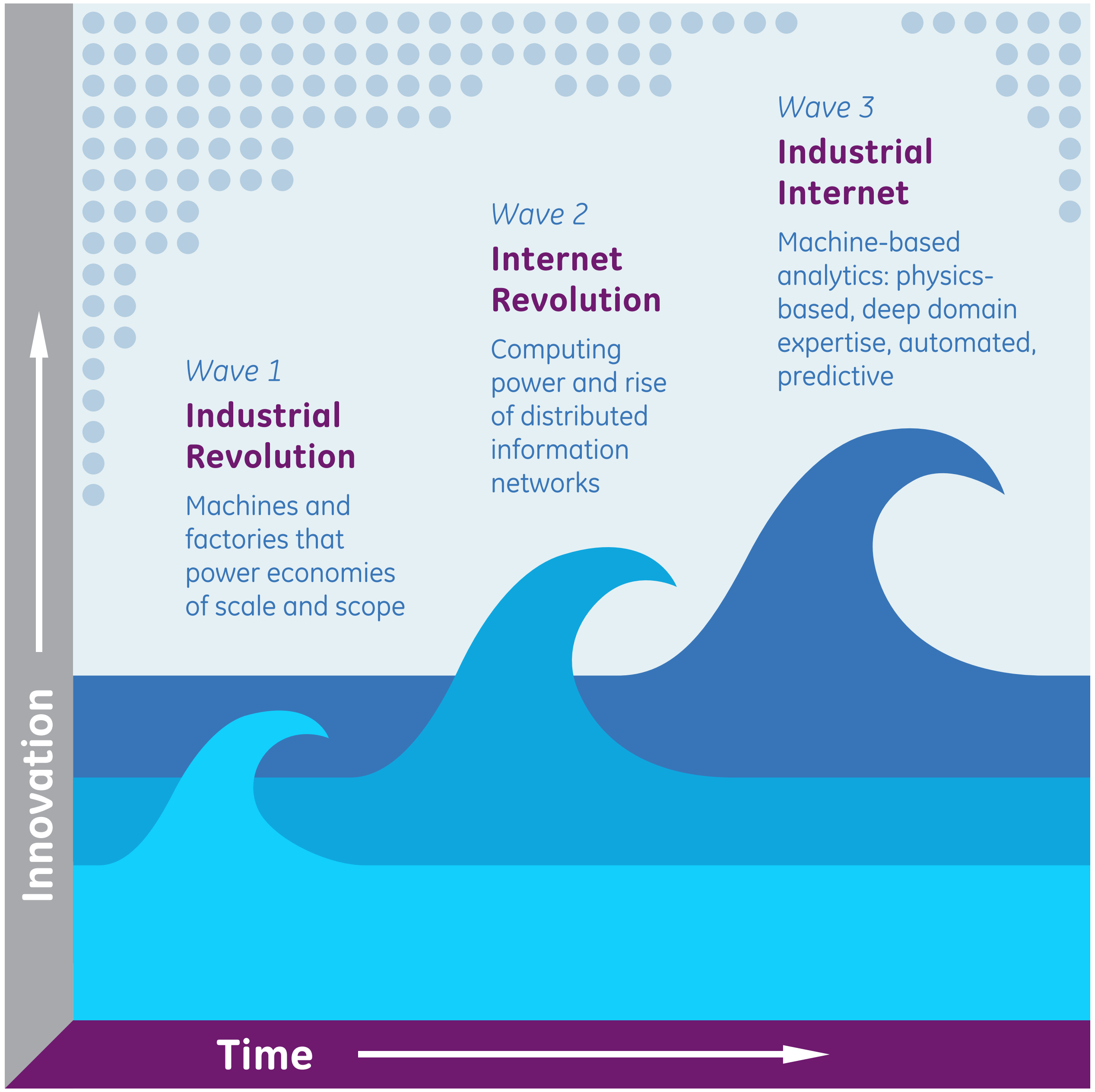
Sparx
State St
Thales
Thematix
TIBCO
Toshiba
Toyota
Twin Oaks
Unisys
VDMbee
Visumpoint
WebRatio
(200+ more)

Availability

- OMG adopts and publishes interface specifications
  - Implementation available from at least one OMG member
- Interfaces freely available to all (members or not)
  - No export restrictions
  - No specification licence, no payment
  - Best-effort assurances on IPR constraints
- Decisions taken by members
  - Strategic direction controlled by Board
  - Technical direction determined by Technology Committees
- Long-term ties to ISO sees many OMG specifications republished unchanged as International Standards

IIoT: The Next Economic Revolution?

- Industrial revolution replaced muscle power with machines
  - Dramatic, continuing rise in global living standards began
- Information revolution similarly boosted brain power
- Their covergence promises further wave of rising productivity and prosperity


Wave 1

Industrial Revolution

Machines and factories that power economies of scale and scope

Wave 2

Internet Revolution

Computing power and rise of distributed information networks

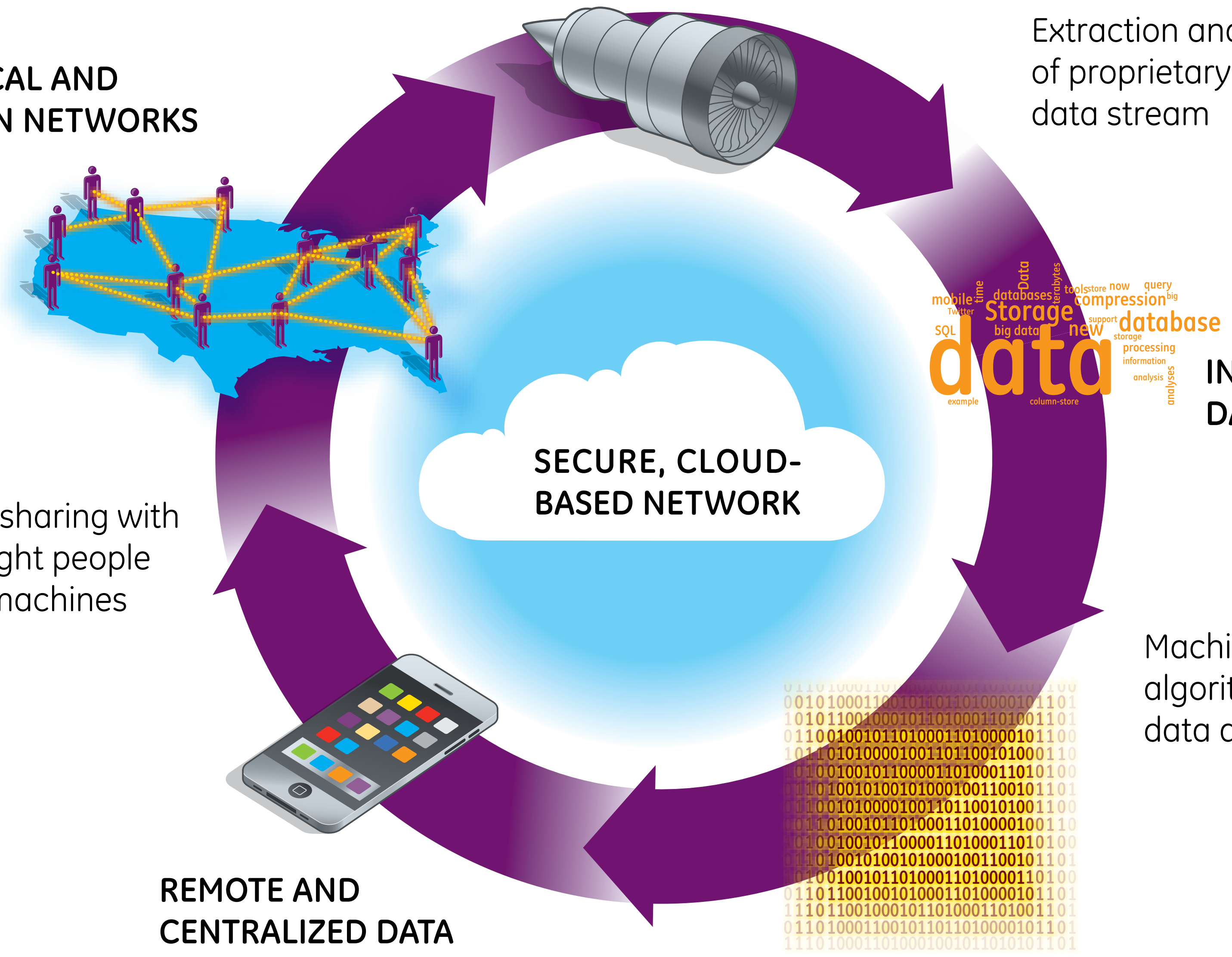
Wave 3

Industrial Internet

Machine-based analytics: physics-based, deep domain expertise, automated, predictive

Source: Evans & Annunziata, GE, 26 Nov 2012

Industrial Internet Data Loop



INSTRUMENTED INDUSTRIAL MACHINE

Extraction and storage of proprietary machine data stream

INDUSTRIAL DATA SYSTEMS

Machine-based algorithms and data analysis

BIG DATA ANALYTICS

REMOTE AND CENTRALIZED DATA VISUALIZATION

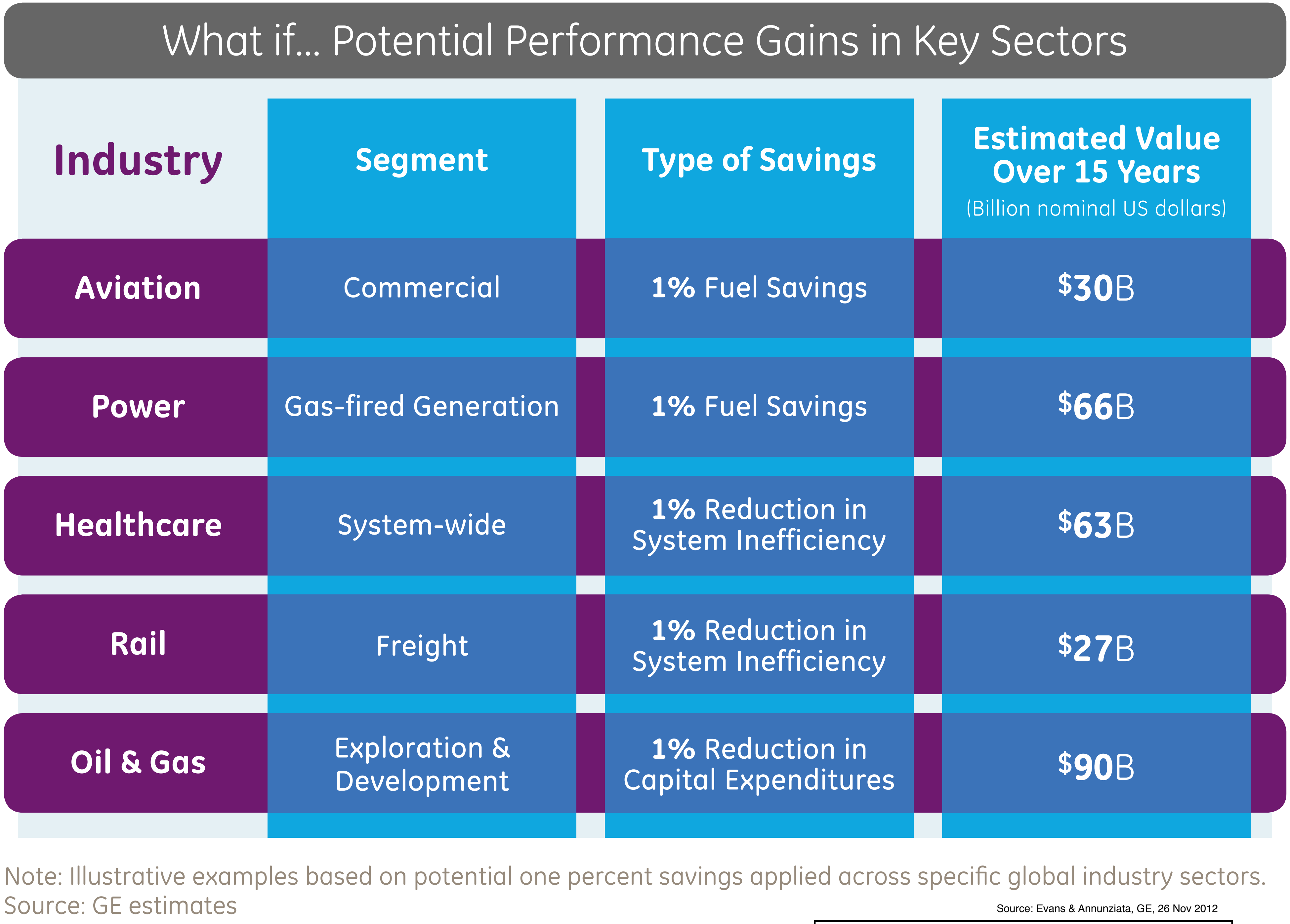
Data sharing with the right people and machines

PHYSICAL AND HUMAN NETWORKS

Intelligence flows back into machines

Source: Evans & Annunziata, GE, 26 Nov 2012

The Benefits



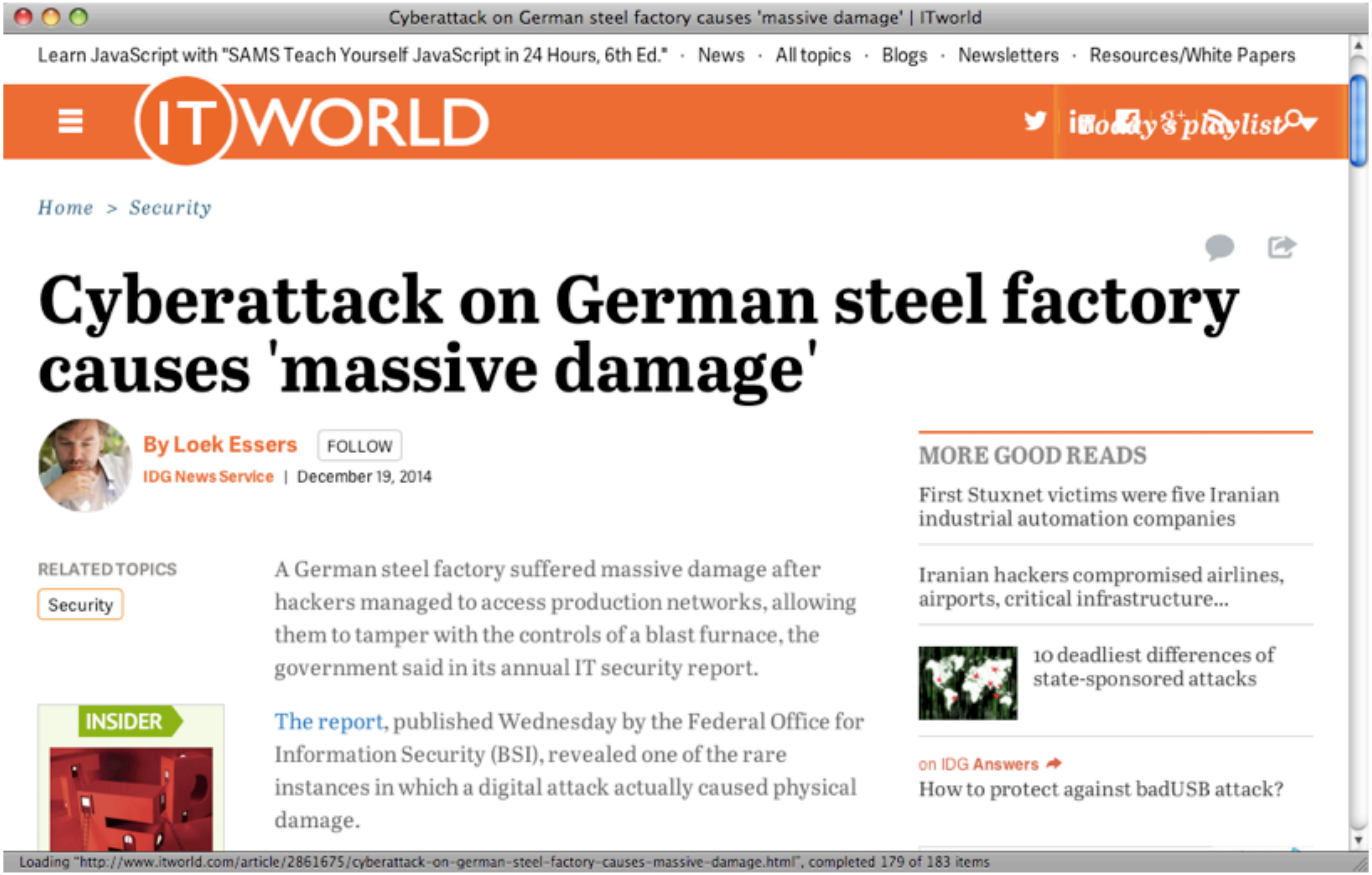
What if… Potential Performance Gains in Key Sectors

Industry	Segment	Type of Savings	Estimated Value Over 15 Years (Billion nominal US dollars)
Aviation	Commercial	1% Fuel Savings	$30B
Power	Gas-fired Generation	1% Fuel Savings	$66B
Healthcare	System-wide	1% Reduction in System Inefficiency	$63B
Rail	Freight	1% Reduction in System Inefficiency	$27B
Oil & Gas	Exploration & Development	1% Reduction in Capital Expenditures	$90B

Note: Illustrative examples based on potential one percent savings applied across specific global industry sectors.
Source: GE estimates

Source: Evans & Annunziata, GE, 26 Nov 2012

The Risks


Learn JavaScript with "SAMS Teach Yourself JavaScript in 24 Hours, 6th Ed." · News · All topics · Blogs · Newsletters · Resources/White Papers
IT WORLD
Today's playlist
Home > Security
FOLLOW
RELATED TOPICS
Security
INSIDER

Cyberattack on German steel factory causes 'massive damage' | ITworld

Cyberattack on German steel factory causes 'massive damage'

By Loek Essers
IDG News Service | December 19, 2014

A German steel factory suffered massive damage after hackers managed to access production networks, allowing them to tamper with the controls of a blast furnace, the government said in its annual IT security report.

The report, published Wednesday by the Federal Office for Information Security (BSI), revealed one of the rare instances in which a digital attack actually caused physical damage.

MORE GOOD READS

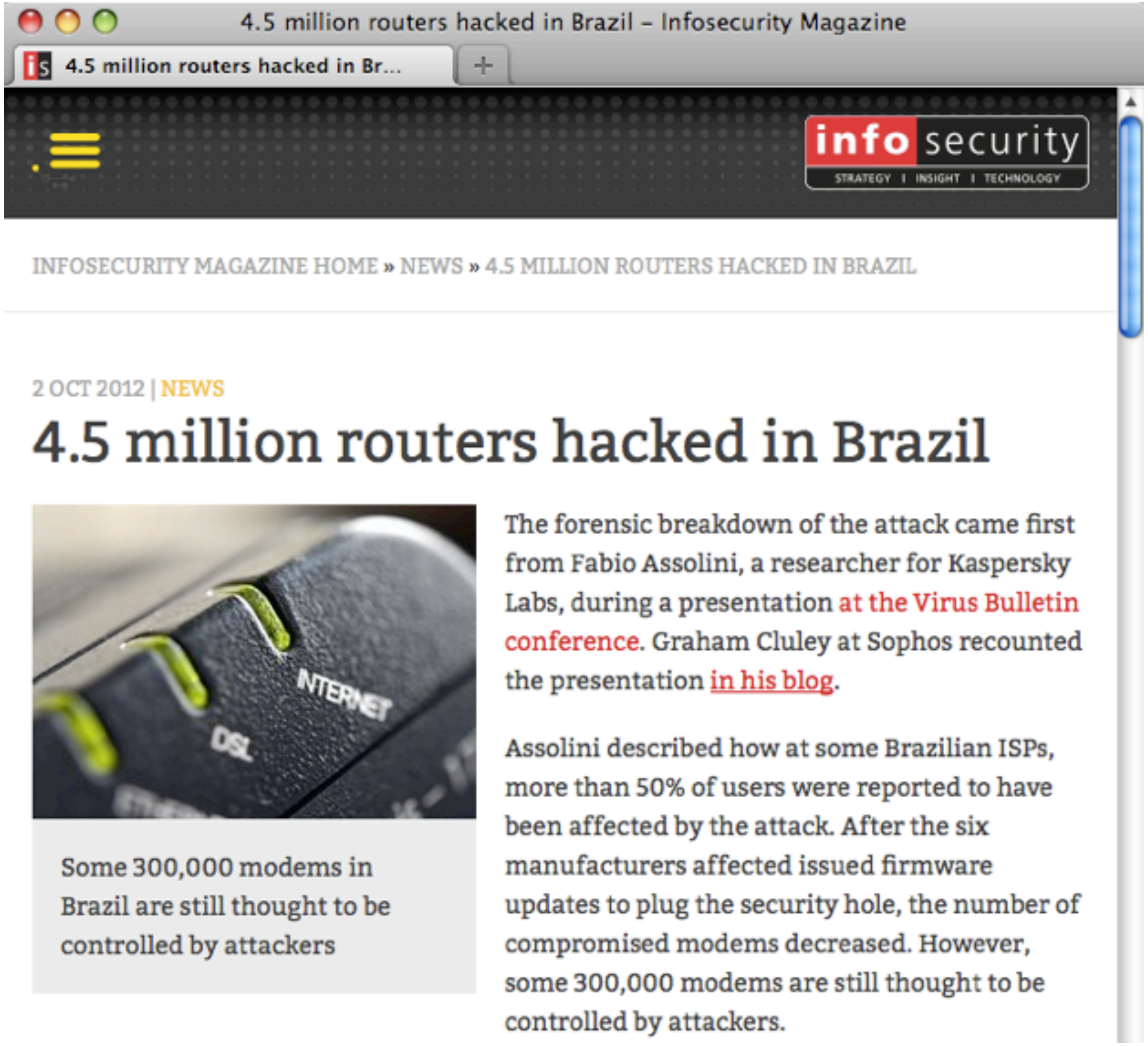
First Stuxnet victims were five Iranian industrial automation companies

Iranian hackers compromised airlines, airports, critical infrastructure...

10 deadliest differences of state-sponsored attacks

on IDG Answers
How to protect against badUSB attack?

Loading "http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html", completed 179 of 183 items


4.5 million routers hacked in Brazil – Infosecurity Magazine
4.5 million routers hacked in Br...
+
info security
STRATEGY | INSIGHT | TECHNOLOGY
INTERNET
DSL

INFOSECURITY MAGAZINE HOME » NEWS » 4.5 MILLION ROUTERS HACKED IN BRAZIL

2 OCT 2012 | NEWS

4.5 million routers hacked in Brazil

Some 300,000 modems in Brazil are still thought to be controlled by attackers

The forensic breakdown of the attack came first from Fabio Assolini, a researcher for Kaspersky Labs, during a presentation at the Virus Bulletin conference. Graham Cluley at Sophos recounted the presentation in his blog.

Assolini described how at some Brazilian ISPs, more than 50% of users were reported to have been affected by the attack. After the six manufacturers affected issued firmware updates to plug the security hole, the number of compromised modems decreased. However, some 300,000 modems are still thought to be controlled by attackers.

IIoT prerequisites include ...

- Sensors & advanced instrumentation embedded in machines of all types, collecting data & providing fine-grained control
  - Enormous data volumes distributed & analysed in real time
- Unparalleled cyber security to protect sensitive information
  - Stop bad actors remotely interfering in physical systems
- Designers with tools & skills cutting across multiple engineering disciplines, data science, cyber security, UIs
  - Squeezing inefficiencies out of complex systems
- OMG publishes widely-used specifications in all these areas
  - *Already* enabling IIoT-based innovation
  - Some relevant OMG activities are ...

SysML

- Graphical modelling language for specifying, analyzing, designing & verifying complex systems that may include hardware, software, information, personnel, procedures
  - Provides means to precisely model large, complex systems-of-systems, from requirements to acceptance
- Aids communication across engineering disciplines
  - Co-developed with International Council on Systems Engineering (INCOSE)
  - Widespread tool support

Interaction Flow Modelling Language (IFML)

- User interface design will make or break IIoT systems
  - Requires seamless interaction with hardware & software to minimise unnecessary input & undesired output, yet achieve desired results
  - Example: Cockpit interface of airliner (within airline fleet)
- IFML describes user’s interaction with system, independent of presentation technology
  - Interaction Flow Models formally specify different perspectives of the front-end: content, interface composition, interaction, navigation options, connection with business logic, presentation

Systems Assurance specifications

- Common framework for analysis & exchange of information about system assurance and trustworthiness, including ...
- Structured Assurance Case Metamodel
  - For representing auditable claims, arguments & evidence that system satisfies particular requirements
- Automated Source Code Security Measure
  - Measured by detecting most-exploited source-code weaknesses (e.g. SQL Injection 1st, Buffer overflow 3rd)
- Dependability Assurance Framework for Safety-Sensitive Consumer Devices
  - Methodology for dependability argumentation for safety-sensitive consumer devices with embedded software

Data Distribution Service

- **Integration "glue" for IIoT applications spanning data centres to edge sensors**
  - **Creates virtual, decentralised global data space abstraction**
  - **Excellent performance with real-time guarantees**
  - **Proven-interoperable products from multiple vendors**
  - **Available for safety-critical systems to DO-178C Level A**
  - **Integrated security framework**
  - **Fine-grained access control**
  - **Highly scalable**
  - **Proven in multiple mission-critical applications**

Next ...

- Expert presenters from OMG Member organisations provide much more detail on:
  - DDS in the IIoT
  - IFML & the Role of User Interaction in the IIoT vision
  - CISQ & controlling risk in the IoT Universe
  - System Assurance - Discipline of Building Confidence that System is Trustworthy
  - SysML & System Modelling Benefits for Complex IIoT systems

For more information

OMG:	**http://www.omg.org**
Email:	**andrew@omg.org**

Thank You!

Questions?